GENERALISED KEY DISTRIBUTION PATTERNS

Julia Catherine Novak

Royal Holloway
University of London

Thesis submitted to
The University of London
for the degree of
Doctor of Philosophy
2012.

Declaration

The work presented in this thesis is the result of original research carried out by myself whilst enrolled in the Department of Mathematics at Royal Holloway, University of London as a candidate for the degree of Doctor of Philosophy. Where I have consulted the work of others, this is always clearly stated.

Julia Novak

Julia Novak
February 2012

Acknowledgements

My biggest thanks go to my supervisor Professor Keith Martin for his never ending patience and support. My second supervisors, Professor Peter Wild and Professor Chris Mitchell have also offered me great support and helpful advice along the way, for which I am very grateful. Most importantly, however, I wish to thank my friends and family, simply for being my friends and family. I will not name these people, since they know who they are and will (almost certainly) never read this thesis.

I am thankful to all staff in the mathematics departments of three separate universities:

1. The University of Salford, where I completed my MMath. I am forever indebted to the staff there for introducing me to the pleasure of mathematics. In particular, I wish to thank John Wakefield, I never understood mathematics before he showed me how to and Professor Ray Hill, without whom I would never have considered a PhD.

2. Royal Holloway, University of London. I am grateful to all the staff (particularly Keith) for their constant support throughout the ups and downs of my PhD studies.

3. The University of Auckland, where I now work as a Teaching Fellow. I am thankful that the department accommodated both me and my continued work on this thesis, and gave me the opportunity to teach and introduce others to the pleasure of mathematics.

Finally, I wish to thank Vodafone Group Research and Development for their generous financial support and the Engineering and Physical Sciences Research Council (EPSRC) for the joint CASE award, with Vodafone, that enabled this research.

Abstract

Given a network of users, with certain secure communication requirements, we examine the mathematics that underpins the distribution of the necessary secret information, to enable the secure communications within that network. More precisely, we let $\mathscr{P}$ be a network of users and $\mathscr{G}$, $\mathscr{F}$ be some predetermined families of subsets of those users. The secret information (*keys* or *subkeys*) must be distributed in such a way that for any $G \in \mathscr{G}$, the members of G can communicate securely among themselves without fear of the members of some $F \in \mathscr{F}$ (that have no users in common with G), colluding together to either eavesdrop on what is being said (and understand the content of the message) or tamper with the message, undetected.

In the case when $\mathscr{G}$ and $\mathscr{F}$ comprise of all the subsets of $\mathscr{P}$ that have some fixed cardinality t and w respectively, we have a well-known and much studied problem. However, in this thesis we remove these rigid cardinality constraints and make $\mathscr{G}$ and $\mathscr{F}$ as unrestricted as possible. This allows for situations where the members of $\mathscr{G}$ and $\mathscr{F}$ are completely irregular, giving a much less well-known and less studied problem.

Without any regularity emanating from cardinality constraints, the best approach to the study of these general structures is unclear. It is unreasonable to expect that highly regular objects (such as designs or finite geometries) play any significant role in the analysis of such potentially irregular structures. Thus, we require some new techniques and a more general approach. In this thesis we use methods from set theory and ideas from convex analysis in order to construct these general structures and provide some mathematical insight into their behaviour. Furthermore, we analyse these general structures by exploiting the proof techniques of other authors in new ways, tightening existing inequalities and generalising results from the literature.

Contents

Chapter 1

Introduction

In this chapter we present the background material required for our investigations and give a brief overview of some relevant concepts. (More detailed background material can be found in [56, 70] or [83].)

We begin with Section 1.1 where we discuss the notion of *cryptography* and highlight the importance of *cryptographic keys.* Then, in Section 1.2 we consider the management of *cryptographic keys* and the establishment of *common keys* for groups of users wishing to communicate *securely.*

Following on from these discussions of *cryptography* we explore *key predistribution schemes*, which are a specific type of *key establishment scheme.* Section 1.3 covers settings for *key predistribution schemes*, a model of their structure and some measures of their *efficiency.* In Section 1.4 we examine different approaches to the construction of *key predistribution schemes.*

Section 1.5 then focusses upon *key distribution patterns*, which can be used in the construction of *key predistribution schemes*, and form the basis of this thesis. We discuss previous work completed by other authors in this area and finally, we conclude Chapter 1, with Section 1.6, which summarises the aims of this thesis and presents an overview of the thesis structure.

1.1 Cryptography

The basic aim of *cryptography* is to enable two people to communicate over an insecure channel (be it a telephone line, a radio, or a computer network) in a *secure* way. That is, in such a way that any *attacker* (i.e. any other person attempting to listen in, or interfere with the conversation) is unable to understand what is being said or tamper with the message undetected. The term cryptography describes a range of cryptographic services, including techniques for providing both *confidentiality*, ensuring the secrecy of the content of a message, and *authentication*, ensuring that a message arrives unchanged and from an identified originator. We shall phrase our discussions in terms of confidentiality, but note that they also apply to cryptography in its broadest sense.

Over recent years cryptography has developed into a toolkit of mathematical techniques necessary for the confidentiality of electronic communication. In the modern world cryptography is all around us and plays an essential role in our everyday lives. Cryptographic mechanisms are used in mobile phones, banking services, secure internet connections and many other places.

The majority of cryptographic mechanisms are publicly available and as such are open to scrutiny and analysis. The security of an entire mechanism relies upon the use of *keys.* Keys are usually numbers, selected at random, from a large set of numbers and are a feature of almost all cryptographic mechanisms. Each group of users within a network who wish to communicate confidentially will require their own key in order to do so (all other users may be considered as potential attackers).

In *symmetric-key cryptography* the key to be used by the sender to encrypt a message, and the key to be used by the receiver to decrypt that message are identical and must be kept private. Assuming the secrecy of the key, any attacker who gains access to an encrypted message must have only a very small probability of recovering either the original sent message, or the key itself. The confidentiality of the encrypted message is entirely dependent on the secrecy of the key used, even if complete knowledge of the cryptographic mechanism is made publicly available.

In *public-key cryptography* each user has a pair of keys, one needs to be kept private and the other key can be made publicly available. Messages are encrypted using the recipient's public key and can only be decrypted using the corresponding private key. In order for public-key cryptography to be considered secure, it must be computationally unfeasible to determine a private key from the corresponding public key, even if an attacker has gained access to encrypted messages and has complete knowledge of the cryptographic mechanism used. As with symmetric-key cryptography, the confidentiality of the encrypted message is entirely dependent on the secrecy of the private keys.

Both symmetric-key and public-key cryptographic mechanisms are used extensively and often in tandem. However, for a range of applications symmetric-key mechanisms are favoured, due to their speed and simplicity. Within this thesis we restrict ourselves solely to the study of symmetric-key cryptography.

1.2 Key Management and Establishment

As stated previously, the security of a cryptographic mechanism is based upon the use of keys. Due to this, the management of crytographic keys is an important area of research, see [4, 7, 12] and [52]. The study of key management can be broken down into phases concerning the life-cycle of a cryptographic key. Four of these phases are:

1. *Key generation*, which covers the creation of keys.
2. *Key establishment*, which is the methods by which the keys are distributed to the relevant users in the network.

3. *Key update*, which is the techniques used to renew or refresh the keys in the system.

4. *Key destruction*, which covers the deletion and disposal of keys when they are no longer of use.

In symmetric-key cryptography, the fundamental key management challenge is key establishment. The focus of key establishment is that of giving each group of users within a network who wish to communicate securely the ability to establish a common key. A *key establishment scheme* is a set of protocols that allows us to do just that. We must ensure that within a network of users, the right keys are established in the right places.

We shall normally assume the existence of a *trusted authority* (or TA), which is an entity that is considered to be trusted and secure by all users in a network. In many systems, a TA generates and distributes both secret and public information. All secret information must be distributed using *secure communication channels* between the TA and the users in the network. Secure channels provide both confidentiality and authentication for the information transmitted on them. Any public information can be distributed using inexpensive *broadcast channels* which ensure only the authentication of the transmitted data.

Key establishment schemes generally consist of the following three operational phases:

1. *Initialisation* - During the initialisation phase the TA generates and distributes all private and public information necessary for the initialisation of the scheme.

2. *Key establishment* - During the key establishment phase each group of users within the network who wish to communicate securely are able to establish a common key.

3. *Update* - During the optional update phase, information (both public and private) within the network is modified or replaced by the TA. The TA will refresh old keys before they expire and/or issue new keys to reflect any changes within the groups of users wishing to communicate securely.

The precise role of the TA is a major distinguisher between different key establishment schemes. In general, we cannot assume that the secure channels that exist between the TA and the users in the network will remain available throughout the lifetime of the scheme. If this were the case then the TA could simply generate and distribute common keys as and when required. In most schemes it is assumed that the secure channels between the TA and the users in the network are available during any update phase, however, it is the existence of these channels during the key establishment phase that is of significance to us.

A key establishment scheme in which the TA has the ability to communicate securely with the users in the network during the key establishment phase is known as a *key distribution scheme*, whereas a scheme in which the TA has no ability to communicate with the users during the key establishment phase is known as a *key predistribution scheme.*

1.3 Key Predistribution Schemes

A *key predistribution scheme (or KPS)* is a key establishment scheme with the following two properties:

- The TA is *offline* during the key establishment phase. That is, the secure channels between the TA and the users in the network are not available.

- The users within the network have no ability to communicate securely between themselves during the key establishment phase.

The reason for these restrictions is motivated by the complexity and the high computational costs of establishing secure communication channels. (The computational costs associated with broadcast channels are much smaller.) As such, schemes where the use of these channels is minimised are often preferred for both cost saving and practical purposes.

1.3.1 Settings for Key Predistribution Schemes

Key Predistribution Schemes are commonly used for key establishment in applications where secure communication is only required between each user and a central node (or *hub*). For example, in mobile telephony, the SIM card (within the mobile phone) is preloaded with keys. Secure communication between every mobile phone and a centralised authentication centre is enabled using a key predistribution scheme. In such a scheme the TA could predistribute just one unique key to each user (or SIM) and preload the hub (or authentication centre) with the set of all keys.

Over recent years network technology has evolved, resulting in the development of more dynamic, ad hoc networks. Without the ability to support an online TA, key predistribution schemes would seem the natural choice for key establishment in these ad hoc networks. Examples of such networks include *tactical networks*, *ambient networks*, *mobile ad hoc networks*, *vehicular networks* and *wireless sensor networks.*

A *wireless sensor network* (or *WSN*) is an ad hoc network consisting of spatially distributed *sensor nodes* that autonomously gather data and use wireless communications in order to relay that data. The nodes themselves are usually small, inexpensive, low powered devices and the number of nodes used varies extensively, depending on the application [75]. Most applications of WSNs involve the monitoring of some sort of hostile environment, (such as a war zone or the aftermath of a natural disaster), where the risk posed to more expensive devices would be deemed too high. It is the challenges posed by these applications that make key establishment schemes, that are specifically designed for use within wireless sensor networks, an interesting family of schemes to study. Due to this, many authors have considered such schemes, see [14] and the references within.

The main challenges for key establishment in a WSN are as follows:

1. There is no predetermined structure to the network.

2. The nodes relay data to other nodes, as well as acting as end points for communications.

3. Due to the hostile environments in which they are often deployed, the unavailability rate of the nodes in the network is potentially very high and there is an increased risk of node compromise.

4. The power, energy and memory constraints on the nodes result in the need for efficient network protocols and restrict the nodes ability to store large numbers of keys.

Given these challenges, it is clear that the use of secure communication channels, during key establishment, is impractical. As such, from the perspective of providing security services, wireless sensor networks lend themselves nicely to the use of symmetric key cryptography and key predistribution for key establishment, see [48, 53] and [82].

1.3.2 Modelling a KPS

A great variety of key predistribution schemes exist in the literature, see for example [8, 32, 43, 55] and [65]. In all cases, a TA distributes secret information among a network of users. Within the network of users we have two specified families of users, *privileged subsets* and *forbidden subsets*. The information from the TA is distributed in such a way that every user in a privileged subset is able to compute the common key associated with that subset. At the same time, any forbidden subset of users, outside of a privileged subset, is not able to obtain, or calculate between them, the key associated with that privileged subset.

More precisely, we have the following model of a KPS for a given family of privileged subsets $\mathscr{G}$ and a given family of forbidden subsets $\mathscr{F}$.

Definition 1.3.1. *A $(\mathscr{G}, \mathscr{F})$-KPS is a key establishment scheme such that:*

1. *For every privileged subset G in $\mathscr{G}$, any user belonging to G can compute the group key associated with the privileged subset G, (say K_G) from his own secret information (usually received from the TA upon initialisation of the scheme) and any publicly available material.*

2. *For any forbidden subset F in $\mathscr{F}$ and any disjoint G in $\mathscr{G}$, if all users belonging to F combine their secret information and take full advantage of any public information, then they remain unable to calculate the group key, K_G, or gain any information about the key.*

In many situations it is appropriate to define the privileged and forbidden subsets of a $(\mathscr{G}, \mathscr{F})$-KPS according to their cardinality. More specifically, we define:

- the set of privileged subsets to be all sets of users of some maximum specified cardinality, say t; and
- the set of forbidden subsets to be all sets of users of some maximum specified cardinality, say w.

Such a scheme would enable each subset of t or fewer users to communicate securely against any colluding subset of w or fewer other users. That is, if we let $\mathscr{P}$ be the set of all users in the network, then for some $t, w \geq 1$,

$$\mathscr{G} = \{G \in 2^{\mathscr{P}} : 1 \leq |G| \leq t\} \quad \text{and} \quad \mathscr{F} = \{F \in 2^{\mathscr{P}} : 1 \leq |F| \leq w\}.$$

We shall refer to key predistribution schemes defined in this way as *cardinality schemes* (since the privileged and forbidden subsets are defined according to their cardinality), or more precisely as (t, w)-*KPSs*.

In this thesis we only wish to consider KPSs in which all the privileged subsets are certain to be able to compute a common key. Therefore, we will concentrate on *deterministic* schemes, as opposed to *probabilistic* schemes (such as [19, 26, 31] and [50]) where the key associated with a privileged subset can be calculated with a certain probability. Also, we wish to concentrate on schemes whose security is independent of any computational assumptions. That is, we are interested in schemes with *unconditional security*, as opposed to schemes with *computational security*, where the security of the scheme is dependent on the computational resources available to an attacker.

1.3.3 Efficiency Measures

A basic KPS can be defined where the TA generates one secret key per privileged subset and distributes that key to every user in that privileged subset. Consider a KPS of this type for a network of v users, within which every pair of users forms a privileged subset and every individual user forms a forbidden subset. That is, we have a cardinality scheme, or more precisely, a $(2, 1)$-KPS. Since, if we let $\mathscr{P}$ be the set of all users in the network, then we have a $(\mathscr{G}, \mathscr{F})$-KPS, where $\mathscr{G} = \{G \in 2^{\mathscr{P}} : 1 \leq |G| \leq 2\}$ and $\mathscr{F} = \{F \in 2^{\mathscr{P}} : |F| = 1\}$.

Every pair of users (every $G \in \mathscr{G}$) holds a unique key in common and is able to communicate securely using that key. At the same time, no individual user outside of that pair (no $F \in \mathscr{F}$ such that $F \cap G = \varnothing$) is able to obtain any information on the secret key held by that pair of users.

In such a scheme each user would be required to store $v - 1$ keys, with the total number of keys in the system being $\frac{v(v-1)}{2}$. For large networks these storage requirements are considerable and, in many cases, impractical.

The network storage and user storage requirements in a KPS are important measures of the *efficiency* of a scheme; the smaller the storage, the more efficient the scheme is considered to be. As such, key predistribution schemes in which the key storage is lower than that of this most basic of KPSs (whilst maintaining the desired level of security) are usually preferred and are often referred to as "good" KPSs.

Reducing the key storage requirements in a KPS was a problem first tackled by Blom [5] in 1982 and continues to be an important area of research, see, for example [2, 6, 26, 39, 55, 59, 60, 63]. In the context of this thesis, this measure of storage requirements is the only efficiency measure that we are interested in. However, it should be noted that other efficiency measures (such as measures of computational requirements) are also considered in the literature [67].

1.4 KPS Constructions

The design and construction of "good" Key Predistribution Schemes can be approached in different ways. In all cases, every user in a privileged subset must be able to compute a common key associated with that subset, and any forbidden subset of users that is disjoint from the aforementioned privileged subset must not be able to obtain, or calculate between them, the key associated with that privileged subset.

Rather than expecting every user to store a key associated with each privileged subset that they belong to, we can instead give each user the means to calculate that key for themselves. In order to do this, each user will need a function and the necessary input values required for that function to calculate the secret keys. The storage requirements for this could easily be large, unless some of the predistributed information could be made publicly available. There are two ways in which to approach this:

1. The function is kept private and the input data for that function is made publicly available.

2. The function is made publicly available and the input data for that function is kept private.

We shall now consider an important family of key predistribution schemes for each of these two approaches. Following this, we also consider an application driven approach which has recently erupted in the literature.

1.4.1 Symmetric Polynomial Constructions

In 1982 Blom introduced a construction for $(2, w)$-KPSs based upon the use of *symmetric polynomials* [5, 6]. To describe Blom's scheme we must first suppose that $P_1, P_2, \ldots, P_n$ are users in a network N and that q is a prime number larger than n. To establish a $(2, w)$-KPS on N, (with $w \leq n-2$), Blom suggested the following protocol:

1. The TA randomly chooses a secret 2-variable, degree w *symmetric polynomial* $P(x, y)$ with coefficients over the finite field $GF(q)$.
   $\big($By symmetric we mean that $P(x, y) = P(y, x)$.$\big)$

2. Using secure communication channels, the TA distributes to each user P_i, the polynomial $f_i(x) = P(x, i)$, $\big($that is, the polynomial obtained by evaluating $P(x, y)$ at $y = i\big)$.

3. In order for the users P_{j_1} and P_{j_2} to establish a group key, user P_{j_1} evaluates $f_{j_1}(x)$ at $x = j_2$ and user P_{j_2} evaluates $f_{j_2}(x)$ at $x = j_1$.

4. Users P_{j_1} and P_{j_2} can then enable secure communications by using the group key given by $f_{j_1}(j_2) = P(j_2, j_1) = P(j_1, j_2) = f_{j_2}(j_1)$.

This protocol gives rise to an unconditionally secure $(2, w)$-KPS in the following restricted sense. The probability that any group of w colluders, $P_{j_1}, P_{j_2}, \ldots P_{j_w}$ can correctly guess the group key $P(i_1, i_2)$ of two users P_{i_1} and P_{i_2} $\big($where $\{P_{j_1}, P_{j_2}, \ldots P_{j_w}\} \cap \{P_{i_1}, P_{i_2}\} = \varnothing\big)$ is exactly $\big(1/q\big)$. That is, the colluders $P_{j_1}, P_{j_2}, \ldots P_{j_w}$ gain no extra advantage by pooling their knowledge of the polynomials $f_{j_1}, f_{j_2}, \ldots, f_{j_w}$. $\big($Recall that every user has a chance of $1/q$ of correctly guessing the value of any randomly chosen element of $GF(q)$ and hence of guessing any group key.$\big)$ Also note that under this scheme every user must hold (and keep private) $w+1$ elements of $GF(q)$ and the TA must privately store $\binom{w+2}{2}$ elements of $GF(q)$.

In 1992 Blundo *et al.* [8] generalised Blom's scheme to that of a (t, w)-KPS. As with Blom's scheme, we suppose that $P_1, P_2, \ldots, P_n$ are users in a network N and that q is a prime number larger than n. Then, to establish a (t, w)-KPS on N, (with $t + w \leq n$), Blundo *et al.* suggested the following modification of Blom's protocol:

1. The TA randomly chooses a secret t-variable, degree w *symmetric polynomial* $P(x_1, x_2, \ldots, x_t)$ with coefficients over the finite field $GF(q)$. $\big($By symmetric we mean that for any permutation π on $\{1, 2, \ldots n\}$, $P(x_1, x_2, \ldots, x_t) = P(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(t)})$.$\big)$

2. Using secure communication channels, the TA distributes to each user P_i, the polynomial $f_i(x_2, x_3, \ldots, x_t) = P(i, x_2, x_3, \ldots, x_t)$, $\big($that is, the polynomial obtained by evaluating $P(x_1, x_2, \ldots, x_t)$ at $x_1 = i\big)$.

3. In order for the users $P_{j_1}, P_{j_2}, \ldots, P_{j_t}$ to establish a group key, user P_{j_i} evaluates $f_{j_i}(x_2, x_3, \ldots x_t)$ at $(x_2, x_3, \ldots x_t) = (j_1, \ldots j_{i-1}, j_{i+1}, \ldots j_t)$.

4. Users $P_{j_1}, P_{j_2}, \ldots, P_{j_t}$ can then enable secure communications by using the group key given by $P(j_1, j_2, \ldots, j_t)$.

Blundo *et al.* [8] prove that this protocol gives rise to a (t, w)-KPS. Each group of w colluding users has only a one in q chance of correctly guessing a group key for any group of t users disjoint from those w colluding users. It is shown explicitly in [8], that every user in this scheme must hold (and keep private) $\binom{t+w-1}{t-1}$ elements of $GF(q)$ and the TA must privately store $\binom{t+w}{t}$ elements of $GF(q)$.

In the literature [65] it is shown that (under certain conditions) these symmetric polynomial schemes can be considered as examples of a wider family of *linear key predistribution schemes* which can be described in linear algebraic terms. Most importantly, it is shown in [8] that the user storage in these schemes is optimally small for any deterministic cardinality scheme with unconditional security. However, this optimally secure user storage comes at the cost of placing the burden of computation (the evaluation of a polynomial over very large finite fields) on each user.

1.4.2 The Key Ring Approach

In 1986 Jansen [39] introduced a key predistribution scheme with a storage reduction system based on the the use of *combinatorial keys*. As defined by Martin in [52], a secret key (used to enable secure communication between a subset of privileged users) is a *combinatorial key*, if it can be represented as a subset of the collective secret data held by the users in that privileged subset. In Jansen's scheme users are issued with sets of secret data, called *subkeys* and these subkeys are allocated based on the "divide and conquer" principle.

The network of users is divided into a number of subsets (all of the same size), those subsets are divided into smaller subsets etc, until $n-1$ partitions have been made, producing an n-level scheme. One set of subkeys is introduced for each level of the scheme, so in an n-level scheme, n sets of subkeys are required. In order to communicate securely, a pair of users must calculate a common key by applying a publicly known function to subkeys that they share.

In [39], Jansen demonstrates the advantage in storage capacity of his scheme. However, the common keys used by some pairs of users are also known to other individuals in that network. As such, Jansen's scheme can not be considered as a (2,1)-KPS. In [59], Mitchell and Piper noted that, "This can be seen as the cost of adopting an otherwise attractive scheme for reducing key storage requirements".

Mitchell and Piper [59, 60] refined and generalised Jansen's scheme to produce a family of (t, w) key predistribution schemes based on the use of *finite incidence structures* with special properties, called *key distribution patterns.* Within this family of schemes (presented in detail in Section 1.5) the key to be used by a privileged subset of users is made up from a combination of some of the subkeys held in common by those users. In [52] schemes of this sort are called *key ring predistribution schemes.*

A *key ring* is defined to be a set of public identifiers, (each of which is allocated at random to a unique subkey from a set of subkeys) and a collection of subsets of those identifiers. In order to use a key ring to establish a *key ring predistribution scheme* the TA must:

1. broadcast the set of subsets of identifiers (the key ring);
2. publicly allocate one subset of identifiers per user in the network;
3. distribute the subkeys to the users with the corresponding identifiers, using secure communication channels.

A privileged subset of users can communicate securely in such a scheme by first checking their public identifiers to see which secret subkeys they share in common. Then, each user in that privileged subset can calculate a common key by applying a publicly known function to the secret subkeys that they share. An immediate attribute of this system is that the subkeys could actually be physical keys (or smartcards) where several of these physical keys are required to open one set of locks in order to gain access to a restricted area.

Whether a key ring predistribution scheme offers unconditional security, or computational security, is determined by the public function used to combine the secret subkeys and calculate the common keys. Achieving unconditional security in such a scheme is relatively straightforward. It is simply required that the public function has the property that if a set of users can (between them) determine the secret key associated with a privileged subset, then they must also be able to deduce all of the common subkeys for that privileged subset. A simple example of such a function is the function that takes the common subkeys $x_1, x_2, \ldots, x_n$ (which we may assume are numbers) and returns the ordered string $(x_1; x_2; \ldots; x_n)$. This example is similar to an example given by Martin in [52].

Key ring predistribution schemes have been studied extensively and under different guises, consider for example [26, 32, 45, 84] and [85]. The user storage in these schemes is reduced, and key rings have been shown to produce some "good" KPSs, [60, 82, 85] and [73]. However, since the user storage in the symmetric polynomial schemes (given in Section 1.4.1) has already been shown to be optimally small, for any unconditionally secure cardinality scheme, we cannot better this. On the other hand, key ring predistribution schemes potentially offer more flexibility than symmetric polynomial schemes, since they are not restricted by algebraic structures.

1.4.3 KPSs for Wireless Sensor Networks

As we saw in Section 1.3.1, key predistribution schemes are the natural choice for key establishment within wireless sensor networks. Interest in the study of wireless sensor networks has grown dramatically over recent years. This growth has given rise to a new family of key predistribution schemes, designed specifically for use within wireless sensor networks. In all such schemes secret key information is installed in the nodes before they are distributed and secure communication is enabled where:

1. it is not necessary for every pair of nodes (or users) to have the ability to communicate securely;

2. it is sufficient for nodes to be able to communicate securely with some or all of their neighbouring nodes.

This secure communication is designed to achieve *connectivity* throughout the network. That is, to enable active nodes to relay data through other active nodes (where necessary), to the end points.

Research on the study of key predistribution schemes for wireless sensor networks began in earnest in 2002, with the seminal paper [31] by Eschenauer and Gligor. In this paper Eschenauer and Gligor proposed a randomised key ring predistribution scheme with computational security and "good" average connectivity of nodes. The existence of efficient schemes of this sort had previously been proven in [26], but the application of such schemes to wireless sensor networks was new.

The basic ideas proposed in [31] established a new avenue for key ring predistribution schemes. A standard model for the application of key ring predistribution schemes to wireless sensor networks has since been adopted [68]. In this model two nodes can communicate securely if and only if:

- the two nodes are within communication range of one another; and
- the two nodes share some subkeys uniquely in common.

Subsequent research on key ring predistribution schemes for wireless sensor networks has developed in three areas:

1. Eschenauer and Gligor's probabilistic scheme has been generalised, [19].
2. The use of deterministic schemes has been investigated, [13, 45, 88].
3. A combined approach using a key ring predistribution scheme along with another scheme (often a symmetric polynomial scheme) has been considered [22, 48, 50, 53, 88].

Of most interest to us are the deterministic schemes and the combination of these with symmetric polynomial schemes to produce a combined or *multiple space* key predistribution scheme. Within wireless sensor networks such schemes are normally applied in situations where the nodes are randomly distributed. That is, situations in which the geometry of the distribution of nodes cannot be predicted and/or taken into account.

Numerous deterministic schemes have been advocated, based upon various types of combinatorial structures. In order to get a feel for the variety of combinatorial structures used in the design of key predistribution schemes for wireless sensor networks, we mention a few of them here:

- projective geometry [13, 15, 18, 45];
- generalised quadrangles [13, 15];
- common intersection designs [44, 46, 48, 49];
- transversal designs [16, 17, 18, 44, 46, 48];
- spherical geometries [21];
- orthogonal arrays [20, 89];
- orthogonal latin squares [89];
- rational normal curves in projective space [69].

Other authors have analysed key predistribution schemes applied to wireless sensor networks where the nodes are not distributed randomly. Nodes may be distributed in groups, or in a grid (usually a square or hexagonal grid), giving extra deployment information that can be exploited in the KPS. Combinatorial structures, such as transversal designs and Costas arrays have been suggested for these specialised WSNs, [2, 3, 54, 76, 77].

The concept of combined key predistribution schemes has the benefit of producing a KPS with a mix of the inherent properties of the component schemes. As such, a symmetric polynomial scheme, with its optimal key storage, makes for an ideal component. (Symmetric polynomial schemes have also been considered individually for wireless sensor networks, see [53], but the computational cost involved in the polynomial evaluation required for key establishment is an issue.)

Combined schemes have been successfully constructed using a symmetric polynomial scheme (or a modified version thereof) as one component and a combinatorial structure of some sort as the other component [45, 48, 67] and [88]. Within wireless sensor networks, fast and efficient key computation is of benefit and the use of key ring predistribution schemes (with their combinatorial keys) potentially enables this. Therefore these combined schemes are able to exploit both the optimal key storage of the polynomial schemes and the efficient key computation of the key ring predistribution schemes.

The majority of research in this area is based upon KPSs with "good" overall connectivity. However, the flexibility of the key ring predistribution schemes (since they are not restricted to cardinality schemes) makes them applicable in situations where nodes are not distributed randomly. Therefore, we can consider $(\mathscr{G}, \mathscr{F})$-KPSs for more specified sets of privileged and forbidden subsets. This is just what we do, and we focus on the seminal family of key ring predistribution schemes defined by Mitchell and Piper [59] and [60], called *key distribution patterns.*

1.5 Key Distribution Patterns

A *key distribution pattern* or *KDP*, introduced by Mitchell and Piper [59] and [60] is a certain kind of *finite incidence structure* that can be used, as a key ring, to form a key ring predistribution scheme.

Definition 1.5.1. *An* ***incidence structure*** $\mathscr{K}$ *is a triple* $(\mathscr{P}, \mathscr{B}, \mathscr{I})$ *where* $\mathscr{P}$ *and* $\mathscr{B}$ *are sets and* $\mathscr{I} \subseteq \mathscr{P} \times \mathscr{B}$ *is a binary relation between them.*

An incidence structure is *finite* if both $\mathscr{P}$ and $\mathscr{B}$ are finite. The set $\mathscr{P}$ is called the *point set* and the elements of the point set are called *points*. In a similar way, the set $\mathscr{B}$ is called the *block set* and the elements of the block set are called *blocks*.

A point P is *incident with a block* x if, and only if, $(P, x) \in \mathscr{I}$. In the same way a block x is *incident with a point* P if, and only if, $(P, x) \in \mathscr{I}$. We shall often consider the set of all points incident with a block x, which we denote by (x), or the set of all blocks incident with a point P, which we denote by (P). Similarly, for any set of points X and any set of blocks Y, (X) and (Y) will denote the set of all blocks incident with any point in X and the set of all points incident with any block in Y, respectively.

Definition 1.5.2. *Let* $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ *be a finite incidence structure and let* $\mathscr{G}$ *and* $\mathscr{F}$ *be families of non-empty subsets of* $\mathscr{P}$*. Then* $\mathscr{K}$ *is called a* $\boldsymbol{(\mathscr{G}, \mathscr{F})}$***-Key Distribution Pattern*** *(or* $(\mathscr{G}, \mathscr{F})$*-KDP), if for all* $G \in \mathscr{G}$ *and* $F \in \mathscr{F}$ *such that* $G \cap F = \varnothing$,

$$\bigcap_{P \in G} (P) \nsubseteq \bigcup_{Q \in F} (Q).$$

As with our general model of a KPS, (Section 1.3.2) we call the members of $\mathscr{G}$ *privileged subsets* and the members of $\mathscr{F}$ *forbidden subsets.* Note that in [60], Mitchell and Piper defined KDPs in the setting of $(2,1)$-KPSs. Later, in the same paper, they extended this definition to the more general setting of (t, w)-KPSs, introducing the notion of (t, w)*-KDPs.* Several further generalisations, similar to the definition given here (Definition 1.5.2) have also been considered in the literature [65, 82, 84]. With no constraints on the privileged or forbidden subsets we will often refer to $(\mathscr{G}, \mathscr{F})$-KDPs (as we have defined them in Definition 1.5.2) as *generalised KDPs.*

In order to get a feel for this definition, we give an example. However, before we can set up our example, we require an observation concerning the representation of incidence structures.

Observation 1.5.3. *A non-empty finite incidence structure* $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$, *where* $\mathscr{P} = \{P_1, \ldots, P_v\}$ *and* $\mathscr{B} = \{x_1, \ldots, x_b\}$, *can be represented by a* $v \times b$ *binary matrix* $A = (a_{i,j})$, *defined as follows:*

$$a_{i,j} = \begin{cases} 1 & \textit{if } (P_i, x_j) \in \mathscr{I} \\ 0 & \textit{otherwise.} \end{cases}$$

Conversely, any binary matrix $A = (a_{i,j})$ can be used to represent a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$, simply by labelling the rows as points, $P_1, \ldots, P_v$ and the columns as blocks, $x_1, \ldots, x_b$. Then, $(P_i, x_j) \in \mathscr{I}$ if, and only if, $a_{i,j} = 1$. Now, let us consider the following example.

Example 1.5.1. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure represented by the following binary matrix.

$$\begin{array}{cccccc} & x_1 & x_2 & x_3 & x_4 & x_5 \\ P_1 & 1 & 0 & 1 & 1 & 1 \\ P_2 & 1 & 1 & 0 & 1 & 0 \\ P_3 & 0 & 1 & 1 & 1 & 0 \\ P_4 & 1 & 0 & 1 & 0 & 1 \\ P_5 & 1 & 1 & 0 & 0 & 1 \end{array}$$

Then, we can verify that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP for

$$\begin{aligned} \mathscr{G} = \big\{ & \{P_1, P_2, P_4, P_5\},\ \{P_2, P_3, P_5\},\ \{P_1, P_3, P_4\},\ \{P_1, P_2, P_3\},\ \{P_1, P_4, P_5\}, \\ & \{P_1, P_2\},\ \{P_1, P_3\},\ \{P_1, P_4\},\ \{P_2, P_3\},\ \{P_2, P_5\},\ \{P_1\},\ \{P_2\},\ \{P_3\},\ \{P_5\} \big\}. \end{aligned}$$

$$\mathscr{F} = \big\{ \{P_1\},\ \{P_2\},\ \{P_3\},\ \{P_4\},\ \{P_5\},\ \{P_1, P_4\},\ \{P_2, P_3\},\ \{P_2, P_5\},\ \{P_4, P_5\} \big\}.$$

In order to confirm that $\mathscr{K}$ is indeed a $(\mathscr{G}, \mathscr{F})$-KDP we must check each subset in $\mathscr{G}$ against every disjoint subset in $\mathscr{F}$. If we start with $\{P_1, P_2, P_4, P_5\} \in \mathscr{G}$ then we only need to consider $\{P_3\} \in \mathscr{F}$, since that is the only subset in $\mathscr{F}$ that is disjoint from $\{P_1, P_2, P_4, P_5\}$. Now, we must check that the blocks incident with all points P_1, P_2, P_4 and P_5 are not all incident with the point P_3 as well. It is clear from the matrix above that the points P_1, P_2, P_4 and P_5 are all incident with the block x_1 and that the point P_3 is not. Therefore, the subset $\{P_1, P_2, P_4, P_5\} \in \mathscr{G}$ is indeed privileged against our family of forbidden subsets $\mathscr{F}$. Next we can check that $\{P_2, P_3, P_5\} \in \mathscr{G}$ is privileged against the subsets $\{P_1\}, \{P_4\}$ and $\{P_1, P_4\} \in \mathscr{F}$, which are the only members of $\mathscr{F}$ that are disjoint from $\{P_2, P_3, P_5\}$. Continuing in this way we can easily verify that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP for $\mathscr{G}$ and $\mathscr{F}$ as given in this example.

To use a KDP, $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$, as a key ring (in a key ring predistribution scheme) we must first associate each point of $\mathscr{P}$ with a user from a network of users and each block of $\mathscr{B}$ with a subkey. The subkeys are distributed by the TA according to the KDP, (the user associated with the point P receives the subkey associated with the block x if, and only if, P is incident with x in the incident structure $\mathscr{K}$). The distribution of the subkeys amongst the users is broadcast publicly, (using inexpensive broadcast channels) with all the subkeys being represented using identifiers. However, the subkeys themselves are distributed using secure communication channels and remain private.

The key to be used by a privileged subset of users, G say, to enable secure communication within the subset, is calculated by combining all the subkeys held in common by all the members of G. In most cases this calculation is performed by using a publicly known one-way function. The public function will then yield a secret key for use by the subset G. None of the forbidden subsets of users that do not contain any members of G will be able to determine the secret key as, by Definition 1.5.2, the collusion of all users in any forbidden subset disjoint from G will not possess all the subkeys held in common by the users within G. This condition of security for privileged subsets against the collusion of any disjoint forbidden subset will be referred to throughout this thesis as the *security condition*.

1.5.1 Previous Work

Mitchell and Piper's 1988 paper [60] was the first to investigate key distribution patterns in any depth. They gave some simple examples of $(\mathscr{G}, \mathscr{F})$-KDPs and made use of previous research in the area of *design theory* in order to construct families of examples. Mitchell and Piper continued by giving some theoretical results on the lower bound of the number of blocks in a $(\mathscr{G}, \mathscr{F})$-KDP. They also analysed the security levels of $(\mathscr{G}, \mathscr{F})$-KDPs, particularly when using combinatorial structures. Finally, in [60], Mitchell and Piper proved that their results apply, not only to $(2, 1)$-KDPs, but also to (t, w)-KDPs.

Since then, key distribution patterns have, in one form or another, been investigated and analysed by many authors. As discussed in Section 3.4, some of these investigations have been completed under different names. Much of the recent research on key predistribution schemes for wireless sensor networks (Section 1.4.3) can be viewed as research on key distribution patterns. The numerous schemes listed in Section 1.4.3 are in fact examples of specific key distribution patterns with particular properties. In the literature as a whole, research on $(\mathscr{G}, \mathscr{F})$-KDPs has developed in two main areas, the construction of $(\mathscr{G}, \mathscr{F})$-KDPs, and the analysis of bounds on their efficiency measures (usually the number of blocks).

There are three known approaches when it comes to constructing $(\mathscr{G}, \mathscr{F})$-KDPs. The first approach was that used in 1988 by Mitchell and Piper and involves taking existing key distribution patterns and constructing new key distribution patterns from them. Mitchell and Piper were able to use this construction technique extensively in [60], where they presented several constructions for (t, w)-KDPs.

The second approach to $(\mathscr{G}, \mathscr{F})$-KDP constructions is to construct $(\mathscr{G}, \mathscr{F})$-KDPs directly from other mathematical objects. Several authors have used this approach and constructed $(\mathscr{G}, \mathscr{F})$-KDPs from combinatorial objects.

In 1993 and 1995 O'Keefe [62, 63, 64] used special finite geometric structures, (more specifically *circle geometries* and *Minkowski planes*) in order to construct (t, w)-KDPs. In 1994, Quinn [72] constructed (t, w)-KDPs from *conics* arising from finite *projective planes* and *affine planes*, and later, in 2004, Rinaldi [74] used *tangent circle structures* in the construction of (t, w)-KDPs. Also, Lee, Stinson and VanTrung, [47, 48, 82, 84] used *design theory*, *graph theory*, *orthogonal* and *perpendicular arrays* in order to construct specific $(\mathscr{G}, \mathscr{F})$-KDPs with particular properties.

The third approach to $(\mathscr{G}, \mathscr{F})$-KDP constructions uses probabilistic techniques. In 1995, Dyer *et al.* [26], used probabilistic methods [1, 10, 80], to give non-constructive existence results for (t, w)-KDPs. They gave constructions to show the existence of (t, w)-KDPs with a specified number of subkeys and devised a method of de-randomization. Also, in the same paper, Dyer *et al.* [26] used their probabilistic approach to find bounds on the number of subkeys in a system.

In 1994 [78], Ruszinkó used a combinatorial approach to give an upper bound for (t, w)-KDPs. In 1991 and 1999 [71, 73], Quinn presented several lower bounds for (t, w)-KDPs using combinatorics and *design theory.* In these papers, Quinn also introduced a technique for improving the efficiency of KDPs. She reduced the information content of the keys, by using an *information map.*

In a similar vein, in 1997 and 1998, Stinson *et al.* [82, 84] introduced a technique for improving the efficiency of $(\mathscr{G}, \mathscr{F})$-KDPs. This method was based on the use of *resilient functions* and allowed for a trade off between the level of security in a $(\mathscr{G}, \mathscr{F})$-KDP and the amount of key storage. Later, in 2000 and 2004, Stinson *et al.* [85, 86], used combinatorics and inductive arguments, to provide various new bounds for (t, w)-KDPs.

1.6 Overview

The aim of this thesis is to investigate generalised Key Distribution Patterns and study the mathematics behind them. There are two motivations for this.

The first motivation is simply the desire to lay bare the basic structure and intrinsic properties of key distribution patterns. It is hoped that by studying the mathematics of $(\mathscr{G}, \mathscr{F})$-KDPs, we will gain insight into the mathematical behaviour of (t, w)-KDPs.

The second motivation comes from potential applications. Suppose that we have a network of users, where a family of specified subsets of users $\mathscr{G}$, wishes to communicate securely without fear of other subsets of users $\mathscr{F}$, colluding together to eavesdrop on what is being said. In this general framework there are several situations that require a more general approach than that afforded by (t, w)-KDPs. For example, one or more of the following may occur:

1. $\mathscr{G}$ (and/or $\mathscr{F}$) may have many fewer members than the number of pairs of users in the network;

2. the sizes of the members of $\mathscr{G}$ (and/or $\mathscr{F}$) may vary considerably;

3. the cardinality of the largest member of $\mathscr{G}$ added to the cardinality of the largest member of $\mathscr{F}$ may be greater than the total number of users in the network;

4. $\mathscr{G}$ may have many members while $\mathscr{F}$ has very few members, or else, $\mathscr{F}$ may have many members while $\mathscr{G}$ has very few members.

All of these situations appear possible and can easily be modelled using generalised KDPs. However, the irregular nature of the members of $\mathscr{G}$ and $\mathscr{F}$ (in the above situations) rules out the use of cardinality schemes.

1.6.1 Thesis Structure

Chapter 1 and Chapter 2 contain the background material and prerequisite mathematics necessary for this thesis. No new research is presented in these chapters.

Chapter 3 explores some of the basic properties and special classes of $(\mathscr{G}, \mathscr{F})$-KDPs. Some of the immediate observations associated with $(\mathscr{G}, \mathscr{F})$-KDPs are presented in this chapter. Trivial schemes are investigated, by first exploring the concepts of *complete security* and *complete communication*. These concepts enable us to gain a benchmark for our later results on the efficiency of $(\mathscr{G}, \mathscr{F})$-KDPs (Chapter 6). The special properties of cardinality schemes are explored in Section 3.3. In Section 3.4 some related notions, introduced by other authors, are analysed and compared to the notion of a $(\mathscr{G}, \mathscr{F})$-KDP.

In Chapter 4 we consider a predefined incidence structure, $\mathscr{K}$, and investigate all possible sets of privileged and forbidden subsets for which $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP. In this way, we are able to study the concepts of redundancy and largest sets, within a $(\mathscr{G}, \mathscr{F})$-KDP. That is, we analyse the points and blocks that play no role in a $(\mathscr{G}, \mathscr{F})$-KDP and observe the trade-off between the size of the set of privileged subsets and the size of the set of forbidden subsets. This chapter broadens our overall understanding of $(\mathscr{G}, \mathscr{F})$-KDPs, however the concepts covered here are somewhat orthogonal to our other studies.

Chapter 5 contains constructions of $(\mathscr{G}, \mathscr{F})$-KDPs. Some well-known structures from design theory are applied to $(\mathscr{G}, \mathscr{F})$-KDPs in order to construct further $(\mathscr{G}, \mathscr{F})$-KDPs. For complement structures, a simple construction (Theorem 5.1.31) is presented. In Section 5.2, three constructions of Mitchell and Piper [60] are generalised and in Section 5.3 we introduce a new direct construction for $(\mathscr{G}, \mathscr{F})$-KDPs. This direct construction uses a discrete analogue of convexity in order to construct many different families of $(\mathscr{G}, \mathscr{F})$-KDPs.

In Chapter 6 some results from earlier chapters are applied to determine bounds on the number of blocks in a $(\mathscr{G}, \mathscr{F})$-KDP. Some results from the literature are generalised and new bounds, using new techniques, are presented. Without introducing any strong constraints on the privileged or forbidden subsets, some informative results are discovered. However, it is the introduction of constraints, such as the constraint that the set of privileged subsets forms a Sperner system, that opens the door to many stronger bounds for $(\mathscr{G}, \mathscr{F})$-KDPs. In Section 6.3 the notions of internal and external structures are generalised and some new bounds are presented.

Chapter 7 summarises this thesis, highlights areas of future study and lists some related open problems. Finally, Appendix A gives the proof of Theorem 6.2.5, which is not included in the main body of the thesis, since it would obfuscate the main purpose of Chapter 6.

The main contributions of this thesis are:

1. The characterisations of when an incidence structure is a $(\mathscr{G}, \mathscr{F})$-KDP in terms of its internal structures, (Theorem 5.1.12) and its external structures, (Theorem 5.1.25). These results go beyond those achieved by Mitchell and Piper in [60]. In fact, in Theorem 5.1.25 we correct an error in [60, Lemma 3.4].

2. A direct construction that uses finite convex structures in order to construct a family of $(\mathscr{G}, \mathscr{F})$-KDPs, (Theorem 5.3.7). For this construction we are able to precisely calculate $|\mathscr{G}|$, $|\mathscr{F}|$ and the block size. This construction seems to be relatively efficient in terms of the number of blocks required for its construction, see Example 6.1.1.

3. New lower bounds on the number of blocks required for general $(\mathscr{G}, \mathscr{F})$-KDPs , (Theorem 6.1.4 and Theorem 6.1.8). These lower bounds do not require the privileged subsets to form a Sperner system.

4. A combinatorial inequality, (Theorem 6.2.5, proved in Appendix A), which is used in conjunction with other results in this thesis in order to prove a lower bound on the number of blocks required for a specific $(\mathscr{G}, \mathscr{F})$-KDP, Corollary 6.2.6.

5. A lower bound on the number of blocks required in a $(\mathscr{G}, \mathscr{F})$-KDP, under the additional assumption that the set of privileged subsets forms a Sperner system, (Theorem 6.2.9).

Chapter 2

Mathematical Preliminaries

In this chapter we present some prerequisite mathematics necessary for this thesis.

2.1 Incidence Structures and Designs

The most important notion for our study of key distribution patterns is that of an incidence structure, see Definition 1.5.1. When appropriate to do so, we will denote the number of points in the point set of an incidence structure by v and the number of blocks in the block set by b.

In most of our considerations of incidence structures, we will want to avoid the situation where two distinct points are incident with the same set of blocks. Therefore, it is convenient for us to introduce the following definition.

Definition 2.1.1. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. We define an equivalence relation $\mathcal{R}$ on the set of points $\mathscr{P}$ by $(P, Q) \in \mathcal{R}$ if, and only if, $(P) = (Q)$ and we let $[P]$ represent the $\mathcal{R}$-equivalence class of P. Then we say that P is a* ***repeated point*** *if $\big|[P]\big| > 1$.*

Similarly, we usually want to avoid the situation where two distinct blocks are incident with the same set of points.

Definition 2.1.2. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. We define an equivalence relation $\mathcal{R}$ on the set of blocks $\mathscr{B}$ by $(x, y) \in \mathcal{R}$ if, and* *only if, $(x) = (y)$ and we let $[x]$ represent the $\mathcal{R}$-equivalence class of x. Then we say that x is a* ***repeated block*** *if $\big|[x]\big| > 1$.*

Given any finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ there is a natural partial ordering on the point set $\mathscr{P}$.

Definition 2.1.3. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure without repeated points, then define a partial order "$\leq$" on $\mathscr{P}$ by $P \leq Q$ if, and only if, $(P) \subseteq (Q)$. We say that a point $P \in \mathscr{P}$ is the* ***largest element*** *of $\mathscr{P}$ if $Q \leq P$ for all $Q \in \mathscr{P}$. In the same way we say that a point $P \in \mathscr{P}$ is the* ***smallest element*** *of $\mathscr{P}$ if $P \leq Q$ for all $Q \in \mathscr{P}$.*

Designs are perhaps the most important class of incidence structures. These structures are used widely in many areas of mathematics.

Definition 2.1.4. *We define a* $\boldsymbol{t}$***-$\boldsymbol{(v, k, \lambda)}$ design*** *to be a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ with v points and without repeated blocks, such that:*
(i) every block is incident with exactly k points; and
(ii) every set of t points is incident with exactly λ common blocks. That is, for all $T \subseteq \mathscr{P}$ such that $|T| = t$, $\big|\bigcap_{P \in T}(P)\big| = \lambda$.

The following result is a generalisation of Fisher's inequality [33]. Fisher's inequality has been proved in a variety of different and ingenious ways [37, 66, 79]. The proof given here (taken from [11]) uses linear algebra and is particularly elegant and concise.

Result 2.1.5. (Fisher's Inequality) Let $\mathscr{A}$ be a finite set of cardinality n and let $A_1, A_2, \ldots, A_m$ be m non-empty subsets of $\mathscr{A}$. If $|A_i \cap A_j| = \lambda$ for all $i \neq j$ then $n \geq m$. In particular, if $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a t-(v, k, λ) design with $t \geq 2$, then $|\mathscr{B}| \geq |\mathscr{P}|$.

Proof. The result is clearly true if $\lambda = 0$, so we shall assume that $\lambda > 0$. If $|A_i| = \lambda$ for some i, then $A_i \subsetneqq A_j$ for all $j \neq i$. That is, $\{A_j \setminus A_i : i \neq j\}$

is a collection of $m-1$ non-empty pair-wise disjoint subsets of $\mathscr{A} \setminus A_i$. So, $m-1 \leq n-\lambda$ implying that $m \leq n+1-\lambda \leq n$. Therefore, we may assume that $a_i = |A_i| > \lambda$ for all i.

Let $\boldsymbol{v}_i = (v_{i1}, v_{i2}, \ldots, v_{in}) \in \mathbb{R}^n$ be the indicator vector of the set A_i then,

$$v_{i,j} = \begin{cases} 1 & \text{if } j \in A_i \\ 0 & \text{otherwise.} \end{cases}$$

Then, $\boldsymbol{v}_i \cdot \boldsymbol{v}_i = |A_i| = a_i > \lambda$ and $\boldsymbol{v}_i \cdot \boldsymbol{v}_j = |A_i \cap A_j| = \lambda$ for all $i \neq j$. We shall show that $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots \boldsymbol{v}_m\}$ is linearly independent and thus $m \leq n$. To this end, let $\displaystyle\sum_{i=1}^{m} c_i \boldsymbol{v}_i = 0$.

Now, by taking the dot product of both sides with $\boldsymbol{v}_j$, we get the following:

$$0 = \sum_{i=1}^{m} c_i(\boldsymbol{v}_i \cdot \boldsymbol{v}_j) = \sum_{\substack{i=1 \\ i \neq j}}^{m} c_i(\boldsymbol{v}_i \cdot \boldsymbol{v}_j) + c_j(\boldsymbol{v}_j \cdot \boldsymbol{v}_j) = \lambda \sum_{i=1}^{m} c_i + (a_j - \lambda)c_j.$$

Now, let $\displaystyle\sum_{i=1}^{m} c_i = \mathcal{F}$ and hence $0 = \lambda\mathcal{F} + (a_j - \lambda)c_j \Longrightarrow c_j = \dfrac{\lambda}{\lambda - a_j}\mathcal{F}$. So,

$$\mathcal{F} = \sum_{j=1}^{m} c_j = \mathcal{F} \sum_{j=1}^{m} \frac{\lambda}{\lambda - a_j} \text{ and since } a_j > \lambda \text{ we know that } \sum_{j=1}^{m} \frac{\lambda}{\lambda - a_j} < 0.$$

Therefore, $\mathcal{F} = 0$ and thus $c_j = 0$ for all j. Hence $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots \boldsymbol{v}_m\}$ is linearly independent and so $n \geq m$. □

2.1.1 Homomorphisms and Isomorphisms

Sometimes in this thesis we will need to compare similar incidence structures. The appropriate way of doing this is via a homomorphism.

Definition 2.1.6. *If $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ and $\mathscr{K}' = (\mathscr{P}', \mathscr{B}', \mathscr{I}')$ are two incidence structures, then we say that a pair of mappings $\varphi : \mathscr{P} \to \mathscr{P}'$ and $\psi : \mathscr{B} \to \mathscr{B}'$ form a **homomorphism** from $\mathscr{K}$ to $\mathscr{K}'$ provided that $(P, x) \in \mathscr{I}$ if and only if $(\varphi(P), \psi(x)) \in \mathscr{I}'$ for all $(P, x) \in \mathscr{P} \times \mathscr{B}$.*

An important special case of a homomorphism is the following.

Definition 2.1.7. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ and $\mathscr{K}' = (\mathscr{P}', \mathscr{B}', \mathscr{I}')$ be two incidence structures. If a pair of mappings $\varphi : \mathscr{P} \to \mathscr{P}'$ and $\psi : \mathscr{B} \to \mathscr{B}'$ form a homomorphism from $\mathscr{K}$ to $\mathscr{K}'$ and are both bijective, then we say that φ and ψ form an* ***isomorphism*** *from $\mathscr{K}$ to $\mathscr{K}'$. In this case we say that $\mathscr{K}$ and $\mathscr{K}'$ are* ***isomorphic****.*

Throughout this thesis we will not distinguish between isomorphic incidence structures, that is, we shall consider them to be equivalent. Next, we give a representation of incidence structures in terms of points and sets of points. We call this point representation of an incidence structure our *standard representation.*

Definition 2.1.8. *The* ***standard representation*** *of an incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is defined to be $\mathscr{K}^S = (\mathscr{P}^S, \mathscr{B}^S, \mathscr{I}^S)$, where $\mathscr{P}^S = \mathscr{P}$, $\mathscr{B}^S = \{(x) : x \in \mathscr{B}\}$ and $\mathscr{I}^S$ is defined by $(P, X) \in \mathscr{I}^S$ if, and only if, $P \in X$.*

Our interest in the standard representation of an incidence structure stems from the following observation.

Observation 2.1.9. *For any incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ and its standard representation $\mathscr{K}^S = (\mathscr{P}^S, \mathscr{B}^S, \mathscr{I}^S)$, the pair of mappings $\varphi : \mathscr{P} \to \mathscr{P}^S$ and $\psi : \mathscr{B} \to \mathscr{B}^S$ defined by $\varphi(P) = P$ and $\psi(x) = (x)$ form a homomorphism from $\mathscr{K}$ to $\mathscr{K}^S$.*

Proof. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be an incidence structure, $\mathscr{K}^S = (\mathscr{P}^S, \mathscr{B}^S, \mathscr{I}^S)$ be the standard representation of $\mathscr{K}$, and φ and ψ be the pair of mappings as defined in the statement of this observation.
Consider $(P, x) \in \mathscr{P} \times \mathscr{B}$, then

$$\begin{aligned} (P, x) \in \mathscr{I} &\iff P \in (x) \\ &\iff \varphi(P) \in \psi(x) \\ &\iff (\varphi(P), \psi(x)) \in \mathscr{I}^S. \end{aligned}$$

That is, φ and ψ form a homomorphism from $\mathscr{K}$ to $\mathscr{K}^S$. □

An interesting special case of Observation 2.1.9 is given next.

Corollary 2.1.10. *Every incidence structure without repeated blocks is isomorphic to its standard representation.*

Proof. This is a special case of Observation 2.1.9. Clearly, without repeated blocks the mappings φ and ψ are 1-to-1 and onto. □

We next define a representation for incidence structures that is essentially the dual of our standard representation (Definition 2.1.8).

Definition 2.1.11. *The* ***block representation*** *of an incidence structure* $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ *is given by* $\mathscr{K}^B = (\mathscr{P}^B, \mathscr{B}^B, \mathscr{I}^B)$, *where* $\mathscr{P}^B = \{(Q) : Q \in \mathscr{P}\}$, $\mathscr{B}^B = \mathscr{B}$ *and* $\mathscr{I}^B$ *is defined by* $(P, x) \in \mathscr{I}^B$ *if, and only if,* $x \in P$.

As is the case with the standard representation, our interest in the block representation of an incidence structure emanates from the following observation.

Observation 2.1.12. *For any incidence structure* $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ *and its block representation* $\mathscr{K}^B = (\mathscr{P}^B, \mathscr{B}^B, \mathscr{I}^B)$, *the pair of mappings* $\varphi : \mathscr{P} \to \mathscr{P}^B$ *and* $\psi : \mathscr{B} \to \mathscr{B}^B$ *defined by* $\varphi(P) = (P)$ *and* $\psi(x) = x$ *form a homomorphism from* $\mathscr{K}$ *to* $\mathscr{K}^B$.

Proof. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be an incidence structure, $\mathscr{K}^B = (\mathscr{P}^B, \mathscr{B}^B, \mathscr{I}^B)$ be the block representation of $\mathscr{K}$, and φ and ψ be the pair of mappings as defined in the statement of this observation.
Consider $(P, x) \in \mathscr{P} \times \mathscr{B}$, then

$$\begin{aligned} (P, x) \in \mathscr{I} &\iff x \in (P) \\ &\iff \psi(x) \in \varphi(P) \\ &\iff (\varphi(P), \psi(x)) \in \mathscr{I}^B. \end{aligned}$$

That is, φ and ψ form a homomorphism from $\mathscr{K}$ to $\mathscr{K}^B$. □

In the important special case of an incidence structure without repeated points we get the following canonical result.

Corollary 2.1.13. *Every incidence structure without repeated points is isomorphic to its block representation.*

Proof. This is a special case of Observation 2.1.12. Clearly, without repeated points the mappings φ and ψ are 1-to-1 and onto. □

A more detailed introduction to incidence structures and design theory is given in [38].

2.2 Set Theory and Sperner Systems

We now consider some basic set operations.

Definition 2.2.1. *Let X be a set and let A, B be subsets of X. Then we define the* **symmetric difference** *of A and B, denoted by Δ, to be*

$$A\Delta B = A\backslash B \ \cup \ B\backslash A.$$

Note that $(2^X, \Delta)$ is an Abelian group. Next, we recall the notions of union and intersection over arbitrary index sets.

Definition 2.2.2. *Suppose that A, B and X are sets. If $\{S_b : b \in B\} \subseteq 2^X$ and $\varnothing \neq A \subseteq B$ then,*

$$\bigcup_{a \in A} S_a = \{x \in X : x \in S_a \textit{ for some } a \in A\} \quad \textit{and}$$

$$\bigcap_{a \in A} S_a = \{x \in X : x \in S_a \textit{ for all } a \in A\}.$$

In the case when $A = \varnothing$, $\displaystyle\bigcup_{a \in A} S_a = \varnothing$ and $\displaystyle\bigcap_{a \in A} S_a = X$.

When studying partially ordered sets, it is natural to consider totally ordered subsets of them (namely *chains*).

Definition 2.2.3. *Given a set X, we call any $\mathcal{C} \subseteq 2^X$ a* ***chain*** *in $(2^X, \subseteq)$ if for any $A, B \in \mathcal{C}$, either $A \subseteq B$ or $B \subseteq A$.*

In some circumstances it is also natural to consider the opposite of a chain, i.e. an *anti-chain* or a *Sperner system.*

Definition 2.2.4. *Given a set X, we call any $\mathcal{A} \subseteq 2^X$ an* ***anti-chain*** *in $(2^X, \subseteq)$ (or alternatively, a* ***Sperner system*** *over X) if for any $B, C \in \mathcal{A}$, if $B \subseteq C$ then $B = C$.*

In [81] (1928), Sperner proved the following theorem (Result 2.2.5) which now bears his name. The proof that we present here is based upon a simple proof of Sperner's Theorem due to Lubell [51]. Similar, but ultimately less straightforward proofs may also be found in [9, 11, 57, 58, 90]. Our proof relies on the fact that for $1 \leq j \leq n$ we know that $j!(n-j)! \geq \lfloor n/2 \rfloor!(n - \lfloor n/2 \rfloor)!$, which follows from the fact that $\binom{n}{j} \leq \binom{n}{\lfloor n/2 \rfloor}$ for all $1 \leq j \leq n$.

Result 2.2.5. (Sperner's Theorem) A Sperner system $\mathcal{S}$ on a set X where $|X| = n$ consists of at most $\binom{n}{\lfloor n/2 \rfloor}$ sets.

Proof. Let Σ denote the set of all bijections from $\{1, 2, ..., n\}$ onto X, then $|\Sigma| = n!$. Next we define a relation $\mathcal{R} \subseteq \Sigma \times \mathcal{S}$ by $(\pi, S) \in \mathcal{R}$ if, and only if, $S = \{\pi(1), \pi(2), \ldots, \pi(j)\}$ for some $1 \leq j \leq n$. Then we let $D = \{\pi \in \Sigma : (\pi, S) \in \mathcal{R}$ for some $S \in \mathcal{S}\}$. Since $\mathcal{S}$ forms a Sperner system, for each $\pi \in \Sigma$ there is at most one $S \in \mathcal{S}$ such that $(\pi, S) \in \mathcal{R}$, hence we can define a function $f : D \to \mathcal{S}$ by $f(\pi) = S$ if, and only if, $(\pi, S) \in \mathcal{R}$. Now, $\{f^{-1}(S) : S \in \mathcal{S}\}$ forms a partition of D and by a simple counting argument we see that $|f^{-1}(S)| = |S|!(n - |S|)!$ for each $S \in \mathcal{S}$. Therefore,

$$\begin{aligned} n! \;\geq\; |D| \;&=\; \Big| \bigcup_{S \in \mathcal{S}} f^{-1}(S) \Big| \;=\; \sum_{S \in \mathcal{S}} |f^{-1}(S)| \;=\; \sum_{S \in \mathcal{S}} |S|!(n - |S|)! \\ &\geq\; \sum_{S \in \mathcal{S}} \lfloor n/2 \rfloor!(n - \lfloor n/2 \rfloor)! \;=\; |\mathcal{S}| \lfloor n/2 \rfloor!(n - \lfloor n/2 \rfloor)! \end{aligned}$$

and hence, $|\mathcal{S}| \;\leq\; \dfrac{n!}{\lfloor n/2 \rfloor!(n - \lfloor n/2 \rfloor)!} \;=\; \dbinom{n}{\lfloor n/2 \rfloor}$. □

As a corollary to Sperner's Theorem we have the following result (also due to Sperner, [81]), which will be used later, in Theorem 6.2.7.

Result 2.2.6. *Let $\mathcal{S}$ be a Sperner system on a set X where $|X| = n$. If $|S| \leq t \leq n/2$ for all $S \in \mathcal{S}$ then,*

$$|\mathcal{S}| \leq \left|\{T \in 2^X : |T| = t \textit{ and } S \subseteq T \textit{ for some } S \in \mathcal{S}\}\right|.$$

Proof. Let $A = \{T \in 2^X : |T| = t \text{ and } S \subseteq T \text{ for some } S \in \mathcal{S}\}$ and let $B = \{(x_1, x_2, \ldots, x_t) \in X^t : \{x_1, x_2, \ldots, x_t\} \in A\}$, then $|B| = |A|t!$. As in Sperner's theorem, let Σ denote the set of all bijections from $\{1, 2, ..., n\}$ onto X and let $D = \{\pi \in \Sigma : (\pi, S) \in \mathcal{R} \text{ for some } S \in \mathcal{S}\}$.

Then define $g : D \to B$ by $g(\pi) = (\pi(1), \pi(2), \ldots, \pi(t))$. Note that g is well-defined because of the definition of D and the fact that $|S| \leq t$ for all $S \in \mathcal{S}$. Now, for each $(x_1, x_2, \ldots, x_t) \in g(D)$, $|g^{-1}((x_1, x_2, \ldots, x_t))| = (n-t)!$.

Therefore, $|D| = |g(D)|(n-t)! \leq |B|(n-t)!$ and hence $|D|/t!(n-t)! \leq |A|$. However, from the proof of Sperner's theorem $|D| = \sum_{S \in \mathcal{S}} |S|!(n - |S|)!$ and so,

$$|A| \geq \frac{|D|}{t!(n-t)!} = \sum_{S \in \mathcal{S}} \frac{|S|!(n-|S|)!}{t!(n-t)!} \geq \sum_{S \in \mathcal{S}} 1 = |\mathcal{S}|. \qquad \square$$

In Section 6.2, we use the following well-known inequality in order to exploit Sperner's Theorem.

Result 2.2.7. *For all $n \in \mathbb{N}$, $2^{n-1} \geq \binom{n}{\lfloor n/2 \rfloor}$.*

Proof. Let $P(n)$ be the statement "$2^{n-1} \geq \binom{n}{\lfloor n/2 \rfloor}$", then $P(1)$ is obviously true.

Now suppose that $P(k)$ is true, then

$$2^{(k+1)-1} = 2^k = 2(2^{k-1}) \geq 2\binom{k}{\lfloor k/2 \rfloor} \geq \frac{k+1}{\lfloor \frac{k+1}{2} \rfloor \lceil \frac{k+1}{2} \rceil}\binom{k}{\lfloor k/2 \rfloor} = \binom{k+1}{\lfloor \frac{k+1}{2} \rfloor}.$$

Therefore, by induction, $2^{n-1} \geq \binom{n}{\lfloor n/2 \rfloor}$, for all positive integers n. $\square$

We can make better use of Sperner's theorem if we obtain a better bound on $\binom{n}{\lfloor n/2 \rfloor}$ than $2^{n-1} \geq \binom{n}{\lfloor n/2 \rfloor}$. The following result from Stromberg [87] allows us to do just that.

Result 2.2.8. [87, page 256] *For all $n \in \mathbb{N}$ with $n \geq 2$, we have*

$$\exp\left(\frac{-1}{6n}\right) \;<\; \binom{2n}{n} 2^{-2n}\sqrt{\pi n} \;<\; \exp\left(\frac{-1}{12n+1}\right).$$

We can now give an improved bound on $\binom{n}{\lfloor n/2 \rfloor}$, which appears to be new.

Corollary 2.2.9. *For all $n \in \mathbb{N}$ with $n \geq 4$, we have*

$$\binom{n}{\lfloor n/2 \rfloor} < \frac{2^n}{\sqrt{(\frac{\pi n}{2})}}.$$

Proof. We consider two cases, even n and odd n.

For even n, (and $n \geq 4$), $\binom{n}{\lfloor n/2 \rfloor} < \frac{2^n}{\sqrt{(\frac{\pi n}{2})}}$ follows from Result 2.2.8 since $\exp\left(\frac{-1}{12(n/2)+1}\right) < 1$.

For odd n, (and $n \geq 5$), $\binom{n}{\lfloor n/2 \rfloor} = \binom{2r+1}{r}$ for $r = \lfloor n/2 \rfloor$.
Therefore,

$$\binom{2r+1}{r} = \left[\binom{2r+1}{r} \Big/ \binom{2r}{r}\right] \binom{2r}{r} = \frac{2r+1}{r+1}\binom{2r}{r} < \frac{2r+1}{r+1}\frac{2^{2r}}{\sqrt{\pi r}}.$$

Now,

$$\frac{2^{2r}}{\sqrt{\pi r}}\frac{2r+1}{r+1} \leq \frac{2^{2r+1}}{\sqrt{\pi(r+\frac{1}{2})}} \iff \frac{2r+1}{\sqrt{r}(r+1)} \leq \frac{2}{\sqrt{r+\frac{1}{2}}}$$

$$\iff (4r^2+4r+1)(2r+1) \leq 8r(r^2+2r+1) \iff 1 \leq 4r^2+2r$$

which is clearly true for all $r \in \mathbb{N}$.
Therefore, for all $n \in \mathbb{N}$ with $n \geq 4$, $\binom{n}{\lfloor n/2 \rfloor} < \frac{2^n}{\sqrt{(\frac{\pi n}{2})}}$. □

We note that, for all $n \geq 4$, the bound from Corollary 2.2.9 is strictly better than the bound from Result 2.2.7.

Chapter 3

Initial Observations

In this chapter we explore some of the basic properties and special classes of $(\mathscr{G}, \mathscr{F})$-KDPs. We begin by presenting some simple observations that offer insight into the mathematics of $(\mathscr{G}, \mathscr{F})$-KDPs.

In Section 3.2 we investigate *trivial* $(\mathscr{G}, \mathscr{F})$*-KDPs*. To this end, we first explore the concept of *complete security*, where all members of each privileged subset of users can communicate securely against any disjoint set of colluding attackers. Then, we explore the converse concept of *complete communication*, where no colluding forbidden subset of users is able to eavesdrop on any secure communication taking place between any disjoint subset of users. These concepts have both been explored by other authors, so we relate this work to our own and clarify some terminology.

In Section 3.3, we consider $(\mathscr{G}, \mathscr{F})$-KDPs with cardinality constraints on the privileged and/or forbidden subsets. We explore some of the basic properties of these cardinality schemes and investigate extreme cases that give rise to *trivial* $(\mathscr{G}, \mathscr{F})$*-KDPs*. We complete Section 3.3 by presenting a 1-to-1 relationship for $(\mathscr{G}, \mathscr{F})$-KDPs (used later in Chapter 6) that applies to certain cardinality schemes.

Finally, in Section 3.4, we present some related definitions from the literature and clarify their exact relationship to $(\mathscr{G}, \mathscr{F})$-KDPs.

In summary, the main purpose of this chapter, is simply to establish some of the basic properties of $(\mathscr{G}, \mathscr{F})$-KDPs and answer some of the obvious questions. The main concepts that we cover are:

1. *Trivial $(\mathscr{G}, \mathscr{F})$-KDPs* - We characterise *complete communication* and *complete security*, exhaustively investigating both concepts.

2. Cardinality schemes - We give an analysis of $(\mathscr{G}, \mathscr{F})$-KDPs with cardinality constraints on the privileged and/or forbidden subsets.

3. Related definitions - We relate $(\mathscr{G}, \mathscr{F})$-KDPs to other areas of research such as *Cover Free Families* and *Intersection Schemes.*

By covering these concepts and establishing the basic properties of $(\mathscr{G}, \mathscr{F})$-KDPs, we are laying the ground work for the rest of this thesis.

3.1 Basic Properties

We begin this section by reiterating our definition of a $(\mathscr{G}, \mathscr{F})$-KDP (Definition 1.5.2).

Definition 3.1.1. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{G}$ and $\mathscr{F}$ be families of non-empty subsets of $\mathscr{P}$. Then $\mathscr{K}$ is called a* ***$(\mathscr{G}, \mathscr{F})$-Key Distribution Pattern*** *(or $(\mathscr{G}, \mathscr{F})$-KDP), if for all $G \in \mathscr{G}$ and $F \in \mathscr{F}$ such that $G \cap F = \varnothing$,*

$$\bigcap_{P \in G} (P) \not\subseteq \bigcup_{Q \in F} (Q).$$

As can be seen from Definition 3.1.1, there are situations in which the security condition will be satisfied vacuously. For example, we allow for the possibility that:

- there are no disjoint privileged and forbidden subsets;

- the family of privileged subsets $\mathscr{G}$ is empty;

- the family of forbidden subsets $\mathscr{F}$ is empty.

In each of these cases the security condition is satisfied vacuously. We note that since it is possible for the security condition to be satisfied vacuously, it is also possible that the users in a privileged subset have no subkeys in common, yet still satisfy Definition 3.1.1. We also allow for privileged subsets of cardinality one, that is, we allow for the seemingly meaningless situation where a user can set up secure communication with himself. Practically speaking, the absence of cardinality constraints and other assumptions in Definition 3.1.1 lead to some "small" $(\mathscr{G}, \mathscr{F})$-KDPs. Whilst these "small" $(\mathscr{G}, \mathscr{F})$-KDPs are of limited practical use, keeping Definition 3.1.1 very general permits flexibility and reveals essential properties when proving theorems throughout this thesis. In practice however, we will tend to impose constraints such as:

- the families of privileged and forbidden subsets must be of a certain size;
- at least one privileged subset must be disjoint from at least one forbidden subset; and
- the network itself must contain a minimum number of users.

We now make a simple observation directly from Definition 3.1.1.

Observation 3.1.2. *Any finite incidence structure is a $(\mathscr{G}, \mathscr{F})$-KDP for some $\mathscr{G}$ and some $\mathscr{F}$.*

Proof. For any finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$, if we let $\mathscr{G} = \varnothing$, then $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP for any $\mathscr{F}$ and if we let $\mathscr{F} = \varnothing$, then $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP for any $\mathscr{G}$. Less trivially, if $\mathscr{I} \neq \varnothing$, we can set $\mathscr{G} = \{(x) : x \in \mathscr{B} \text{ and } (x) \neq \varnothing\}$ and $\mathscr{F} = 2^{\mathscr{P}} \setminus \{\varnothing\}$. Then, $\mathscr{K}$ is again a $(\mathscr{G}, \mathscr{F})$-KDP. Such a $(\mathscr{G}, \mathscr{F})$-KDP will later be called a *trivial $\mathscr{G}$-KDP*, see Definition 3.2.4. □

We now consider a simple proposition demonstrating that a $(\mathscr{G}, \mathscr{F})$-KDP is also a KDP for any smaller collection of sets.

Proposition 3.1.3. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then $\mathscr{K}$ is a $(\mathscr{G}', \mathscr{F}')$-KDP for any $\mathscr{G}' \subseteq \mathscr{G}$ and any $\mathscr{F}' \subseteq \mathscr{F}$.*

Proof. The proof of this proposition follows directly from Definition 3.1.1. $\square$

Another observation that follows immediately from Definition 3.1.1 is that, in some sense, $(\mathscr{G}, \mathscr{F})$-KDPs are stable under the union operation. We first consider the union of privileged subsets.

Proposition 3.1.4. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is both a $(\mathscr{G}, \mathscr{F})$-KDP and a $(\mathscr{G}', \mathscr{F})$-KDP, then $\mathscr{K}$ is also a $(\mathscr{G} \cup \mathscr{G}', \mathscr{F})$-KDP.*

We now consider the union of forbidden subsets in the same way.

Proposition 3.1.5. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is both a $(\mathscr{G}, \mathscr{F})$-KDP and a $(\mathscr{G}, \mathscr{F}')$-KDP, then $\mathscr{K}$ is also a $(\mathscr{G}, \mathscr{F} \cup \mathscr{F}')$-KDP.*

Although Proposition 3.1.3 shows that, in one sense, being a $(\mathscr{G}, \mathscr{F})$-KDP is a hereditary property, our next example demonstrates that in another sense it is not. Specifically, it may be the case that for some $G' \subseteq G \in \mathscr{G}$ there exists an $F \in \mathscr{F}$ disjoint from G' such that $\bigcap_{P \in G'}(P) \subseteq \bigcup_{Q \in F}(Q)$ and similarly, it may be the case that for some $F' \subseteq F \in \mathscr{F}$ there exists a $G \in \mathscr{G}$ disjoint from F' such that $\bigcap_{P \in G}(P) \subseteq \bigcup_{Q \in F'}(Q)$. Essentially, this is because G' may be disjoint from an F that no $G \in \mathscr{G}$ is disjoint from, and similarly F' may be disjoint from a G that no $F \in \mathscr{F}$ is disjoint from.

Example 3.1.1. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure represented by the following binary matrix.

$$\begin{array}{ccccc}
 & x_1 & x_2 & x_3 & x_4 \\
P_1 & 1 & 0 & 1 & 1 \\
P_2 & 1 & 1 & 1 & 0 \\
P_3 & 0 & 1 & 1 & 1 \\
P_4 & 0 & 1 & 0 & 0 \\
P_5 & 1 & 0 & 0 & 1
\end{array}$$

Then, $\mathscr{K}$ is a $(\mathscr{G},\mathscr{F})$-KDP for $\mathscr{G} = \big\{\{P_1,P_2,P_5\}, \{P_2,P_3,P_4\}, \{P_1,P_2,P_3\}, \{P_1,P_3,P_5\}, \{P_1,P_2\}, \{P_1,P_3\}, \{P_1,P_5\}, \{P_2,P_3\}, \{P_1\}, \{P_2\}, \{P_3\}, \{P_4\}\big\}$ and $\mathscr{F} = \big\{\{P_1\}, \{P_4\}, \{P_5\}, \{P_1,P_3\}, \{P_1,P_5\}, \{P_2,P_4\}, \{P_3,P_4\}, \{P_4,P_5\}\big\}$.

We note that $\{P_1,P_3,P_5\} \in \mathscr{G}$ and $\{P_3,P_5\} \subseteq \{P_1,P_3,P_5\}$. However, $\mathscr{K}$ is not a $(\mathscr{G}',\mathscr{F})$-KDP for $\mathscr{G}' = \mathscr{G} \cup \{P_3,P_5\}$ since $(P_3) \cap (P_5) \subseteq (P_1), \{P_1\} \in \mathscr{F}$ and $\{P_3,P_5\} \cap \{P_1\} = \varnothing$. We also note that $\{P_2,P_4\} \in \mathscr{F}$ and $\{P_2\} \subseteq \{P_2,P_4\}$. However, $\mathscr{K}$ is not a $(\mathscr{G},\mathscr{F}')$-KDP for $\mathscr{F}' = \mathscr{F} \cup \{P_2\}$ since $(P_4) \subseteq (P_2), \{P_4\} \in \mathscr{G}$ and $\{P_4\} \cap \{P_2\} = \varnothing$.

The final basic concept that we cover in this section is that of removing users from a KDP. There are many practical reasons why users may be removed from a system, so the motivation for this is clear. When users are removed from a $(\mathscr{G},\mathscr{F})$-KDP it is natural to consider the remaining users and the associated $(\mathscr{G}',\mathscr{F}')$-KDP. In terms of incidence structures this corresponds to deleting points from the incidence structure, as shown in the following proposition.

Proposition 3.1.6. *If a finite incidence structure* $\mathscr{K} = (\mathscr{P},\mathscr{B},\mathscr{I})$ *is a* $(\mathscr{G},\mathscr{F})$*-KDP and* $D \subseteq \mathscr{P}$*, then* $\mathscr{K}' = (\mathscr{P}',\mathscr{B}',\mathscr{I}')$*, where:*

$$\mathscr{P}' = \mathscr{P} \setminus D, \;\; \mathscr{B}' = \mathscr{B} \;\; \textit{and}$$
$$\mathscr{I}' \textit{ is defined by } (P,x) \in \mathscr{I}' \textit{ if, and only if, } (P,x) \in \mathscr{I},$$

$$\textit{is a } (\mathscr{G}',\mathscr{F}')\textit{-KDP, for}$$
$$\mathscr{G}' = \{G \setminus D : G \in \mathscr{G} \textit{ and } G \setminus D \neq \varnothing\} \textit{ and } \mathscr{F}' = \{F \in \mathscr{F} : F \cap D = \varnothing\}.$$

Proof. Let $\mathscr{K} = (\mathscr{P},\mathscr{B},\mathscr{I})$ be a $(\mathscr{G},\mathscr{F})$-KDP and suppose, in order to obtain a contradiction, that $\mathscr{K}' = (\mathscr{P}',\mathscr{B}',\mathscr{I}')$ is not a $(\mathscr{G}',\mathscr{F}')$-KDP. Then, there exists a $G' \in \mathscr{G}'$ and an $F' \in \mathscr{F}' \subseteq \mathscr{F}$ such that $G' \cap F' = \varnothing$ and $\bigcap_{P' \in G'}(P') \subseteq \bigcup_{Q' \in F'}(Q')$. Now, by definition there exists a $G \in \mathscr{G}$ such that $G' = G \setminus D$. Then, $\bigcap_{P \in G}(P) \subseteq \bigcap_{P' \in G'}(P') \subseteq \bigcup_{Q' \in F'}(Q')$. Also, since $F' \cap D = \varnothing$, we know that $G \cap F' = \varnothing$. Therefore, $\mathscr{K}$ is not a $(\mathscr{G},\mathscr{F})$-KDP and we have a contradiction. □

In Chapter 4, we consider further ways in which an incidence structure is a $(\mathscr{G},\mathscr{F})$-KDP for several different families of privileged and forbidden subsets. In particular, in Section 4.2 we look at the largest possible families of privileged and forbidden subsets that make a given incidence structure a $(\mathscr{G},\mathscr{F})$-KDP. We also consider the trade-off between the size of the family of privileged subsets relative to the size of the family of forbidden subsets.

3.2 Trivial $(\mathscr{G},\mathscr{F})$-KDPs

Up to this point we have not considered the problem of how to assign subkeys in order to obtain a $(\mathscr{G},\mathscr{F})$-KDP for a previously specified family of privileged and forbidden subsets. We now consider two fundamental methods of achieving this. One of these cases is when a given family of privileged subsets of users can communicate securely against any collection of colluders, while the other is the case in which any family of users may communicate safely against a given family of forbidden subsets of colluders. Both cases will be used throughout this thesis as a benchmark for all other $(\mathscr{G},\mathscr{F})$-KDPs.

3.2.1 Complete Security

We begin by defining the basic concept.

Definition 3.2.1. *Let $\mathscr{K}=(\mathscr{P},\mathscr{B},\mathscr{I})$ be a finite incidence structure and let $\mathscr{G}$ be a family of non-empty subsets of $\mathscr{P}$. Then, $\mathscr{G}$ is said to be* ***completely secure*** *with respect to $\mathscr{K}$ if for every $G\in\mathscr{G}$, $\bigcap_{P\in G}(P)\not\subseteq\bigcup_{Q\in\mathscr{P}\setminus G}(Q)$.*

When the context is clear we shall simply say that $\mathscr{G}$ is *completely secure* and if $\mathscr{K}$ is a $(\mathscr{G},\mathscr{F})$-KDP where $\mathscr{G}$ is completely secure, then we may informally refer to $\mathscr{K}$ as a *completely secure $(\mathscr{G},\mathscr{F})$-KDP*.

By observing that if $\bigcap_{P\in G}(P)\not\subseteq\bigcup_{Q\in\mathscr{P}\setminus G}(Q)$ then $\bigcap_{P\in G}(P)\not\subseteq\bigcup_{Q\in F}(Q)$ for any $\varnothing\neq F\subseteq\mathscr{P}\setminus G$, we see that $\mathscr{G}$ is completely secure if, and only if, for each $G \in \mathscr{G}$ and each $F \in 2^{\mathscr{P}} \setminus \{\varnothing\}$, such that $G \cap F = \varnothing$,

$$\bigcap_{P \in G} (P) \not\subseteq \bigcup_{Q \in F} (Q).$$

Therefore, if $\mathscr{G}$ is completely secure, then $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP for $\mathscr{F} = 2^{\mathscr{P}} \setminus \{\varnothing\}$ and conversely, if $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP for any $\mathscr{F}$ that contains $\big\{\mathscr{P} \setminus G : G \in \mathscr{G} \setminus \{\mathscr{P}\}\big\}$, then $\mathscr{G}$ is completely secure.

More informally, for a $(\mathscr{G}, \mathscr{F})$-KDP, if all members of each privileged subset of users can communicate securely against any colluders disjoint from that subset, then we have a completely secure $(\mathscr{G}, \mathscr{F})$-KDP.

We now consider a completely secure $(\mathscr{G}, \mathscr{F})$-KDP that can be specified for any incidence structure.

Observation 3.2.2. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{G} = \{(x) : x \in \mathscr{B}$ and $(x) \neq \varnothing\}$. Then $\mathscr{G}$ is completely secure.*

Proof. Suppose that $\mathscr{G}$ is not completely secure. Then there exists a $G \in \mathscr{G}$ such that $\bigcap_{P \in G}(P) \subseteq \bigcup_{Q \in \mathscr{P} \setminus G}(Q)$. Now, $G = (x)$ for some $x \in \mathscr{B}$, so $x \in \bigcap_{P \in G}(P) \subseteq \bigcup_{Q \in \mathscr{P} \setminus G}(Q)$. Therefore, there exists a $Q \in \mathscr{P} \setminus G$ such that $x \in (Q)$, or equivalently $Q \in (x) = G$. Hence, $Q \in G \cap [\mathscr{P} \setminus G] = \varnothing$ and we have a contradiction. □

So, for any incidence structure, we have a method of constructing a completely secure $(\mathscr{G}, \mathscr{F})$-KDP and, conversely, we have the following remark.

Remark 3.2.3. For any specified family of privileged subsets of users $\mathscr{G}$ on a set $\mathscr{P}$, we can construct an incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$, where $\mathscr{P}$ is the set of all users, $\mathscr{B} = \mathscr{G}$ and $\mathscr{I}$ is defined by $(P, X) \in \mathscr{I}$ if, and only if, $P \in X$ for $P \in \mathscr{P}$ and $X \in \mathscr{B}$. Then, our set of privileged subsets of users $\mathscr{G}$ is completely secure with respect to $\mathscr{K}$.

Definition 3.2.4. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{G}$ be a family of non-empty subsets of $\mathscr{P}$. Then, $\mathscr{K}$ is called a **trivial $\mathscr{G}$-KDP** if $\mathscr{G} \subseteq \{(x) : x \in \mathscr{B}$ and $(x) \neq \varnothing\}$.*

Alternatively, and more traditionally, we can define a trivial $\mathscr{G}$-KDP by indexing both the blocks and the privileged subsets. If $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a finite incidence structure and $\mathscr{G}$ is a family of non-empty subsets of $\mathscr{P}$, where $\mathscr{B} = \{x_1, \ldots, x_b\}$ and $\mathscr{G} = \{G_i : i \in J \subseteq \{1, \ldots, b\}\}$, then $\mathscr{K}$ is a *trivial $\mathscr{G}$-KDP* if for each $i \in J$, $(P, x_i) \in \mathscr{I}$ if, and only if, $P \in G_i$. That is, a user P holds a subkey x_i for any $i \in J \subseteq \{1, 2, \ldots, b\}$ if, and only if, the user P is a member of the corresponding privileged subset G_i.

For any trivial $\mathscr{G}$-KDP, every member of each privileged subset of users holds a subkey that is unique to that subset. In this case, the total number of privileged subsets can be at most equal to the number of blocks in the incidence structure.

We also know from Observation 3.2.2 that a trivial $\mathscr{G}$-KDP is a $(\mathscr{G}, \mathscr{F})$-KDP for any $\mathscr{F} \subseteq 2^{\mathscr{P}} \setminus \{\varnothing\}$.

We have already established that a trivial $\mathscr{G}$-KDP is completely secure, but we have still to consider the converse.

Theorem 3.2.5. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. If $\mathscr{G}$ is a completely secure family of non-empty subsets of $\mathscr{P}$ and $\mathscr{P} \notin \mathscr{G}$, then $\mathscr{K}$ is a trivial $\mathscr{G}$-KDP.*

Proof. Suppose that $\mathscr{G}$ is completely secure, $\mathscr{P} \notin \mathscr{G}$ but $\mathscr{K}$ is not a trivial $\mathscr{G}$-KDP. Then there exists a $G \in \mathscr{G}$ such that $G \neq (x)$ for any $x \in \mathscr{B}$, and in particular $G \neq (x)$ for $x \in \bigcap_{P \in G}(P)$. Now, $\bigcap_{P \in G}(P) \neq \varnothing$, since $\bigcap_{P \in G}(P) \nsubseteq \bigcup_{Q \in \mathscr{P} \setminus G}(Q)$. Also, $G \subseteq (x)$ for every $x \in \bigcap_{P \in G}(P) = \{x_1, \ldots, x_n\}$, so G is a proper subset of (x) for any $x \in \bigcap_{P \in G}(P)$. For each $1 \leq i \leq n$, choose $P_i \in (x_i) \setminus G$ and let $F = \{P_i : 1 \leq i \leq n\}$. Note that $G \cap F = \varnothing$ and $x_i \in (P_i)$ for each $1 \leq i \leq n$. Then,

$$\bigcap_{P \in G}(P) = \{x_1, \ldots, x_n\} \subseteq (P_1) \cup \cdots \cup (P_n) = \bigcup_{Q \in F}(Q) \subseteq \bigcup_{Q \in \mathscr{P} \setminus G}(Q),$$

and we have a contradiction. □

The problem of complete security is now totally understood and there is nothing more for us to investigate. However, later in this thesis we will be able to refer to and use complete security in order to aid our understanding of $(\mathscr{G}, \mathscr{F})$-KDPs.

3.2.2 Complete Communication

Again, we begin this subsection with a definition.

Definition 3.2.6. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{F}$ be a family of non-empty subsets of $\mathscr{P}$. Then, $\mathscr{F}$ is said to permit* ***complete communication*** *with respect to $\mathscr{K}$ if for every $F \in \mathscr{F}$, $\bigcap_{P\in\mathscr{P}\setminus F}(P) \not\subseteq \bigcup_{Q\in F}(Q)$.*

When the context is clear we shall simply say that $\mathscr{F}$ permits *complete communication* and, if $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP where $\mathscr{F}$ permits complete communication, then we may informally refer to $\mathscr{K}$ as a $(\mathscr{G}, \mathscr{F})$*-KDP with complete communication.*

By observing that if $\bigcap_{P\in\mathscr{P}\setminus F}(P) \not\subseteq \bigcup_{Q\in F}(Q)$ then $\bigcap_{P\in G}(P) \not\subseteq \bigcup_{Q\in F}(Q)$ for any $\varnothing \neq G \subseteq \mathscr{P} \setminus F$, we see that $\mathscr{F}$ permits complete communication if, and only if, for each $F \in \mathscr{F}$ and each $G \in 2^{\mathscr{P}} \setminus \{\varnothing\}$, such that $G \cap F = \varnothing$,

$$\bigcap_{P\in G}(P) \not\subseteq \bigcup_{Q\in F}(Q).$$

Therefore, if $\mathscr{F}$ permits complete communication, then we have a $(\mathscr{G}, \mathscr{F})$-KDP for $\mathscr{G} = 2^{\mathscr{P}} \setminus \{\varnothing\}$ and conversely, if we have a $(\mathscr{G}, \mathscr{F})$-KDP for any $\mathscr{G}$ that contains $\{\mathscr{P} \setminus F : F \in \mathscr{F} \setminus \{\mathscr{P}\}\}$, then $\mathscr{F}$ permits complete communication.

More informally, for a $(\mathscr{G}, \mathscr{F})$-KDP, if no colluding forbidden subset of users is able to eavesdrop on any secure communication taking place between any outside subset of users, then we have a $(\mathscr{G}, \mathscr{F})$-KDP with complete communication.

We now consider a $(\mathscr{G}, \mathscr{F})$-KDP with complete communication that can be specified for any incidence structure.

Observation 3.2.7. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{F} = \{\mathscr{P} \setminus (x) : x \in \mathscr{B}$ and $(x) \neq \mathscr{P}\}$. Then $\mathscr{F}$ permits complete communication.*

Proof. Suppose that $\mathscr{F}$ does not permit complete communication. Then there exists an $F \in \mathscr{F}$ such that $\bigcap_{P \in \mathscr{P} \setminus F}(P) \subseteq \bigcup_{Q \in \mathscr{F}}(Q)$. Now, $F = \mathscr{P} \setminus (x)$ for some $x \in \mathscr{B}$, so $x \notin \bigcup_{Q \in F}(Q)$. On the other hand $[\mathscr{P} \setminus F] \cap F = \varnothing$ and so $\mathscr{P} \setminus F \subseteq (x)$. Hence, $x \in \bigcap_{P \in \mathscr{P} \setminus F}(P) \subseteq \bigcup_{Q \in \mathscr{F}}(Q)$, but $x \notin \bigcup_{Q \in F}(Q)$, and so we have a contradiction. □

So, for any incidence structure, we have a method of constructing a $(\mathscr{G}, \mathscr{F})$-KDP with complete communication. Conversely, for any specified family of forbidden subsets of users, $\mathscr{F}$, we can construct an incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$, where $\mathscr{P}$ is the set of all users, $\mathscr{B} = \{\mathscr{P} \setminus F,$ for all $F \in \mathscr{F}\}$ and $\mathscr{I}$ is defined by $(P, X) \in \mathscr{I}$ if, and only if, $P \in X$ for $P \in \mathscr{P}$ and $X \in \mathscr{B}$. Then, $\mathscr{F}$ permits complete communication with respect to $\mathscr{K}$.

Definition 3.2.8. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{F}$ be a family of non-empty subsets of $\mathscr{P}$. Then, $\mathscr{K}$ is called a* ***cotrivial $\mathscr{F}$-KDP*** *if $\mathscr{F} \subseteq \{\mathscr{P} \setminus (x) : x \in \mathscr{B}$ and $(x) \neq \mathscr{P}\}$.*

As with trivial $\mathscr{G}$-KDPs, we can give an alternative definition for cotrivial $\mathscr{F}$-KDPs by indexing the blocks and the forbidden subsets. If $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a finite incidence structure and $\mathscr{F}$ is a family of non-empty subsets of $\mathscr{P}$ where $\mathscr{B} = \{x_1, \ldots, x_b\}$ and $\mathscr{F} = \{F_i : i \in J \subseteq \{1, \ldots, b\}\}$, then $\mathscr{K}$ is a *cotrivial $\mathscr{F}$-KDP* if for each $i \in J$, $(P, x_i) \in \mathscr{I}$ if, and only if, $P \notin G_i$. That is, a user P holds a subkey x_i for any $i \in J \subseteq \{1, 2, \ldots, b\}$ if, and only if, user P is not a member of the corresponding forbidden subset F_i.

We know from Observation 3.2.7 that a cotrivial $\mathscr{F}$-KDP is a $(\mathscr{G}, \mathscr{F})$-KDP for any $\mathscr{G} \subseteq 2^{\mathscr{P}} \setminus \{\varnothing\}$.

For any cotrivial $\mathscr{F}$-KDP, every forbidden subset of users does not hold between them a subkey that every other user disjoint from that forbidden subset holds. So, all subsets of users disjoint from forbidden subsets can use the subkeys not held by those forbidden subsets in order to enable secure communication. That is, for cotrivial $\mathscr{F}$-KDPs all subsets of users are able to communicate securely against all disjoint forbidden subsets of users. In a similar way as for trivial $\mathscr{G}$-KDPs, the total number of forbidden subsets is at most equal to the number of blocks in the incidence structure.

Since we have already established that a cotrivial $\mathscr{F}$-KDP permits complete communication, we now show the converse.

Theorem 3.2.9. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. If $\mathscr{F}$ is a family of non-empty subsets of $\mathscr{P}$ that permits complete communication and $\mathscr{P} \notin \mathscr{F}$, then $\mathscr{K}$ is a cotrivial $\mathscr{F}$-KDP.*

Proof. Suppose that $\mathscr{F}$ permits complete communication, $\mathscr{P} \notin \mathscr{F}$, but $\mathscr{K}$ is not a cotrivial $\mathscr{F}$-KDP. Then there exists an $F \in \mathscr{F}$ such that $F \neq \mathscr{P} \setminus (x)$ for any $x \in \mathscr{B}$, and in particular $F \neq \mathscr{P} \setminus (x)$ for $x \in \mathscr{B} \setminus \bigcup_{Q \in F}(Q)$. Now, $\bigcup_{Q\in F}(Q) \neq \mathscr{B}$, since $\bigcap_{P \in \mathscr{P}\setminus F}(P) \not\subseteq \bigcup_{Q\in F}(Q)$ and $\mathscr{P} \setminus F = \varnothing$. Also, $F \subseteq \mathscr{P} \setminus (x)$ for every $x \in \mathscr{B} \setminus \bigcup_{Q\in F}(Q) = \{x_1, \ldots, x_n\}$, so F is a proper subset of $\mathscr{P} \setminus (x)$ for any $x \in \mathscr{B} \setminus \bigcup_{Q \in F}(Q)$. For each $1 \leq i \leq n$,choose $P_i \in [\mathscr{P} \setminus (x_i)] \setminus F$, then let $G = \{P_i : 1 \leq i \leq n\}$. Note that $G \cap F = \varnothing$ and $x_i \notin (P_i)$ for each $1 \leq i \leq n$. Therefore, $\{x_1, \ldots, x_n\} \cap \bigcap_{1 \leq i \leq n}(P_i) = \varnothing$, so

$$\bigcap_{P \in \mathscr{P} \setminus F}(P) \subseteq \bigcap_{P \in G}(P) = \bigcap_{1 \leq i \leq n}(P_i) \subseteq \mathscr{B} \setminus \{x_1, \ldots, x_n\} = \bigcup_{Q \in F}(Q),$$

and we have a contradiction. □

The problem of complete communication is now totally understood and there is nothing more for us to investigate. However, as with complete security, we will later be able to refer to and use complete communication to aid our understanding of $(\mathscr{G}, \mathscr{F})$-KDPs.

3.2.3 Terminology and Relationships

The notions of trivial $\mathscr{G}$-KDPs and cotrivial $\mathscr{F}$-KDPs were alternatively defined by Martin [52] as *Trivial Inclusion KDPs* and *Trivial Exclusion KDPs* respectively. Trivial $\mathscr{G}$-KDPs were first introduced as a special case of $(2,1)$-KDPs in [60] and cotrivial $\mathscr{F}$-KDPs were first introduced in [32] in the special case where the set of forbidden subsets consists of all users of size at most w.

We say that a $(\mathscr{G},\mathscr{F})$-KDP is *non-trivial* if it is neither a trivial $\mathscr{G}$-KDP nor a cotrivial $\mathscr{F}$-KDP. Later, in Section 5.1.3 we introduce the complement of a $(\mathscr{G},\mathscr{F})$-KDP. In fact, Theorem 5.1.31 shows that the complement of a trivial $\mathscr{G}$-KDP is a cotrivial $\mathscr{F}$-KDP and the complement of a cotrivial $\mathscr{F}$-KDP is a trivial $\mathscr{G}$-KDP. Due to the fact that both trivial cases usually result in large numbers of subkeys, more efficient, and therefore more interesting, $(\mathscr{G},\mathscr{F})$-KDPs occur somewhere between these two extremes. To this end, we use trivial $\mathscr{G}$-KDPs and cotrivial $\mathscr{F}$-KDPs as a benchmark for measuring the levels of security, communication and efficiency of other $(\mathscr{G},\mathscr{F})$-KDPs.

3.3 Special Classes of $(\mathscr{G},\mathscr{F})$-KDPs

Historically, cardinality constraints have been used to specify special classes of KDPs. We begin by considering the situation where each subset of users of size at most t wishes to communicate securely against all colluding subsets of users of size at most w.

Definition 3.3.1. *A finite incidence structure $\mathscr{K}=(\mathscr{P},\mathscr{B},\mathscr{I})$ is said to be a* $\boldsymbol{(t,w)}$***-KDP*** *for $t\geq 1$ and $w\geq 1$ if $\mathscr{K}$ is a $(\mathscr{G},\mathscr{F})$-KDP for,*

$$\mathscr{G}=\{G\in 2^{\mathscr{P}}:1\leq |G|\leq t\} \text{ and } \mathscr{F}=\{F\in 2^{\mathscr{P}}:1\leq |F|\leq w\}.$$

The first KDPs introduced by Mitchell and Piper in [59] were $(2,1)$-KDPs. These KDPs enable every pair of users to communicate securely against any individual eavesdropper. Also in [59], and in more detail in [60], they considered the concept of *w security*, as introduced by Blom in [5]. A $(2, w)$-KDP (or *w-secure KDP*) enables every pair of users to communicate securely against any other w colluding users.

Whilst investigating further developments in [60], Mitchell and Piper introduced (t, w)-KDPs. Since their introduction, (t, w)-KDPs have been investigated and analysed by many authors in a variety of different ways. *Design theory*, *finite geometry*, *orthogonal arrays*, *projective planes* and *graph theory* are among some of the techniques used in [47, 63, 64, 72, 74, 82, 84] to construct (t, w)-KDPs. The combinatorial nature and cardinality constraints of (t, w)-KDPs have enabled extensive analysis.

Under certain circumstances results for (t, w)-KDPs give rise to results for $(\mathscr{G}, \mathscr{F})$-KDPs. This is demonstrated in the following remark.

Remark 3.3.2. If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a (t, w)-KDP where $t + w \leq |\mathscr{P}|$, then $\mathscr{K}$ is also a $(\mathscr{G}, \mathscr{F})$-KDP for any $\mathscr{G}$ and $\mathscr{F}$ such that $\max\{|G| : G \in \mathscr{G}\} \leq t$ and $\max\{|F| : F \in \mathscr{F}\} \leq w$.

We can further generalise (t, w)-KDPs to $(t, \mathscr{F})$-KDPs and $(\mathscr{G}, w)$-KDPs, the definitions of which follow in a natural way from Definition 3.1.1 and Definition 3.3.1. Also, we say that a trivial $\mathscr{G}$-KDP where $\mathscr{G} = \{G \in 2^{\mathscr{P}} : 1 \leq |G| \leq t\}$ is a *trivial t-KDP* and a cotrivial $\mathscr{F}$-KDP where $\mathscr{F} = \{F \in 2^{\mathscr{P}} : 1 \leq |F| \leq w\}$ is a *cotrivial w-KDP*. Therefore, a $(t, \mathscr{F})$-KDP with complete security is a trivial t-KDP and a $(\mathscr{G}, w)$-KDP with complete communication is a cotrivial w-KDP.

3.3.1 Extreme Cases

In this subsection we deal with some extreme cases of (t, w)-KDPs. These extreme cases are essentially (t, w)-KDPs with cardinality constraints that give rise to trivial $\mathscr{G}$-KDPs or cotrivial $\mathscr{F}$-KDPs.

We firstly consider (t, w)-KDPs where $t + w \geq |\mathscr{P}|$.

Proposition 3.3.3. *Let a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a (t, w)-KDP such that $t < |\mathscr{P}|$ and $t + w \geq |\mathscr{P}|$. Then, for every $G \in 2^{\mathscr{P}}$ such that $|\mathscr{P}| - w \leq |G| \leq t$, $G = (x)$ for some $x \in \mathscr{B}$. That is, $\mathscr{K}$ is a trivial $\mathscr{G}$-KDP for $\mathscr{G} = \{G \in 2^{\mathscr{P}} : |\mathscr{P}| - w \leq |G| \leq t\}$.*

Proof. For every $G \in \mathscr{G}$, $\bigcap_{P \in G}(P) \not\subseteq \bigcup_{Q \in \mathscr{P} \setminus G}(Q)$ since $|\mathscr{P} \setminus G| = |\mathscr{P}| - |G| \leq w$. So, by Definition 3.2.1, $\mathscr{G}$ is completely secure and hence by Theorem 3.2.5, $\mathscr{K}$ is a trivial $\mathscr{G}$-KDP. □

In a similar way to Proposition 3.3.3 we can consider a cotrivial result.

Proposition 3.3.4. *Let a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a (t, w)-KDP such that $w < |\mathscr{P}|$ and $t + w \geq |\mathscr{P}|$. Then, for every $F \in 2^{\mathscr{P}}$ such that $|\mathscr{P}| - t \leq |F| \leq w$, $F = \mathscr{P} \setminus (x)$ for some $x \in \mathscr{B}$. That is, $\mathscr{K}$ is a cotrivial $\mathscr{F}$-KDP for $\mathscr{F} = \{F \in 2^{\mathscr{P}} : |\mathscr{P}| - t \leq |F| \leq w\}$.*

Proof. For every $F \in \mathscr{F}$, $\bigcap_{P \in \mathscr{P} \setminus F}(P) \not\subseteq \bigcup_{Q \in F}(Q)$ since $|\mathscr{P} \setminus F| = |\mathscr{P}| - |F| \leq t$. So, by Definition 3.2.6, $\mathscr{F}$ permits complete communication and hence by Theorem 3.2.9, $\mathscr{K}$ is a cotrivial $\mathscr{F}$-KDP. □

It is interesting to note from Proposition 3.3.3 and Proposition 3.3.4 that if $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a finite incidence structure and $\mathscr{K}$ is a (t, w)-KDP where $t < |\mathscr{P}|, w < |\mathscr{P}|$ and $t + w \geq |\mathscr{P}|$, then $\mathscr{K}$ is both a trivial $\mathscr{G}$-KDP for $\mathscr{G} = \{G \in 2^{\mathscr{P}} : |\mathscr{P}| - w \leq |G| \leq t\}$ and a cotrivial $\mathscr{F}$-KDP for $\mathscr{F} = \{F \in 2^{\mathscr{P}} : |\mathscr{P}| - t \leq |F| \leq w\}$.

Next we consider $(\mathscr{G}, w)$-KDPs where $w \geq |\mathscr{B}|$.

Proposition 3.3.5. *Let a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a $(\mathscr{G}, w)$-KDP. If $w \geq |\mathscr{B}|$, then $\mathscr{K}$ is a trivial $\mathscr{G}$-KDP.*

Proof. Suppose that $\mathscr{K}$ is a $(\mathscr{G}, w)$-KDP for some $w \geq |\mathscr{B}|$. By Theorem 3.2.5 it is sufficient to show that for any $G \in \mathscr{G}$, $\bigcap_{P \in G}(P) \not\subseteq \bigcup_{Q \in \mathscr{P} \setminus G}(Q)$. Suppose, in order to obtain a contradiction, that there exists a $G \in \mathscr{G}$ such that $\bigcap_{P\in G}(P) \subseteq \bigcup_{Q\in\mathscr{P}\setminus G}(Q)$. Then, for each $x \in \bigcap_{P\in G}(P)$, there exists a $Q \in \mathscr{P}\setminus G$ such that $x \in (Q)$. Since $\left|\bigcap_{P\in G}(P)\right| \leq |\mathscr{B}|$, $\bigcap_{P\in G}(P) \subseteq \bigcup_{Q\in F}(Q)$ for some $F \in 2^{\mathscr{P}}$ such that $1 \leq |F| \leq |\mathscr{B}| \leq w$. Therefore, $\mathscr{K}$ is not a $(\mathscr{G}, w)$-KDP and we have a contradiction. □

In a similar way to Proposition 3.3.5, we will now consider $(t, \mathscr{F})$-KDPs where $t \geq |\mathscr{B}|$.

Proposition 3.3.6. *Let a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a $(t, \mathscr{F})$-KDP. If $t \geq |\mathscr{B}|$, then $\mathscr{K}$ is a cotrivial $\mathscr{F}$-KDP.*

Proof. Suppose that $\mathscr{K}$ is a $(t, \mathscr{F})$-KDP for some $t \geq |\mathscr{B}|$. By Theorem 3.2.9 it is sufficient to show that for any $F \in \mathscr{F}$, $\bigcap_{P\in\mathscr{P}\setminus F}(P) \not\subseteq \bigcup_{Q\in F}(Q)$. Suppose, in order to obtain a contradiction, that there exists an $F \in \mathscr{F}$ such that $\bigcap_{P\in\mathscr{P}\setminus F}(P) \subseteq \bigcup_{Q\in F}(Q)$. Then, for each $x \in \mathscr{B} \setminus \bigcup_{Q\in F}(Q)$, there exists a $P \in \mathscr{P} \setminus F$ such that $x \notin (P)$. Since $\left|\mathscr{B} \setminus \bigcup_{Q\in F}(Q)\right| \leq |\mathscr{B}|$, $\bigcap_{P\in G}(P) \subseteq \bigcup_{Q\in F}(Q)$ for some $G \in 2^{\mathscr{P}}$ such that $1 \leq |G| \leq |\mathscr{B}| \leq t$. Therefore, $\mathscr{K}$ is not a $(t, \mathscr{F})$-KDP and we have a contradiction. □

The following observation yields a simple lower bound on the number of blocks in a (t, w)-KDP that follows immediately from some of our earlier propositions.

Observation 3.3.7. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a (t, w)-KDP where $t + w \leq |\mathscr{P}|$, then $|\mathscr{B}| \geq \binom{w+t}{t}$.*

Proof. Suppose that $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a (t, w)-KDP where $t + w \leq |\mathscr{P}|$. Then, for some $0 \leq d \leq |\mathscr{P}| - 2$, we know that $t + w = |\mathscr{P}| - d$. From Proposition 3.1.6 we can remove d points from the point set and create an incidence structure $\mathscr{K}' = (\mathscr{P}', \mathscr{B}', \mathscr{I}')$ where $|\mathscr{P}'| = |\mathscr{P}| - d$ and $\mathscr{B}' = \mathscr{B}$ such that $\mathscr{K}'$ is a (t, w)-KDP. Since $t + w = |\mathscr{P}'| = |\mathscr{P}| - d$, it follows from Proposition 3.3.3 that $\mathscr{K}'$ is a trivial $\mathscr{G}$-KDP where $\mathscr{G} = \{G \in 2^{\mathscr{P}'} : |G| = t\}$.

By Definition 3.2.4, we know that $|\mathscr{G}| \leq |\mathscr{B}|$. Now,

$$|\mathscr{G}| = \binom{|\mathscr{P}'|}{t} = \binom{|\mathscr{P}| - d}{t} = \binom{w+t}{t}.$$

Therefore, $|\mathscr{B}| \geq \binom{w+t}{t}$ and the proof is complete. □

Using this observation it is easy to see how rapidly the number of blocks in a (t, w)-KDP grows with respect to t and w. For example, any $(3, 3)$-KDP on 6 or more points requires at least 20 blocks, any $(4, 4)$-KDP on 8 or more points requires at least 70 blocks and any $(5, 5)$-KDP on 10 or more points requires at least 252 blocks.

3.3.2 When $(\mathscr{G}, w)$-KDPs are (t, w)-KDPs

It is natural to speculate that any $(\mathscr{G}, w)$-KDP where $\mathscr{G} = \{G \in 2^{\mathscr{P}} : |G| = t\}$ is also a (t, w)-KDP. The following example demonstrates that this is not always the case.

Example 3.3.1. Let $t \geq 2$ and let $\mathscr{P}$ be any finite set with $|\mathscr{P}| > t$. Further, let $\mathscr{B} = \{X \in 2^{\mathscr{P}} : |X| = t\}$ and $\mathscr{I} \subseteq \mathscr{P} \times \mathscr{B}$ be defined by $(P, X) \in \mathscr{I}$ if, and only if, $P \in X$. Then $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a finite incidence structure. Next let $\mathscr{G} = \{G \in 2^{\mathscr{P}} : |G| = t\}$ and let $\mathscr{F} \supseteq \{F \in 2^{\mathscr{P}} : 1 \leq |F| \leq |\mathscr{P}| - t + 1\}$. Then, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP but not a $(t, \mathscr{F})$-KDP. More specifically, for $w \geq |\mathscr{P}| - t + 1$, $\mathscr{K}$ is a $(\mathscr{G}, w)$-KDP but not a (t, w)-KDP.

Proof. First let us note that from Definition 3.2.4, $\mathscr{K}$ is a trivial $\mathscr{G}$-KDP and hence is a $(\mathscr{G}, \mathscr{F}')$-KDP for any $\mathscr{F}' \subseteq 2^{\mathscr{P}} \setminus \{\varnothing\}$. To show that $\mathscr{K}$ is not a $(t, \mathscr{F})$-KDP we let H be any subset of $\mathscr{P}$ with $|H| = t - 1$. Let $F = \mathscr{P} \setminus H$, then $F \in \mathscr{F}$, since $|F| = |\mathscr{P}| - t + 1$. Furthermore, $F \cap H = \varnothing$ and $\bigcap_{P \in H}(P) \subseteq \bigcup_{Q \in F}(Q)$. To see that $\bigcap_{P \in H}(P) \subseteq \bigcup_{Q \in F}(Q)$, note that if $X \in \bigcap_{P \in H}(P)$ then $H \subseteq X$, and $H \neq X$ (since $|H| = t - 1$ and $|X| = t$). Therefore, there exists a point $Q' \in X \setminus H \subseteq F$ and hence $X \in (Q') \subseteq \bigcup_{Q \in F}(Q)$. Thus, $\mathscr{K}$ is not a $(t, \mathscr{F})$-KDP. □

Despite Example 3.3.1, there are many situations in which a $(\mathscr{G}, w)$-KDP where $\mathscr{G} = \{G \in 2^{\mathscr{P}} : |G| = t\}$ is a (t, w)-KDP. We now consider the most general situation.

Proposition 3.3.8. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. Let $\mathscr{G}, \mathscr{G}'$ and $\mathscr{F}$ be families of non-empty subsets of $\mathscr{P}$ with the property that for every $G' \in \mathscr{G}'$ and every $F \in \mathscr{F}$ such that $G' \cap F = \varnothing$, there exists a $G \in \mathscr{G}$ such that $G' \subseteq G$ and $G \cap F = \varnothing$. If $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then $\mathscr{K}$ is a $(\mathscr{G}', \mathscr{F})$-KDP.*

Proof. Suppose that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP and that $\mathscr{G}, \mathscr{G}'$ and $\mathscr{F}$ are defined as in the statement of the proposition. Now, suppose that $G' \in \mathscr{G}'$ and $F \in \mathscr{F}$ are such that $G' \cap F = \varnothing$. Choose $G \in \mathscr{G}$ such that $G' \subseteq G \subseteq \mathscr{P} \setminus F$, (or $G \cap F = \varnothing$). Then $\varnothing \neq \bigcap_{P \in G}(P) \setminus \bigcup_{Q \in F}(Q) \subseteq \bigcap_{P' \in G'}(P') \setminus \bigcup_{Q \in F}(Q)$. Therefore, $\mathscr{K}$ is a $(\mathscr{G}', \mathscr{F})$-KDP. □

We can now use Proposition 3.3.8 to obtain a result for (t, w)-KDPs.

Corollary 3.3.9. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP for some t such that $1 \leq t < |\mathscr{P}|$, $\mathscr{G} = \{G \in 2^{\mathscr{P}} : |G| = t\}$ and $\mathscr{F} \subseteq \{F \in 2^{\mathscr{P}} : 1 \leq |F| \leq |\mathscr{P}| - t\}$, then $\mathscr{K}$ is a $(t, \mathscr{F})$-KDP. In particular, if $\mathscr{K}$ is a $(\mathscr{G}, w)$-KDP and $1 \leq w \leq |\mathscr{P}| - t$, then $\mathscr{K}$ is a (t, w)-KDP.*

Proof. Suppose that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP as defined in the statement of the corollary and let $\mathscr{G}' = \{G' \in 2^{\mathscr{P}} : 1 \leq |G'| < t\}$. Choose $G' \in \mathscr{G}'$ and $F \in \mathscr{F}$ such that $G' \cap F = \varnothing$. Now, let H be any subset of $\mathscr{P} \setminus [G' \cup F]$ such that $|H| = t - |G'| \geq 1$. Note that this is possible since,

$$\begin{aligned} \big|\mathscr{P} \setminus [G' \cup F]\big| &= |\mathscr{P}| - |G' \cup F| \\ &= |\mathscr{P}| - \big[|G'| + |F|\big] \text{ (since } G' \cap F = \varnothing) \\ &\geq |\mathscr{P}| - |G'| - \big[|\mathscr{P}| - t\big] \\ &= t - |G'|. \end{aligned}$$

We know that $|G' \cup H| = t$, so $G = G' \cup H \in \mathscr{G}$. That is, there exists a $G \in \mathscr{G}$ such that $G' \subseteq G$ and $G \cap F = \varnothing$. Therefore, by Proposition 3.3.8, $\mathscr{K}$ is a $(t, \mathscr{F})$-KDP. □

3.3.3 When $(t, \mathscr{F})$-KDPs are (t, w)-KDPs

In a similar way to Example 3.3.1, Example 3.3.2 demonstrates that it is not always the case that any $(t, \mathscr{F})$-KDP where $\mathscr{F} = \{F \in 2^{\mathscr{P}} : |F| = w\}$ is also a (t, w)-KDP.

Example 3.3.2. Let $w \geq 2$ and let $\mathscr{P}$ be any finite set with $|\mathscr{P}| > w$. Further, let $\mathscr{B} = \{X \in 2^{\mathscr{P}} : |X| = |\mathscr{P}| - w\}$ and $\mathscr{I} \subseteq \mathscr{P} \times \mathscr{B}$ be defined by $(P, X) \in \mathscr{I}$ if, and only if, $P \in X$. Then $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a finite incidence structure. Next let $\mathscr{G} \supseteq \{G \in 2^{\mathscr{P}} : 0 < |G| \leq |\mathscr{P}| - w + 1\}$ and let $\mathscr{F} = \{F \in 2^{\mathscr{P}} : |F| = w\}$. Then, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP but not a $(\mathscr{G}, w)$-KDP. More specifically, for $t \geq |\mathscr{P}| - w + 1$, $\mathscr{K}$ is a $(t, \mathscr{F})$-KDP but not a (t, w)-KDP.

Proof. First, let us note that from Definition 3.2.8, $\mathscr{K}$ is a cotrivial $\mathscr{F}$-KDP and hence is a $(\mathscr{G}', \mathscr{F})$-KDP for any $\mathscr{G}' \subseteq 2^{\mathscr{P}} \setminus \{\varnothing\}$. To show that $\mathscr{K}$ is not a $(\mathscr{G}, w)$-KDP, we let H be any subset of $\mathscr{P}$ with $|H| = w - 1$. Let $G = \mathscr{P} \setminus H$ and note that $|G| = |\mathscr{P}| - w + 1$, and thus $G \in \mathscr{G}$. Also, $G \cap H = \varnothing$ and $\bigcap_{P \in G}(P) \subseteq \bigcup_{Q \in H}(Q)$, since $\bigcap_{P \in G}(P) = \varnothing$. That is, $\mathscr{K}$ is not a $(\mathscr{G}, w)$-KDP. □

In contrast to Example 3.3.2, there are many situations in which a $(t, \mathscr{F})$-KDP where $\mathscr{F} = \{F \in 2^{\mathscr{P}} : |G| = w\}$ is a (t, w)-KDP.

Proposition 3.3.10 is similar to Proposition 3.3.8 and sets up the most general situation.

Proposition 3.3.10. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. Let $\mathscr{G}, \mathscr{F}$ and $\mathscr{F}'$ be families of non-empty subsets of $\mathscr{P}$ with the property that* *for every $F' \in \mathscr{F}'$ and $G \in \mathscr{G}$ such that $G \cap F' = \varnothing$, there exists an $F \in \mathscr{F}$ such that $F' \subseteq F$ and $G \cap F = \varnothing$. If $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F}')$-KDP.*

Proof. Suppose that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP and that $\mathscr{G}, \mathscr{F}$ and $\mathscr{F}'$ are as defined in the statement of the proposition. Now, suppose that $F' \in \mathscr{F}'$ and $G \in \mathscr{G}$ are such that $G \cap F' = \varnothing$. Choose $F \in \mathscr{F}$ such that $F' \subseteq F \subseteq \mathscr{P} \setminus G$, (or $G \cap F = \varnothing$). Then $\varnothing \neq \bigcap_{P \in G}(P) \setminus \bigcup_{Q \in F}(Q) \subseteq \bigcap_{P \in G}(P) \setminus \bigcup_{Q' \in F'}(Q')$. Therefore, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F}')$-KDP. □

The following corollary is similar to Corollary 3.3.9.

Corollary 3.3.11. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP for some w such that $1 \leq w < |\mathscr{P}|$, $\mathscr{G} \subseteq \{G \in 2^{\mathscr{P}} : 1 \leq |G| \leq |\mathscr{P}| - w\}$ and $\mathscr{F} = \{F \in 2^{\mathscr{P}} : |F| = w\}$, then $\mathscr{K}$ is a $(\mathscr{G}, w)$-KDP. In particular, if $\mathscr{K}$ is a $(t, \mathscr{F})$-KDP and $1 \leq t \leq |\mathscr{P}| - w$, then $\mathscr{K}$ is a (t, w)-KDP.*

Proof. Suppose that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP as defined in the statement of the corollary and let $\mathscr{F}' = \{F' \in 2^{\mathscr{P}} : 1 \leq |F'| < w\}$. Choose $F' \in \mathscr{F}'$ and $G \in \mathscr{G}$ such that $G \cap F' = \varnothing$. Now, let H be any subset of $\mathscr{P} \setminus [G \cup F']$ such that $|H| = w - |F'| \geq 1$. Note that this is possible since,

$$\begin{aligned}
\big|\mathscr{P} \setminus [G \cup F']\big| &= |\mathscr{P}| - |G \cup F'| \\
&= |\mathscr{P}| - \big[|G| + |F'|\big] \text{ (since } G \cap F' = \varnothing) \\
&\geq |\mathscr{P}| - \big[|\mathscr{P}| - w\big] - |F'| \\
&= w - |F'|.
\end{aligned}$$

We know that $|F' \cup H| = w$, so $F = F' \cup H \in \mathscr{F}$. That is, there exists an $F \in \mathscr{F}$ such that $F' \subseteq F$ and $G \cap F = \varnothing$. Therefore, by Proposition 3.3.10, $\mathscr{K}$ is a $(\mathscr{G}, w)$-KDP. □

3.3.4 Special Properties of $(\mathscr{G}, w)$-KDPs

In this subsection we make an observation establishing a 1-to-1 relationship within $(\mathscr{G}, \mathscr{F})$-KDPs possessing certain properties. This observation is presented here because it applies particularly to the case of $(\mathscr{G}, w)$-KDPs.

Observation 3.3.12. *Let a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a $(\mathscr{G}, \mathscr{F})$-KDP with the property that if $G, G' \in \mathscr{G}$ and $G \neq G'$ then there exists an $F \in \mathscr{F}$ such that either:*
(i) $G \cap F \neq \varnothing$ and $G' \cap F = \varnothing$; or (ii) $G \cap F = \varnothing$ and $G' \cap F \neq \varnothing$.
Then, the mapping $G \to \bigcap_{P \in G}(P)$ from $\mathscr{G}$ into subsets of $\mathscr{B}$ is 1*-to-*1*.*

Proof. Suppose that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP as defined in the statement of the observation and choose $G, G' \in \mathscr{G}$ such that $G \neq G'$. Then, there exists an $F \in \mathscr{F}$ such that either (i) $G \cap F \neq \varnothing$ and $G' \cap F = \varnothing$ or (ii) $G \cap F = \varnothing$ and $G' \cap F \neq \varnothing$.
If (i) holds, then $\bigcap_{P \in G}(P) \subseteq \bigcup_{Q \in F}(Q)$ and $\bigcap_{P' \in G'}(P') \nsubseteq \bigcup_{Q \in F}(Q)$, and if (ii) holds then $\bigcap_{P \in G}(P) \nsubseteq \bigcup_{Q \in F}(Q)$ and $\bigcap_{P' \in G'}(P') \subseteq \bigcup_{Q \in F}(Q)$, since $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP. In either case, it follows that $\bigcap_{P \in G}(P) \neq \bigcap_{P' \in G'}(P')$ and hence the mapping $G \to \bigcap_{P \in G}(P)$ from $\mathscr{G}$ into subsets of $\mathscr{B}$ is 1-to-1. □

Observation 3.3.12 can be applied to many different $(\mathscr{G}, \mathscr{F})$-KDPs and Remark 3.3.13 specifies some of them, including any $(\mathscr{G}, w)$-KDP.

Remark 3.3.13. If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP and $\mathscr{F}$ contains all the singletons (in particular any $(\mathscr{G}, w)$-KDP), then the mapping $G \to \bigcap_{P \in G}(P)$ from $\mathscr{G}$ into subsets of $\mathscr{B}$ is 1-to-1.

Establishing a 1-to-1 mapping from the privileged subsets to the common block sets for those subsets is significant because it will later (Chapter 6) enable us to determine a lower bound for the number of blocks in terms of the number of privileged subsets. That is, for the special classes of $(\mathscr{G}, \mathscr{F})$-KDPs, as specified in Observation 3.3.12, we will find a lower bound for the number of subkeys in terms of the number of groups requiring secure communication.

3.4 Related Definitions

As previously mentioned, $(\mathscr{G}, \mathscr{F})$-KDPs have, in one form or another, been investigated and analysed by many authors in a variety of different ways. In this section we shall compare some of these approaches to our own.

We first compare KDPs from two incidence structures with a homomorphism between them.

Proposition 3.4.1. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ and $\mathscr{K}' = (\mathscr{P}', \mathscr{B}', \mathscr{I}')$ be two incidence structures and let a pair of mappings $\varphi : \mathscr{P} \to \mathscr{P}'$ and $\psi : \mathscr{B} \to \mathscr{B}'$ form a homomorphism from $\mathscr{K}$ to $\mathscr{K}'$. If $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then $\mathscr{K}'$ is a $(\mathscr{G}', \mathscr{F}')$-KDP where $\mathscr{G}' = \{\varphi(G) : G \in \mathscr{G}\}$ and $\mathscr{F}' = \{\varphi(F) : F \in \mathscr{F}\}$.*

Proof. Suppose that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP and consider $\varphi(G) \in \mathscr{G}'$ and $\varphi(F) \in \mathscr{F}'$ for some $G \in \mathscr{G}$ and $F \in \mathscr{F}$ such that $\varphi(G) \cap \varphi(F) = \varnothing$. Then $G \cap F = \varnothing$ and since $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP, there exists an $x \in \mathscr{B}$ such that $x \in \bigcap_{P \in G}(P) \setminus \bigcup_{Q \in F}(Q)$.

$$\begin{aligned}
\text{Now,} \quad & x \in \bigcap_{P \in G}(P) \setminus \bigcup_{Q \in F}(Q) \\
\iff \quad & (P, x) \in \mathscr{I} \text{ and } (Q, x) \notin \mathscr{I}, \text{ for all } P \in G \text{ and all } Q \in F \\
\iff \quad & (\varphi(P), \psi(x)) \in \mathscr{I}' \text{ and } (\varphi(Q), \psi(x)) \notin \mathscr{I}', \\
& \qquad\qquad\qquad\qquad \text{for all } P \in G \text{ and all } Q \in F \\
\iff \quad & (P', \psi(x)) \in \mathscr{I}' \text{ and } (Q', \psi(x)) \notin \mathscr{I}', \\
& \qquad\qquad\qquad\qquad \text{for all } P' \in \varphi(G) \text{ and all } Q' \in \varphi(F) \\
\iff \quad & \psi(x) \in \bigcap_{P' \in \varphi(G)}(P') \setminus \bigcup_{Q' \in \varphi(F)}(Q').
\end{aligned}$$

Therefore, $\mathscr{K}'$ is a $(\mathscr{G}', \mathscr{F}')$-KDP for $\mathscr{G}' = \{\varphi(G) : G \in \mathscr{G}\}$ and $\mathscr{F}' = \{\varphi(F) : F \in \mathscr{F}\}$. □

Loosely speaking, Proposition 3.4.1 shows that homomorphisms acting between incidence structures map a $(\mathscr{G}, \mathscr{F})$-KDP to a $(\mathscr{G}', \mathscr{F}')$-KDP for appropriate $\mathscr{G}'$ and $\mathscr{F}'$. Next, we shall show, with a small additional constraint on the mapping acting between the block sets, that the inverse image of a $(\mathscr{G}', \mathscr{F}')$-KDP under a pair of homomorphism maps is a $(\mathscr{G}, \mathscr{F})$-KDP.

Proposition 3.4.2. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ and $\mathscr{K}' = (\mathscr{P}', \mathscr{B}', \mathscr{I}')$ be two incidence structures and let the pair of mappings $\varphi : \mathscr{P} \to \mathscr{P}'$ and $\psi : \mathscr{B} \to \mathscr{B}'$ form a homomorphism from $\mathscr{K}$ to $\mathscr{K}'$. If $\mathscr{K}'$ is a $(\mathscr{G}', \mathscr{F}')$-KDP and both φ and ψ are surjective, then $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP where $\mathscr{G} = \{\varphi^{-1}(G') : G' \in \mathscr{G}'\}$ and $\mathscr{F} = \{\varphi^{-1}(F') : F' \in \mathscr{F}'\}$.*

Proof. Suppose that $\mathscr{K}'$ is a $(\mathscr{G}', \mathscr{F}')$-KDP and consider $\varphi^{-1}(G') \in \mathscr{G}$ and $\varphi^{-1}(F') \in \mathscr{F}$ for some $G' \in \mathscr{G}'$ and $F' \in \mathscr{F}'$ such that $\varphi^{-1}(G') \cap \varphi^{-1}(F') = \varnothing$. Then, since φ is surjective, $G' \cap F' = \varnothing$ and since $\mathscr{K}'$ is a $(\mathscr{G}', \mathscr{F}')$-KDP there exists a $x' \in \mathscr{B}'$ such that $x' \in \bigcap_{P' \in G'} (P') \setminus \bigcup_{Q' \in F'} (Q')$. Further, since ψ is surjective there exists an $x \in \mathscr{B}$ such that $\psi(x) = x'$.

$$\begin{aligned}
\text{Now,} \quad & x' \in \bigcap_{P' \in G'} (P') \setminus \bigcup_{Q' \in F'} (Q') \\
\iff \quad & (P', x') \in \mathscr{I}' \text{ and } (Q', x') \notin \mathscr{I}', \text{ for all } P' \in G' \text{ and all } Q' \in F' \\
\iff \quad & (\varphi(P), \psi(x)) \in \mathscr{I}' \text{ and } (\varphi(Q), \psi(x)) \notin \mathscr{I}', \\
& \qquad \qquad \text{for all } P \in \varphi^{-1}(G') \text{ and all } Q \in \varphi^{-1}(F') \\
\iff \quad & (P, x) \in \mathscr{I} \text{ and } (Q, x) \notin \mathscr{I}, \\
& \qquad \qquad \text{for all } P \in \varphi^{-1}(G') \text{ and all } Q \in \varphi^{-1}(F') \\
\iff \quad & x \in \bigcap_{P \in \varphi^{-1}(G')} (P) \setminus \bigcup_{Q \in \varphi^{-1}(F')} (Q).
\end{aligned}$$

Therefore, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP for $\mathscr{G} = \{\varphi^{-1}(G') : G' \in \mathscr{G}'\}$ and $\mathscr{F} = \{\varphi^{-1}(F') : F' \in \mathscr{F}'\}$. □

By combining Proposition 3.4.1 and Proposition 3.4.2 we obtain the following useful result.

Theorem 3.4.3. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ and $\mathscr{K}' = (\mathscr{P}', \mathscr{B}', \mathscr{I}')$ be two incidence structures such that a pair of mappings $\varphi : \mathscr{P} \to \mathscr{P}'$ and $\psi : \mathscr{B} \to \mathscr{B}'$ form a homomorphism from $\mathscr{K}$ to $\mathscr{K}'$. If φ is bijective and ψ is surjective, then $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, $\mathscr{K}'$ is a $(\mathscr{G}', \mathscr{F}')$-KDP for $\mathscr{G}' = \{\varphi(G) : G \in \mathscr{G}\}$ and $\mathscr{F}' = \{\varphi(F) : F \in \mathscr{F}\}$.*

Proof. This follows from Propositions 3.4.1 and 3.4.2, since $\varphi^{-1}(\varphi(G)) = G$ and $\varphi^{-1}(\varphi(F)) = F$ for each $G \in \mathscr{G}$ and $F \in \mathscr{F}$. □

If we recall the standard representation of an incidence structure, Definition 2.1.8, then we can present an interesting special case of Theorem 3.4.3.

Corollary 3.4.4. *A finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, the standard representation of $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP.*

We now present another special case of Theorem 3.4.3.

Corollary 3.4.5. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ and $\mathscr{K}' = (\mathscr{P}', \mathscr{B}', \mathscr{I}')$ be two incidence structures such that a pair of mappings $\varphi : \mathscr{P} \to \mathscr{P}'$ and $\psi : \mathscr{B} \to \mathscr{B}'$ form an isomorphism from $\mathscr{K}$ to $\mathscr{K}'$. Then, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, $\mathscr{K}'$ is a $(\mathscr{G}', \mathscr{F}')$-KDP for $\mathscr{G}' = \{\varphi(G) : G \in \mathscr{G}\}$ and $\mathscr{F}' = \{\varphi(F) : F \in \mathscr{F}\}$.*

3.4.1 Stinson's Definition

In [82] Stinson defined $(\mathscr{G}, \mathscr{F})$-KDPs using set notation and by considering each block as a set of points.

Definition 3.4.6. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure where $\mathscr{B} \subseteq 2^{\mathscr{P}} \setminus \{\varnothing\}$ and $\mathscr{I} \subseteq \mathscr{P} \times \mathscr{B}$ is defined by $(P, X) \in \mathscr{I}$ if, and only if, $P \in X$. If $\mathscr{G}$ and $\mathscr{F}$ are families of non-empty subsets of $\mathscr{P}$, then, $\mathscr{K}$ is said to satisfy **Stinson's Definition** with respect to $\mathscr{G}$ and $\mathscr{F}$, if*

$$\{X \in \mathscr{B} : G \subseteq X \text{ and } F \cap X = \varnothing\} \neq \varnothing,$$
$$\text{for all } G \in \mathscr{G} \text{ and } F \in \mathscr{F} \text{ such that } G \cap F = \varnothing.$$

Or, equivalently, for all $G \in \mathscr{G}$ and $F \in \mathscr{F}$ such that $G \cap F = \varnothing$, there exists an $X \in \mathscr{B}$ such that $G \subseteq X$ and $F \cap X = \varnothing$.

The standard representation of an incidence structure (Definition 2.1.8) will now assist us in comparing Stinson's Definition to our own definition of $(\mathscr{G}, \mathscr{F})$-KDPs.

Theorem 3.4.7. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{K}^S = (\mathscr{P}^S, \mathscr{B}^S, \mathscr{I}^S)$ be the standard representation of $\mathscr{K}$. Then, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, $\mathscr{K}^S$ satisfies Stinson's Definition with respect to $\mathscr{G}$ and $\mathscr{F}$.*

Proof. We know from Corollary 3.4.4 that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, $\mathscr{K}^S$ is a $(\mathscr{G}, \mathscr{F})$-KDP. So, it remains to show that $\mathscr{K}^S$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, $\mathscr{K}^S$ satisfies Stinson's Definition with respect to $\mathscr{G}$ and $\mathscr{F}$. Suppose that $G \in \mathscr{G}$, $F \in \mathscr{F}$ and $G \cap F = \varnothing$, then there exists an $X \in \mathscr{B}^S$ such that:

$$\begin{aligned}
& X \in \bigcap_{P \in G} (P) \setminus \bigcup_{Q \in F} (Q) \\
\Longleftrightarrow \quad & X \in (P) \text{ and } X \notin (Q), \text{ for all } P \in G \text{ and all } Q \in F \\
\Longleftrightarrow \quad & (P, X) \in \mathscr{I}^S \text{ and } (Q, X) \notin \mathscr{I}^S, \text{ for all } P \in G \text{ and all } Q \in F \\
\Longleftrightarrow \quad & P \in X \text{ and } Q \notin X, \text{ for all } P \in G \text{ and all } Q \in F \\
\Longleftrightarrow \quad & G \subseteq X \text{ and } F \cap X = \varnothing \\
\Longleftrightarrow \quad & \{X \in \mathscr{B}^S : G \subseteq X \text{ and } F \cap X = \varnothing\} \neq \varnothing.
\end{aligned}$$

Therefore, $\mathscr{K}^S$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, $\mathscr{K}^S$ satisfies Stinson's Definition with respect to $\mathscr{G}$ and $\mathscr{F}$. Hence, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, $\mathscr{K}^S$ satisfies Stinson's Definition with respect to $\mathscr{G}$ and $\mathscr{F}$. □

We are now able to use Stinson's Definition when referring to $(\mathscr{G}, \mathscr{F})$-KDPs, but we should be wary, since Stinson's Definition does not allow for repeated blocks (Definition 2.1.2) within a $(\mathscr{G}, \mathscr{F})$-KDP, whereas our original definition (Definition 3.1.1) does. This is not an important issue, as will be highlighted in Section 4.1, since repeated blocks contribute nothing to the security of a $(\mathscr{G}, \mathscr{F})$-KDP and may be considered redundant.

Stinson used his definition in order to study the relationship between $t-(v, k, \lambda)$-designs (see Definition 2.1.4) and (t, w)-KDPs [82]. He was also able to construct $(\mathscr{G}, \mathscr{F})$-KDPs using combinatorial objects [47, 84], (see Chapter 5).

3.4.2 Cover Free Families

Cover Free Families (CFFs), were first introduced by Kautz and Singleton [40] in 1964. Essentially CFFs are families of finite sets such that the intersection of any collection of t of these sets is not covered by the union of any other collection of w of them.

Definition 3.4.8. *Let X be a set and $\mathcal{S} \subseteq 2^X$. Then, $\mathcal{S}$ is said to be a* ***(t, w)-Cover Free Family*** *(or (t, w)-CFF) on X, for $t \geq 1$ and $w \geq 1$, if for any t subsets $P_1, P_2, ..., P_t \in \mathcal{S}$ and any other w subsets $Q_1, Q_2, \ldots, Q_w \in \mathcal{S}$, $\bigcap\limits_{i=1}^{t} P_i \not\subseteq \bigcup\limits_{j=1}^{w} Q_j$.*

Originally t was set to 1, but since the introduction of CFFs to investigate superimposed binary codes, they have been investigated, discussed and generalised in many different ways [29, 30, 34, 78, 86]. In fact, Key Distribution Patterns are one such generalisation of CFFs.

Superimposed binary codes [24, 40, 42] have been used to represent document attributes within an information retrieval system and as a basis for channel assignments to relieve congestion in crowded communications bands. They consist of a set of codewords whose digit by digit Boolean sums have a prescribed level of distinguishability. More precisely, a binary (t, w)-superimposed code is exactly the incidence matrix of a (t, w)-CFF.

The precise relationship between (t, w)-CFFs and (t, w)-KDPs is given next. However, its simple proof is omitted.

Theorem 3.4.9. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure with no repeated points. Then, $\mathscr{K}$ is a (t, w)-KDP, for $t \geq 1$ and $w \geq 1$, if, and only if, $\mathcal{S} = \{(P) : P \in \mathscr{P}\}$ is a (t, w)-CFF on $\mathscr{B}$.*

Naturally enough, the study of CFFs has been useful in the study of (t, w)-KDPs. In particular, several lower bounds on the information storage of (t, w)-KDPs have been proved [85], see Chapter 6.

Cover Free Families have also been considered under other names. For example, in [26], Dyer, Fenner, Freize and Thomason called (t, w)-CFFs, w-secure t-intersection schemes. By using probabilistic methods [1, 10, 80], as opposed to a deterministic approach, Dyer *et al.* [26] were able to analyse t-intersection schemes in a new way. Generating the sets randomly and minimising the probability of getting "bad cases", that is, $\bigcap_{i=1}^{t} P_i \subseteq \bigcup_{j=1}^{w} Q_j$, they were able to generate "good" t-intersection schemes with high probability.

Also in [26], bounds are given on the number of subkeys in a system, constructions show the existence of t-intersection schemes with a specified number of subkeys and the practical aspects of the probabilistic approach are analysed. We do not pursue the probabilistic approach within this thesis. However, the bounds in [26] on the number of subkeys in a system are considered in Chapter 6, and the existence results allow for the construction of new KDPs from old (see Chapter 5).

Chapter 4

Secondary Observations

In this chapter we consider two main concepts. Firstly, we consider the concept of redundancy within a $(\mathscr{G},\mathscr{F})$-KDP and secondly, we consider the largest possible sets of privileged and forbidden subsets. These two concepts both emerge by first considering some predefined incidence structure, $\mathscr{K}$ and then considering the sets of privileged and forbidden subsets for which $\mathscr{K}$ is a $(\mathscr{G},\mathscr{F})$-KDP. This approach is different to that used throughout the majority of this thesis, and although interesting the results in this chapter do not have a large impact on the rest of the thesis.

In Section 4.1 we begin by considering the points and blocks that, for a given incidence structure $\mathscr{K}$, play no role in any $(\mathscr{G},\mathscr{F})$-KDP, regardless of the choice of privileged and forbidden subsets. We next consider privileged and forbidden subsets that satisfy the security condition vacuously, and in both cases, we show that if an incidence structure $\mathscr{K}$ is a $(\mathscr{G},\mathscr{F})$-KDP, then we can remove the redundancy from $\mathscr{K}$ without affecting any "real" security or communication.

In Section 4.2, for a predefined incidence structure, $\mathscr{K}$, we attempt to find the largest possible set of privileged and forbidden subsets for which $\mathscr{K}$ is a $(\mathscr{G},\mathscr{F})$-KDP. We observe the trade-off between the size of the set of privileged subsets and the size of the set of forbidden subsets and consider the largest set of privileged subsets for a given set of forbidden subsets and the largest set of forbidden subsets for a given set of privileged subsets. Finally, we show that there is, in general, no largest $(\mathscr{G}, \mathscr{F})$-KDP for a given incidence structure, instead there are many distinct maximal $(\mathscr{G}, \mathscr{F})$-KDPs.

4.1 Redundancy

This section contains an analysis of redundancy within a $(\mathscr{G}, \mathscr{F})$-KDP.

4.1.1 Point and Block Redundancy

In an incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ we will consider a point or a block to be *redundant* if it plays no "role" in any $(\mathscr{G}, \mathscr{F})$-KDP regardless of the choice of privileged and forbidden subsets. We start by tackling repeated points and repeated blocks (see Definition 2.1.1 and Definition 2.1.2).

Repeated points correspond to users holding identical sets of subkeys. Such users will have identical communication privileges within any $(\mathscr{G}, \mathscr{F})$-KDP and all secure communications will be visible to any user who holds an identical subset of subkeys to the sender. That is, users holding identical subsets of subkeys will not be able to use the system to exclude each other from any secure communications. On the other hand, there are practical situations where it may be beneficial for two or more users to have identical access. Any job sharing scenario or situation where immediate and complete information sharing is important could be facilitated by users holding identical sets of subkeys. Therefore, we will not consider repeated points to be redundant.

Repeated blocks correspond to subkeys held by an identical set of users. When calculating a secret key, this set of users will combine all such subkeys, but when compared to simply using just one of these repeated subkeys, there is no extra benefit. Intuitively, repeated blocks enable no additional communication and offer no extra security. More precisely, the standard representation of an incidence structure contains no repeated blocks. Recall, from

Corollary 3.4.4 that an incidence structure is a $(\mathscr{G},\mathscr{F})$-KDP if, and only if, its standard representation is a $(\mathscr{G},\mathscr{F})$-KDP, for the same $\mathscr{G}$ and the same $\mathscr{F}$. In this way we see that removing repeated blocks does not affect either the security or the communication within a $(\mathscr{G},\mathscr{F})$-KDP. Therefore, we consider repeated blocks to be redundant for all $(\mathscr{G},\mathscr{F})$-KDPs.

Other blocks that we will consider to be redundant are those that are not incident with any points in the incidence structure. Similarly, we will consider points to be redundant if they are not incident with any blocks in the incidence structure. Such blocks correspond to subkeys held by no users and such points correspond to users holding no subkeys. Clearly, these blocks and points play no significant role in any $(\mathscr{G},\mathscr{F})$-KDP that can be constructed on the incidence structure.

The points and blocks that we have specified as redundant, are redundant for any $(\mathscr{G},\mathscr{F})$-KDP regardless of the choice of privileged and forbidden subsets. However, one might want to consider additional notions of redundancy, specific to a particular choice of privileged and forbidden subsets. For example, given a $(\mathscr{G},\mathscr{F})$-KDP, any block x such that $x \notin \bigcap_{P\in G}(P) \setminus \bigcup_{Q\in F}(Q)$ for any $G \in \mathscr{G}$ and $F \in \mathscr{F}$ such that $G \cap F = \varnothing$, and any point P such that $P \notin \bigcup_{G\in\mathscr{G}} G \cup \bigcup_{F\in\mathscr{F}} F$, play no role in that $(\mathscr{G},\mathscr{F})$-KDP and may be considered redundant.

4.1.2 Irreducible $(\mathscr{G},\mathscr{F})$-KDPs

In this section we consider the consequences of removing redundant points and blocks from a $(\mathscr{G},\mathscr{F})$-KDP. We begin with a definition.

Definition 4.1.1. *Let $\mathscr{K} = (\mathscr{P},\mathscr{B},\mathscr{I})$ be a finite incidence structure. Then, $\mathscr{K}$ is said to be* ***irreducible*** *if (i) it contains no repeated blocks, (ii) for all $P \in \mathscr{P}$ there exists an $x \in \mathscr{B}$ such that $(P,x) \in \mathscr{I}$ and (iii) for all $x \in \mathscr{B}$ there exists a $P \in \mathscr{P}$ such that $(P,x) \in \mathscr{I}$.*

That is, an incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is irreducible if it contains no redundant blocks and no redundant points. If $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is an irreducible incidence structure and $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then we say that $\mathscr{K}$ is an *irreducible* $(\mathscr{G}, \mathscr{F})$*-KDP*.

The following theorem shows that we can reduce a $(\mathscr{G}, \mathscr{F})$-KDP to an irreducible $(\mathscr{G}', \mathscr{F}')$-KDP whilst essentially maintaining the secure communication properties of the original $(\mathscr{G}, \mathscr{F})$-KDP.

Theorem 4.1.2. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure, let $\mathscr{K}^S = (\mathscr{P}^S, \mathscr{B}^S, \mathscr{I}^S)$ be the standard representation of $\mathscr{K}$ and let $\mathscr{G}$ and $\mathscr{F}$ be families of non-empty subsets of $\mathscr{P}$. If $\bigcap_{P \in G}(P) \neq \varnothing$ for all $G \in \mathscr{G}$, then $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, the incidence structure $\mathscr{K}' = (\mathscr{P}', \mathscr{B}', \mathscr{I}')$, where*

$$\mathscr{P}' = \{P \in \mathscr{P} : (P, x) \in \mathscr{I} \text{ for some } x \in \mathscr{B}\},$$

$$\mathscr{B}' = \{x \in \mathscr{B}^S : (P, x) \in \mathscr{I}^S \text{ for some } P \in \mathscr{P}\}$$

$$\text{and } \ \mathscr{I}' = \mathscr{I}^S \cap (\mathscr{P}' \times \mathscr{B}')$$

is an irreducible $(\mathscr{G}, \mathscr{F}')$-KDP for $\mathscr{F}' = \{F \cap \mathscr{P}' \in 2^{\mathscr{P}'} \setminus \{\varnothing\} : F \in \mathscr{F}\}$.

Proof. It is immediate from Definition 4.1.1 that $\mathscr{K}' = (\mathscr{P}', \mathscr{B}', \mathscr{I}')$ is an irreducible incidence structure. It only remains to show that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, $\mathscr{K}'$ is a $(\mathscr{G}, \mathscr{F}')$-KDP.

Firstly, suppose that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP and, in order to obtain a contradiction, suppose that $\mathscr{K}'$ is not a $(\mathscr{G}, \mathscr{F}')$-KDP. Then there exists a $G \in \mathscr{G}$ and an $F' \in \mathscr{F}'$ such that $G \cap F' = \varnothing$ and $\bigcap_{P \in G}(P) \subseteq \bigcup_{Q' \in F'}(Q')$. By the definition of $\mathscr{F}'$, there exists an $F \in \mathscr{F}$ such that $F \cap \mathscr{P}' = F'$. Moreover, since $G \cap \mathscr{P}' = G$, $F \cap G = F \cap \mathscr{P}' \cap G = F' \cap G = \varnothing$. Therefore, $\bigcap_{P \in G}(P) \subseteq \bigcup_{Q' \in F'}(Q') \subseteq \bigcup_{Q \in F}(Q)$, which contradicts the assumption that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP.

Now suppose that $\mathscr{K}'$ is a $(\mathscr{G}, \mathscr{F}')$-KDP and, in order to obtain a contradiction, suppose that $\mathscr{K}$ is not a $(\mathscr{G}, \mathscr{F})$-KDP. Then there exists a $G \in \mathscr{G}$ and an

$F \in \mathscr{F}$ such that $G \cap F = \varnothing$ and $\bigcap_{P \in G}(P) \subseteq \bigcup_{Q \in F}(Q)$. Since $\bigcap_{P \in G}(P) \neq \varnothing$, $F \cap \mathscr{P}' \neq \varnothing$, so by definition $F' = F \cap \mathscr{P}' \in \mathscr{F}'$ and $G \cap F' = \varnothing$. Now, $\bigcap_{P \in G}(P) \subseteq \bigcup_{Q \in F}(Q) = \bigcup_{Q' \in F'}(Q')$, which contradicts the assumption that $\mathscr{K}'$ is a $(\mathscr{G}, \mathscr{F}')$-KDP.

Therefore, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, $\mathscr{K}'$ is a $(\mathscr{G}, \mathscr{F}')$-KDP. $\square$

Since incidence structures are often represented using binary matrices, it is sometimes useful to describe an irreducible incidence structure in terms of its matrix representation. It is easy to see that a matrix representation of an irreducible incidence structure will have no repeated columns, no all zero columns and no all zero rows.

We now demonstrate Theorem 4.1.2 by means of an example.

Example 4.1.1. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure represented by the following 5×5 binary matrix.

$$\begin{array}{cccccc}
 & x_1 & x_2 & x_3 & x_4 & x_5 \\
P_1 & 1 & 0 & 1 & 1 & 0 \\
P_2 & 1 & 0 & 1 & 1 & 1 \\
P_3 & 1 & 0 & 0 & 1 & 1 \\
P_4 & 0 & 0 & 0 & 0 & 0 \\
P_5 & 0 & 1 & 1 & 0 & 1
\end{array}$$

Then, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP where,

$$\mathscr{G} = \big\{\{P_1, P_2, P_3\}, \{P_5\}, \{P_1, P_2, P_5\}, \{P_2, P_3, P_5\}, \{P_1, P_2\}, \{P_2, P_3\}, \{P_2, P_5\}, \{P_1\}, \{P_2\}\big\} \text{ and}$$

$$\mathscr{F} = \big\{\{P_1\}, \{P_3\}, \{P_4\}, \{P_5\}, \{P_1, P_2\}, \{P_4, P_5\}, \{P_1, P_2, P_3\}, \{P_1, P_2, P_5\}, \{P_1, P_2, P_3, P_5\}, \{P_1, P_2, P_4, P_5\}\big\}.$$

Column x_4 is identical to column x_1 and row P_4 contains all 0's, so both column x_1 and row P_4 are redundant. When these redundancies are removed, we are left with the following irreducible incidence structure.

$$\begin{array}{c|cccc} & x_1 & x_2 & x_3 & x_5 \\ P_1 & 1 & 0 & 1 & 0 \\ P_2 & 1 & 0 & 1 & 1 \\ P_3 & 1 & 0 & 0 & 1 \\ P_5 & 0 & 1 & 1 & 1 \end{array}$$

This new matrix represents a $(\mathscr{G}', \mathscr{F}')$-KDP where,

$$\mathscr{G}' = \big\{\{P_1, P_2, P_3\}, \{P_5\}, \{P_1, P_2, P_5\}, \{P_2, P_3, P_5\}, \{P_1, P_2\}, \{P_2, P_3\}, \\ \{P_2, P_5\}, \{P_1\}, \{P_2\}\big\} \text{ and}$$

$$\mathscr{F}' = \big\{\{P_1\}, \{P_3\}, \{P_5\}, \{P_1, P_2\}, \{P_1, P_2, P_3\}, \{P_1, P_2, P_5\}, \{P_1, P_2, P_3, P_5\}\big\}.$$

Note that the only change to the set of privileged and forbidden subsets is that the redundant points (just P_4 in this case) are removed. Redundant points will only appear in a privileged subset if that subset is not disjoint from any forbidden subset. So, in this example (as will often be the case), the set of privileged subsets remains unchanged.

4.1.3 Passive Subsets

A different type of redundancy is that eluded to in Example 4.1.1. Any privileged subset not disjoint from any forbidden subset and any forbidden subset not disjoint from any privileged subset will satisfy the security condition vacuously. In a sense these subsets may be considered redundant as they play no significant role in the $(\mathscr{G}, \mathscr{F})$-KDP.

Definition 4.1.3. *Let a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a $(\mathscr{G}, \mathscr{F})$-KDP. Any $G \in \mathscr{G}$ such that $G \cap F \neq \varnothing$ for all $F \in \mathscr{F}$ is said to be a* ***passive privileged subset****, and any $F \in \mathscr{F}$ such that $G \cap F \neq \varnothing$ for all $G \in \mathscr{G}$ is said to be a* ***passive forbidden subset****.*

Looking back at Example 4.1.1, we see that the two forbidden subsets $\{P_1, P_2, P_5\}$ and $\{P_1, P_2, P_3, P_5\}$ are both passive, since neither of them is disjoint from any privileged subset.

Although passive subsets appear to play no real role in a $(\mathscr{G}, \mathscr{F})$-KDP, there are situations in which they do arise. For example, when the definitions of $\mathscr{G}$ and $\mathscr{F}$ are prescribed (as in $(t, \mathscr{F})$-KDPs and $(\mathscr{G}, w)$-KDPs) they may naturally include passive privileged and/or forbidden subsets. Also, one may simply be given a set of privileged and forbidden subsets with passive subsets already included in them.

Definition 4.1.4. *Let a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ and let $\mathscr{G}$ and $\mathscr{F}$ be families of non-empty subsets of $\mathscr{P}$ such that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP. The set of privileged subsets $\mathscr{G}$ is said to be **tight** if for all $G \in \mathscr{G}$ there exists an $F \in \mathscr{F}$ such that, $G \cap F = \varnothing$. The set of forbidden subsets $\mathscr{F}$ is said to be **tight** if for all $F \in \mathscr{F}$ there exists a $G \in \mathscr{G}$ such that, $G \cap F = \varnothing$. Finally, a $(\mathscr{G}, \mathscr{F})$-KDP is said to be **tight** if both $\mathscr{G}$ and $\mathscr{F}$ are tight.*

That is, a tight $(\mathscr{G}, \mathscr{F})$-KDP is a $(\mathscr{G}, \mathscr{F})$-KDP that does not include any passive privileged subsets or any passive forbidden subsets. We now give a method for reducing any $(\mathscr{G}, \mathscr{F})$-KDP to a tight $(\mathscr{G}', \mathscr{F}')$-KDP.

Theorem 4.1.5. *Let a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a $(\mathscr{G}, \mathscr{F})$-KDP. Let $X \subseteq 2^{\mathscr{G}} \times 2^{\mathscr{F}}$ be the set of all ordered pairs $(\mathscr{G}', \mathscr{F}') \in 2^{\mathscr{G}} \times 2^{\mathscr{F}}$ such that $\mathscr{K}$ is a tight $(\mathscr{G}', \mathscr{F}')$-KDP and let " $\leq$ " be the partial order on X defined by $(\mathscr{G}'', \mathscr{F}'') \leq (\mathscr{G}', \mathscr{F}')$ if $\mathscr{G}'' \subseteq \mathscr{G}'$ and $\mathscr{F}'' \subseteq \mathscr{F}'$. Then*

$$\begin{aligned} \mathscr{G}' &= \{G \in \mathscr{G} : G \cap F = \varnothing \textit{ for some } F \in \mathscr{F}\} \\ \textit{and} \quad \mathscr{F}' &= \{F \in \mathscr{F} : G \cap F = \varnothing \textit{ for some } G \in \mathscr{G}\} \end{aligned}$$

are the largest $\mathscr{G}'$ and $\mathscr{F}'$, with respect to $(X, \leq)$, for which $\mathscr{K}$ is a tight $(\mathscr{G}', \mathscr{F}')$-KDP.

Proof. We begin this proof by showing that the $(\mathscr{G}', \mathscr{F}')$-KDP where $\mathscr{G}'$ and $\mathscr{F}'$ are given by $\mathscr{G}' = \{G \in \mathscr{G} : G \cap F = \varnothing$ for some $F \in \mathscr{F}\}$ and $\mathscr{F}' = \{F \in \mathscr{F} : G \cap F = \varnothing$ for some $G \in \mathscr{G}\}$ is tight. That is, we must show that for every $G \in \mathscr{G}', G \cap F = \varnothing$ for some $F \in \mathscr{F}'$ and for every $F \in \mathscr{F}', G \cap F = \varnothing$

for some $G \in \mathscr{G}'$. Let $\varphi : \mathscr{F}' \to \mathscr{G}$ be any map such that $F \cap \varphi(F) = \varnothing$ for every $F \in \mathscr{F}'$ (note that this is well-defined by the definition of $\mathscr{F}'$). We claim that φ actually maps $\mathscr{F}'$ into $\mathscr{G}'$. Take an arbitrary $F \in \mathscr{F}'$, then since $\varphi(F) \in \mathscr{G}$ and $F \cap \varphi(F) = \varnothing$, it follows that $\varphi(F) \in \mathscr{G}'$. In the same way, let $\psi : \mathscr{G}' \to \mathscr{F}$ be any map such that $G \cap \psi(G) = \varnothing$ for every $G \in \mathscr{G}'$ (again we note that this is well-defined by the definition of $\mathscr{G}'$). We claim that ψ maps $\mathscr{G}'$ into $\mathscr{F}'$. Take an arbitrary $G \in \mathscr{G}'$, then since $\psi(G) \in \mathscr{F}$ and $G \cap \psi(G) = \varnothing$, it follows that $\psi(G) \in \mathscr{F}'$.

It remains to show that the largest element in the partially ordered set $(X, \leq)$ is $(\mathscr{G}', \mathscr{F}')$. Suppose, in order to obtain a contradiction, that there is an ordered pair $(\mathscr{G}'', \mathscr{F}'')$ in the partial order $(X, \leq)$ such that $(\mathscr{G}'', \mathscr{F}'') \nleq (\mathscr{G}', \mathscr{F}')$. Since the $(\mathscr{G}'', \mathscr{F}'')$-KDP is tight, $\mathscr{G}'' \subseteq \{G \in \mathscr{G} : G \cap F = \varnothing \text{ for some } F \in \mathscr{F}\}$ and $\mathscr{F}'' \subseteq \{F \in \mathscr{F} : G \cap F = \varnothing \text{ for some } G \in \mathscr{G}\}$. That is, $\mathscr{G}'' \subseteq \mathscr{G}'$ and $\mathscr{F}'' \subseteq \mathscr{F}'$ and so $(\mathscr{G}'', \mathscr{F}'') \leq (\mathscr{G}', \mathscr{F}')$. Therefore we have a contradiction and so $(\mathscr{G}', \mathscr{F}')$ is indeed the largest element in the partially ordered set $(X, \leq)$. Hence, $\mathscr{G}' = \{G \in \mathscr{G} : G \cap F = \varnothing \text{ for some } F \in \mathscr{F}\}$ and $\mathscr{F}' = \{F \in \mathscr{F} : G \cap F = \varnothing \text{ for some } G \in \mathscr{G}\}$ are the largest $\mathscr{G}'$ and $\mathscr{F}'$, with respect to $(X, \leq)$, for which $\mathscr{K}$ is tight $(\mathscr{G}', \mathscr{F}')$-KDP. □

Theorem 4.1.5 shows that every $(\mathscr{G}, \mathscr{F})$-KDP contains a canonical tight $(\mathscr{G}', \mathscr{F}')$-KDP. Moreover, the following theorem shows that (in a sense) reducing to this tight $(\mathscr{G}', \mathscr{F}')$-KDP preserves the secure communication properties of the larger $(\mathscr{G}, \mathscr{F})$-KDP. This is not really surprising, considering the fact that we are only removing passive privileged and forbidden subsets.

Theorem 4.1.6. *A finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, $\mathscr{K}$ is a $(\mathscr{G}', \mathscr{F}')$-KDP for*

$$\mathscr{G}' = \{G \in \mathscr{G} : G \cap F = \varnothing \textit{ for some } F \in \mathscr{F}\}$$
$$\textit{and } \mathscr{F}' = \{F \in \mathscr{F} : G \cap F = \varnothing \textit{ for some } G \in \mathscr{G}\}.$$

Proof. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and $\mathscr{G}$ and $\mathscr{F}$ be families of non-empty subsets of $\mathscr{P}$. Suppose that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then from Proposition 3.1.3 we know that $\mathscr{K}$ is a $(\mathscr{G}', \mathscr{F}')$-KDP.

Now suppose that $\mathscr{K}$ is a $(\mathscr{G}', \mathscr{F}')$-KDP and, in order to obtain a contradiction, suppose that $\mathscr{K}$ is not a $(\mathscr{G}, \mathscr{F})$-KDP. Then, there exists a $G \in \mathscr{G}$ and an $F \in \mathscr{F}$ such that $G \cap F = \varnothing$ and $\bigcap_{P \in G}(P) \subseteq \bigcup_{Q \in F}(Q)$. Since $G \cap F = \varnothing$, $G \in \mathscr{G}'$ and $F \in \mathscr{F}'$ which contradicts the assumption that $\mathscr{K}$ is a $(\mathscr{G}', \mathscr{F}')$-KDP. Hence $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP. □

From Theorem 4.1.2, Theorem 4.1.5 and Theorem 4.1.6 we see that if an incidence structure $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then by possibly passing to a smaller point set and block set, as well as reducing the size of the sets of privileged and forbidden subsets, we can reduce $\mathscr{K}$ to an irreducible, tight $(\mathscr{G}', \mathscr{F}')$-KDP. In this reduction, no real security or communication between the users is lost.

4.2 Largest Sets

Our goal in this section is to attempt to find, for a given incidence structure $\mathscr{K}$, the largest possible sets of privileged and forbidden subsets for which $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP. From Observation 3.1.2, we know that every finite incidence structure is a $(\mathscr{G}, \mathscr{F})$-KDP for some $\mathscr{G}$ and some $\mathscr{F}$. In fact, from Section 3.2, we know that every finite incidence structure can be a $(\mathscr{G}, \mathscr{F})$-KDP where the set of forbidden subsets is as large as possible $\big($that is, a trivial $\mathscr{G}$-KDP where $\mathscr{F} = 2^{\mathscr{P}} \setminus \{\varnothing\}\big)$ or a $(\mathscr{G}, \mathscr{F})$-KDP where the set of privileged subsets is as large as possible $\big($that is, a cotrivial $\mathscr{F}$-KDP where $\mathscr{G} = 2^{\mathscr{P}} \setminus \{\varnothing\}\big)$. Thus, under any reasonable ordering on the set of privileged and forbidden subsets for a given incidence structure, there appears to be no natural largest element (this is shown more precisely at the end of this section). Hence, we must modify our goal in order to proceed.

One way in which to proceed is based upon the fact that for any $(\mathscr{G},\mathscr{F})$-KDP, there is always a trade-off between the size of the set of privileged subsets and the size of the set of forbidden subsets. That is, adding to the set of privileged subsets restricts the possible set of forbidden subsets, and adding to the set of forbidden subsets restricts the possible set of privileged subsets. Therefore, it makes sense to consider how to maximise the size of the set of privileged subsets relative to the set of forbidden subsets and vice versa. More precisely, for a given incidence structure $\mathscr{K}$ and a set of forbidden subsets $\mathscr{F}$, it makes sense to attempt to find the largest possible set of privileged subsets $\mathscr{G}$ such that $\mathscr{K}$ is a $(\mathscr{G},\mathscr{F})$-KDP.

4.2.1 Largest Sets of Privileged Subsets

For a $(\mathscr{G},\mathscr{F})$-KDP we attempt to add to the set of privileged subsets, whilst measuring the impact on the set of forbidden subsets (and hopefully minimising that impact).

Theorem 4.2.1. *Suppose that a finite incidence structure $\mathscr{K}=(\mathscr{P},\mathscr{B},\mathscr{I})$ is a $(\mathscr{G},\mathscr{F})$-KDP. If $G_1,G_2,\ldots,G_n \in \mathscr{G}$ and $G'=\bigcap_{j=1}^{n} G_j \neq \varnothing$, then $\mathscr{K}$ is a $(\mathscr{G}',\mathscr{F}')$-KDP for*

$$\mathscr{G}'=\mathscr{G}\cup\{G'\} \quad \text{and}$$

$$\mathscr{F}'=\{F\in\mathscr{F} : G_j\cap F=\varnothing \text{ for some } 1\leq j\leq n \text{ or } G'\cap F\neq\varnothing\}.$$

Proof. By Proposition 3.1.3, we know that $\mathscr{K}$ is a $(\mathscr{G},\mathscr{F}')$-KDP. Therefore, it remains to show that $\bigcap_{P\in G'}(P) \nsubseteq \bigcup_{Q\in F}(Q)$ for all $F\in\mathscr{F}'$ such that $G'\cap F=\varnothing$. Suppose that $F\in\mathscr{F}'$ such that $G'\cap F=\varnothing$. Then from the definition of $\mathscr{F}'$, $G_j\cap F=\varnothing$ for some $1\leq j\leq n$. Since $G_j\in\mathscr{G}$ and $\mathscr{K}$ is a $(\mathscr{G},\mathscr{F}')$-KDP, $\bigcap_{P\in G_j}(P)\nsubseteq\bigcup_{Q\in F}(Q)$. However, as $G'=\bigcap_{i=1}^{n}G_i$, $G'\subseteq G_j$, it follows that $\bigcap_{P\in G_j}(P)\subseteq\bigcap_{P\in G'}(P)$. Hence, $\bigcap_{P\in G'}(P)\nsubseteq\bigcup_{Q\in F}(Q)$ and the proof is complete. □

If the set of forbidden subsets consists of all the singletons, then we have an interesting special case of Theorem 4.2.1.

Remark 4.2.2. In Theorem 4.2.1, if $\mathscr{F} = \{F \in 2^{\mathscr{P}} : |F| = 1\}$, then $\mathscr{F}' = \mathscr{F}$.

From Theorem 4.2.1 we can extract a more amenable result for extending the set of privileged subsets without affecting the set of forbidden subsets.

Corollary 4.2.3. *Suppose that a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP where $G_1, G_2, \ldots, G_n \in \mathscr{G}$ and $G' = \bigcap_{j=1}^{n} G_j \neq \varnothing$. Also, for each $P \in \mathscr{P}$ suppose that $\lambda_{G'}(P) = \big|\{j \in \{1, 2, \ldots, n\} : P \in G_j\}\big|$. If $\sum_{P \in F} \lambda_{G'}(P) < n$ for each $F \in \mathscr{F}$ such that $G' \cap F = \varnothing$, then $\mathscr{K}$ is a $(\mathscr{G}', \mathscr{F})$-KDP for $\mathscr{G}' = \mathscr{G} \cup \{G'\}$.*

Proof. From Theorem 4.2.1 it is sufficient to show that

$$\mathscr{F}' = \{F \in \mathscr{F} : G_j \cap F = \varnothing \text{ for some } 1 \leq j \leq n \text{ or } G' \cap F \neq \varnothing\} = \mathscr{F}.$$

Clearly $\mathscr{F}' \subseteq \mathscr{F}$, so it only remains to show that $\mathscr{F} \subseteq \mathscr{F}'$. To this end, consider $F \in \mathscr{F}$. If $G' \cap F \neq \varnothing$, then $F \in \mathscr{F}'$, so we may suppose that $G' \cap F = \varnothing$. Then, since

$$\big|\{j \in \{1, 2, \ldots, n\} : G_j \cap F \neq \varnothing\}\big| \leq \sum_{P \in F} \lambda_{G'}(P) < n,$$

$G_j \cap F = \varnothing$ for some $1 \leq j \leq n$. Therefore, $F \in \mathscr{F}'$ and hence $\mathscr{F} \subseteq \mathscr{F}'$. □

We now consider the special case of $(\mathscr{G}, w)$-KDPs.

Corollary 4.2.4. *Suppose that a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP for $w \geq 1$ and suppose that $G_1, G_2, \ldots, G_n \in \mathscr{G}$. If $G' = \bigcap_{j=1}^{n} G_j = \bigcap_{j \in J} G_j \neq \varnothing$ for all $J \subseteq \{1, 2, \ldots, n\}$ such that $|J| \geq n/w$, then $\mathscr{K}$ is a $(\mathscr{G}', w)$-KDP for $\mathscr{G}' = \mathscr{G} \cup \{G'\}$.*

Proof. From Corollary 4.2.3 it is sufficient to show that $\sum_{P \in F} \lambda_{G'}(P) < n$ for all $F \in 2^{\mathscr{P}}$ such that $1 \leq |F| \leq w$ and $G' \cap F = \varnothing$. Suppose that $F \in 2^{\mathscr{P}}$, $1 \leq |F| \leq w$ and $G' \cap F = \varnothing$. Consider $P \in F$, then $P \notin G'$ and since $G' = \bigcap_{j \in J} G_j$ for all $\varnothing \neq J \subseteq \{1, 2, \ldots, n\}$ such that $|J| \geq n/w$, $\lambda_{G'}(P) < n/w$. Now, since $1 \leq |F| \leq w$, $\sum_{P \in F} \lambda(P) < w(n/w) = n$. □

We demonstrate the effect of Corollary 4.2.4 in the following example.

Example 4.2.1. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be any finite incidence structure represented by the following 4×3 binary matrix.

$$\begin{array}{cccc} & x_1 & x_2 & x_3 \\ P_1 & 0 & 0 & 1 \\ P_2 & 0 & 1 & 0 \\ P_3 & 1 & 0 & 0 \\ P_4 & 1 & 1 & 1 \end{array}$$

Then, $\mathscr{K}$ is a $(\mathscr{G}, 2)$-KDP where, $\mathscr{G} = \big\{\{P_3, P_4\}, \{P_2, P_4\}, \{P_1, P_4\}\big\}$. In fact, one can check that $\mathscr{K}$ is a $(\mathscr{G}, 3)$-KDP.

Now, let $G_1 = \{P_3, P_4\}, G_2 = \{P_2, P_4\}$ and $G_3 = \{P_1, P_4\}$. Then, $G' = \bigcap_{j=1}^{3} G_j = \{P_4\} = \bigcap_{j \in J} G_j$ for $J \subseteq \{1, 2, 3\}$ such that $|J| \geq 3/2$. Therefore, $\mathscr{K}$ is a $(\mathscr{G}', 2)$-KDP, where $\mathscr{G}' = \big\{\{P_3, P_4\}, \{P_2, P_4\}, \{P_1, P_4\}, \{P_4\}\big\}$. Note however, that $\mathscr{K}$ is not a $(\mathscr{G}', 3)$-KDP since $\bigcap_{P \in G'} (P) = (P_4) = \bigcup_{P \in F} (P)$, where $F = \{P_1, P_2, P_3\}$.

In order to be more precise about the meaning of the largest possible set of privileged subsets with respect to a predefined set of forbidden subsets, we introduce the following definition.

Definition 4.2.5. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{F}$ be a family of non-empty subsets of $\mathscr{P}$. Let X be the collection of all families $\mathscr{G}$ of subsets of $\mathscr{P}$ such that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP, and let "$\leq$" be the partial order on X defined by $\mathscr{G}' \leq \mathscr{G}$ if, and only if, $\mathscr{G}' \subseteq \mathscr{G}$. From Proposition 3.1.4 we know that X is closed under finite unions. Therefore, $\bigcup_{\mathscr{G} \in X} \mathscr{G} \in X$ and is clearly the largest element in $(X, \leq)$, which we denote by $\mathscr{G}_{(\mathscr{K}, \mathscr{F})}$ and refer to as the* ***largest $\mathscr{G}$ for $\mathscr{F}$*** *with respect to $\mathscr{K}$.*

When the context is clear, we can refer to $\mathscr{G}_{(\mathscr{K}, \mathscr{F})}$, less formally, as the *largest $\mathscr{G}$*.

We now give another description of the largest $\mathscr{G}$, which follows directly from Definition 3.1.1, by taking all subsets of points and removing those that fail the security condition.

Observation 4.2.6. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{F}$ be a family of non-empty subsets of $\mathscr{P}$, then*

$$\mathscr{G}_{(\mathscr{K},\mathscr{F})} = \left[2^{\mathscr{P}} \setminus \{\varnothing\}\right] \setminus \left\{G \in 2^{\mathscr{P}} : \exists F \in \mathscr{F}, \bigcap_{P \in G} (P) \subseteq \bigcup_{Q \in F} (Q) \text{ and } G \cap F = \varnothing\right\}.$$

We note that if $\mathscr{F} = \{F \in 2^{\mathscr{P}} : 1 \leq |F| \leq w\}$, then we can relabel $\mathscr{G}_{(\mathscr{K},\mathscr{F})}$ as $\mathscr{G}_{(\mathscr{K},w)}$. If we restrict ourselves to $(\mathscr{G}, 1)$-KDPs, then we get the following, more concrete description of the largest $\mathscr{G}$.

Theorem 4.2.7. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure, then*

$$\mathscr{G}_{(\mathscr{K},1)} = \left\{ \bigcap_{x \in J} (x) : J \subseteq \mathscr{B} \text{ and } \bigcap_{x \in J} (x) \neq \varnothing \right\}.$$

Proof. We know from Theorem 4.2.1 and Remark 4.2.2 that $\mathscr{K}$ is a $(\mathscr{G}_{(\mathscr{K},1)}, 1)$-KDP, so it only remains to show that $\mathscr{G}_{(\mathscr{K},1)}$ is the largest $\mathscr{G}$ for $\mathscr{F} = \{F \in 2^{\mathscr{P}} : |F| = 1\}$ with respect to $\mathscr{K}$.
Let $\mathscr{G}$ be a family of non-empty subsets of $\mathscr{P}$ such that $\mathscr{K}$ is a $(\mathscr{G}, 1)$-KDP. Then take any $G \in \mathscr{G}$; either $G = \mathscr{P}$ or $G \neq \mathscr{P}$. If $G = \mathscr{P}$, then $G \in \mathscr{G}_{(\mathscr{K},1)}$ since $\bigcap_{x \in \varnothing} (x) = \mathscr{P}$. If $G \neq \mathscr{P}$, let $J = \bigcap_{P \in G} (P)$. We know that $J \neq \varnothing$ since $\mathscr{K}$ is a $(\mathscr{G}, 1)$-KDP. Now define $G' = \bigcap_{x \in J} (x)$. Clearly, $\varnothing \neq G \subseteq G'$ and so $G' \in \mathscr{G}_{(\mathscr{K},1)}$. We claim that $G = G'$. Suppose, in order to obtain a contradiction, that $G \neq G'$. Then, there exists a $Q \in G' \setminus G$. Since $Q \in G'$, $J \subseteq (Q)$ and so $\bigcap_{P \in G} (P) \subseteq (Q)$ which gives a contradiction since $\mathscr{K}$ is a $(\mathscr{G}, 1)$-KDP. Therefore, in both cases, $G \in \mathscr{G}_{(\mathscr{K},1)}$ and hence $\mathscr{G}_{(\mathscr{K},1)}$ is the largest $\mathscr{G}$. □

At this stage we are unable to give a good description of $\mathscr{G}_{(\mathscr{K},w)}$. However, from Corollary 4.2.4 we are able to show that certain subsets are always included in $\mathscr{G}_{(\mathscr{K},w)}$.

Observation 4.2.8. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure, $w \geq 1$ and $\varnothing \neq J \subseteq \mathscr{B}$. If $G' = \bigcap_{x \in J} (x) \neq \varnothing$ and $G' = \bigcap_{x \in J'} (x)$ for all $J' \subseteq J \subseteq \mathscr{B}$ such that $|J'| \geq |J|/w$, then $G' \in \mathscr{G}_{(\mathscr{K},w)}$.*

4.2.2 Largest Sets of Forbidden Subsets

In the same way as for privileged subsets, we now consider how to maximise the size of the set of forbidden subsets. We begin by considering a $(\mathscr{G},\mathscr{F})$-KDP and attempting to add to the set of forbidden subsets whilst only having a small measured impact on the set of privileged subsets. The proof of the following theorem is analogous to that of Theorem 4.2.1.

Theorem 4.2.9. *Suppose that a finite incidence structure $\mathscr{K}=(\mathscr{P},\mathscr{B},\mathscr{I})$ is a $(\mathscr{G},\mathscr{F})$-KDP. If $F_1,F_2,\ldots,F_n\in\mathscr{F}$ and $F'=\bigcap_{j=1}^{n}F_j\neq\varnothing$, then $\mathscr{K}$ is a $(\mathscr{G}',\mathscr{F}')$-KDP for*

$$\begin{gathered}\mathscr{G}'=\{G\in\mathscr{G}: G\cap F_j=\varnothing \text{ for some } 1\leq j\leq n \text{ or } G\cap F'\neq\varnothing\}\\ \text{and}\quad \mathscr{F}'=\mathscr{F}\cup\{F'\}.\end{gathered}$$

If the set of privileged subsets consists of all the singletons, then we have the following interesting special case.

Remark 4.2.10. In Theorem 4.2.9, if $\mathscr{G}=\{G\in 2^{\mathscr{P}}:|G|=1\}$, then $\mathscr{G}'=\mathscr{G}$.

From Theorem 4.2.9 we can extract a more amenable result for extending the set of forbidden subsets without affecting the set of privileged subsets.

Corollary 4.2.11. *Suppose that a finite incidence structure $\mathscr{K}=(\mathscr{P},\mathscr{B},\mathscr{I})$ is a $(\mathscr{G},\mathscr{F})$-KDP where $F_1,F_2,\ldots,F_n\in\mathscr{F}$ and $F'=\bigcap_{j=1}^{n}F_j\neq\varnothing$. Also, for each $P\in\mathscr{P}$ suppose that $\lambda_{F'}(P)=\big|\{j\in\{1,2,\ldots,n\}:P\in F_j\}\big|$. If $\sum_{P\in G}\lambda_{F'}(P)<n$ for each $G\in\mathscr{G}$ such that $G\cap F'=\varnothing$, then $\mathscr{K}$ is a $(\mathscr{G},\mathscr{F}')$-KDP for $\mathscr{F}'=\mathscr{F}\cup\{F'\}$.*

We now consider the special case of $(t,\mathscr{F})$-KDPs.

Corollary 4.2.12. *Suppose that a finite incidence structure $\mathscr{K}=(\mathscr{P},\mathscr{B},\mathscr{I})$ is a $(t,\mathscr{F})$-KDP for $t\geq 1$ and suppose that $F_1,F_2,\ldots,F_n\in\mathscr{F}$. If $F'=\bigcap_{j=1}^{n}F_j=\bigcap_{j\in J}F_j\neq\varnothing$ for all $\varnothing\neq J\subseteq\{1,2,\ldots,n\}$ such that $|J|\geq n/t$, then $\mathscr{K}$ is a $(t,\mathscr{F}')$-KDP for $\mathscr{F}'=\mathscr{F}\cup\{F'\}$.*

In the same way as Definition 4.2.5, we now precisely define the largest possible set of forbidden subsets with respect to a given set of privileged subsets.

Definition 4.2.13. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{G}$ be a family of non-empty subsets of $\mathscr{P}$. Let Y be the collection of all families $\mathscr{F}$ of subsets of $\mathscr{P}$ such that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP, and let "$\leq$" be the partial order on Y defined by $\mathscr{F}' \leq \mathscr{F}$ if, and only if, $\mathscr{F}' \subseteq \mathscr{F}$. From Proposition 3.1.5 we know that Y is closed under finite unions. Therefore, $\bigcup_{\mathscr{F} \in Y} \mathscr{F} \in Y$ and is clearly the largest element in $(Y, \leq)$, which we denote by $\mathscr{F}_{(\mathscr{K},\mathscr{G})}$ and refer to as the* ***largest $\mathscr{F}$ for $\mathscr{G}$*** *with respect to $\mathscr{K}$.*

When the context is clear, we can refer to $\mathscr{F}_{(\mathscr{K},\mathscr{G})}$, less formally, as *the largest $\mathscr{F}$*.

We now give another description of the largest $\mathscr{F}$ which follows directly from Definition 3.1.1, by taking all subsets of points and removing those that fail the security condition.

Observation 4.2.14. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and $\mathscr{G}$ be a family of non-empty subsets of $\mathscr{P}$, then*

$$\mathscr{F}_{(\mathscr{K},\mathscr{G})} = \left[2^{\mathscr{P}} \setminus \{\varnothing\}\right] \setminus \left\{F \in 2^{\mathscr{P}} : \exists G \in \mathscr{G}, \bigcap_{P \in G} (P) \subseteq \bigcup_{Q \in F} (Q) \text{ and } G \cap F = \varnothing\right\}.$$

Note that if $\mathscr{G} = \{G \in 2^{\mathscr{P}} : 1 \leq |G| \leq t\}$, then we can relabel $\mathscr{F}_{(\mathscr{K},\mathscr{G})}$ as $\mathscr{F}_{(\mathscr{K},t)}$.

In a similar way to Theorem 4.2.7, if we restrict ourselves to $(1, \mathscr{F})$-KDPs, then we get the following, more concrete description of the largest $\mathscr{F}$.

Theorem 4.2.15. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure, then*

$$\mathscr{F}_{(\mathscr{K},1)} = \left\{\bigcap_{x \in J} [\mathscr{P} \setminus (x)] : J \subseteq \mathscr{B} \text{ and } \bigcap_{x \in J} [\mathscr{P} \setminus (x)] \neq \varnothing\right\}.$$

Proof. We already know from Theorem 4.2.9 and Remark 4.2.10 that $\mathscr{K}$ is a $(1, \mathscr{F}_{(\mathscr{K},1)})$-KDP, so it only remains to show that $\mathscr{F}_{(\mathscr{K},1)}$ is the largest $\mathscr{F}$ for $\mathscr{G} = \{G \in 2^{\mathscr{P}} : |G| = 1\}$ with respect to $\mathscr{K}$.

Let $\mathscr{F}$ be a family of non-empty subsets of $\mathscr{P}$ such that $\mathscr{K}$ is a $(1, \mathscr{F})$-KDP. Then take any $F \in \mathscr{F}$; either $F = \mathscr{P}$ or $F \neq \mathscr{P}$. If $F = \mathscr{P}$, then $F \in \mathscr{F}_{(\mathscr{K},1)}$ since $\bigcap_{x \in \varnothing}[\mathscr{P} \setminus (x)] = \mathscr{P}$. If $F \neq \mathscr{P}$, let $J = \bigcap_{Q \in F}[\mathscr{B} \setminus (Q)]$. We know that $J \neq \varnothing$ since $\mathscr{K}$ is a $(1, \mathscr{F})$-KDP. Now define $F' = \bigcap_{x \in J}[\mathscr{P} \setminus (x)]$. Choose $Q \in F$, then for every $x \in J$,

$$x \in \mathscr{B} \setminus (Q) \Longrightarrow x \notin (Q) \Longrightarrow Q \notin (x) \Longrightarrow Q \in [\mathscr{P} \setminus (x)].$$

So, $F \subseteq [\mathscr{P} \setminus (x)]$ for every $x \in J$. Therefore, $\varnothing \neq F \subseteq \bigcap_{x \in J}[\mathscr{P} \setminus (x)] = F'$ and thus $F' \in \mathscr{F}_{(\mathscr{K},1)}$. We claim that $F = F'$. Suppose, in order to obtain a contradiction, that $F \neq F'$. Then, there exists a $P \in F' \setminus F$. Since $P \in F'$, $x \notin (P)$ for each $x \in J$ and so $J \cap (P) = \varnothing$, or equivalently $(P) \subseteq \mathscr{B} \setminus J$. Hence,

$$(P) \subseteq \mathscr{B} \setminus \left[\bigcap_{Q \in F}[\mathscr{B} \setminus (Q)]\right] = \bigcup_{Q \in F}(Q) \text{ (by De Morgan's Law)},$$

which gives a contradiction since $\mathscr{K}$ is a $(1, \mathscr{F})$-KDP. Therefore, in both cases, $F \in \mathscr{F}_{(\mathscr{K},1)}$ and hence $\mathscr{F}_{(\mathscr{K},1)}$ is the largest $\mathscr{F}$. □

As was the case with $\mathscr{G}_{(\mathscr{K},w)}$, we are unable to give a good description of $\mathscr{F}_{(\mathscr{K},t)}$. However, from Corollary 4.2.12 we are able to show that certain subsets are always included in $\mathscr{F}_{(\mathscr{K},t)}$.

Observation 4.2.16. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure, $t \geq 1$ and $\varnothing \neq J \subseteq \mathscr{B}$. If $F' = \bigcap_{x \in J}[\mathscr{P} \setminus (x)] \neq \varnothing$ and $F' = \bigcap_{x \in J'}[\mathscr{P} \setminus (x)]$ for all $J' \subseteq J \subseteq \mathscr{B}$ such that $|J'| \geq |J|/t$, then $F' \in \mathscr{F}_{(\mathscr{K},t)}$.*

4.2.3 Maximal $(\mathscr{G}, \mathscr{F})$-KDPs

We now return to the problem of finding the largest possible set of privileged and forbidden subsets that make a given incidence structure a $(\mathscr{G}, \mathscr{F})$-KDP.

To be more precise about this, we need to introduce a partial ordering on the set of privileged and forbidden subsets. In fact, we will consider a more general notion, namely that of a partial ordering on "extensions" of an existing set of privileged and forbidden subsets.

Definition 4.2.17. *Suppose that a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP. Let $X \subseteq 2^{\mathscr{P}} \times 2^{\mathscr{P}}$ be the set of all ordered pairs $(\mathscr{G}', \mathscr{F}') \in 2^{\mathscr{P}} \times 2^{\mathscr{P}}$ such that $\mathscr{K}$ is a $(\mathscr{G}', \mathscr{F}')$-KDP and $\mathscr{G} \subseteq \mathscr{G}'$ and $\mathscr{F} \subseteq \mathscr{F}'$. Let " $\leq$ " be the partial order on X defined by $(\mathscr{G}'', \mathscr{F}'') \leq (\mathscr{G}', \mathscr{F}')$ if $\mathscr{G}'' \subseteq \mathscr{G}'$ and $\mathscr{F}'' \subseteq \mathscr{F}'$. Then, the largest $(\mathscr{G}', \mathscr{F}')$-KDP with respect to $(X, \leq)$ (if it exists) will be called the* ***largest $(\mathscr{G}', \mathscr{F}')$-KDP for $\mathscr{G}$ and $\mathscr{F}$*** *with respect to $\mathscr{K}$.*

As alluded to at the start of this section, there is, in general, no largest element with respect to the partial ordering given above (see Example 4.2.2). The best that one can do is identify maximal elements with respect to this partial ordering. We will call such elements *maximal $(\mathscr{G}', \mathscr{F}')$-KDPs for $\mathscr{G}$ and $\mathscr{F}$ with respect to $\mathscr{K}$.*

Suppose that we are given a finite incidence structure $\mathscr{K}$ that is a $(\mathscr{G}, \mathscr{F})$-KDP. We can increase $\mathscr{G}$ to the largest $\mathscr{G}$ for $\mathscr{F}$ with respect to $\mathscr{K}$ and let $\mathscr{G}_1 = \mathscr{G}_{(\mathscr{K}, \mathscr{F})}$. Then, we can increase $\mathscr{F}$ to the largest $\mathscr{F}$ for $\mathscr{G}_1$ with respect to $\mathscr{K}$ and label this $\mathscr{F}_1$. In the same way (but in the other order) we can increase $\mathscr{F}$ to the largest $\mathscr{F}$ for $\mathscr{G}$ with respect to $\mathscr{K}$ and let $\mathscr{F}_2 = \mathscr{F}_{(\mathscr{K}, \mathscr{G})}$, then we can increase $\mathscr{G}$ to the largest $\mathscr{G}$ for $\mathscr{F}_2$ with respect to $\mathscr{K}$ and label this $\mathscr{G}_2$.

It is not difficult to show that both $(\mathscr{G}_1, \mathscr{F}_1)$ and $(\mathscr{G}_2, \mathscr{F}_2)$ are maximal with respect to the partial ordering in Definition 4.2.17. So, we now have two potentially distinct maximal $(\mathscr{G}', \mathscr{F}')$-KDPs for $\mathscr{G}$ and $\mathscr{F}$ with respect to $\mathscr{K}$. The following example demonstrates that, in general, these maximal $(\mathscr{G}', \mathscr{F}')$-KDPs are distinct. This in turn shows that there is, in general, no largest $(\mathscr{G}', \mathscr{F}')$-KDP for $\mathscr{G}$ and $\mathscr{F}$ with respect to a given incidence structure $\mathscr{K}$.

Example 4.2.2. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be any finite incidence structure such that $\mathscr{K}$ is not a $(2^{\mathscr{P}} \setminus \{\varnothing\}, 2^{\mathscr{P}} \setminus \{\varnothing\})$-KDP and let $\mathscr{G} = \varnothing$ and $\mathscr{F} = \varnothing$, then $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP. We can show that $\mathscr{G}_1 = \mathscr{G}_{(\mathscr{K}, \mathscr{F})} = 2^{\mathscr{P}} \setminus \{\varnothing\}$, in which case the largest $\mathscr{F}$ for $\mathscr{G}_1$ with respect to $\mathscr{K}$, (denoted $\mathscr{F}_1$) is restricted by the incidence structure and is not all of $2^{\mathscr{P}} \setminus \{\varnothing\}$. Also, $\mathscr{F}_2 = \mathscr{F}_{(\mathscr{K}, \mathscr{G})} = 2^{\mathscr{P}} \setminus \{\varnothing\}$, in which case the largest $\mathscr{G}$ for $\mathscr{F}_2$ with respect to $\mathscr{K}$, (denoted $\mathscr{G}_2$) is restricted by the incidence structure and is not all of $2^{\mathscr{P}} \setminus \{\varnothing\}$.

That is, for almost all incidence structures, $\mathscr{G}_1 \neq \mathscr{G}_2$ and/or $\mathscr{F}_1 \neq \mathscr{F}_2$ and we may have many distinct maximal $(\mathscr{G}', \mathscr{F}')$-KDPs, with no largest one.

Chapter 5

Constructions

The construction of "good"generalised Key Distribution Patterns is an important area of investigation. There are three approaches when it comes to constructing $(\mathscr{G}, \mathscr{F})$-KDPs. The first approach is to take existing $(\mathscr{G}, \mathscr{F})$-KDPs and construct new $(\mathscr{G}, \mathscr{F})$-KDPs from them. Mitchell and Piper use this approach extensively in [60] and present several constructions. In Section 5.1 and Section 5.2 we will generalise some of Mitchell and Piper's constructions (from $(2, w)$-KDPs to $(\mathscr{G}, \mathscr{F})$-KDPs) and use definitions and results from design theory in order to present some new constructions of $(\mathscr{G}, \mathscr{F})$-KDPs from existing $(\mathscr{G}, \mathscr{F})$-KDPs.

The second approach to $(\mathscr{G}, \mathscr{F})$-KDP constructions is to construct $(\mathscr{G}, \mathscr{F})$-KDPs directly from other mathematical objects. As mentioned in Section 3.3, a number of authors have used combinatorial objects in order to construct (t, w)-KDPs. O'Keefe [63, 64] and Rinaldi [74], used special finite geometric structures, (more specifically *circle geometries* and *Minkowski planes*) in the construction of (t, w)-KDPs. Quinn [72] constructed (t, w)-KDPs from *conics* arising from finite *projective planes* and *affine planes.* Also, Lee, Stinson and VanTrung, [47, 48, 82, 84] used *design theory*, *graph theory*, *orthogonal* and *perpendicular arrays* to construct specific $(\mathscr{G}, \mathscr{F})$-KDPs with particular properties.

In Section 5.3 we present a family of constructions of $(\mathscr{G}, \mathscr{F})$-KDPs. These

$(\mathscr{G},\mathscr{F})$-KDPs are constructed directly using a discrete analogue of convexity. Although this is our only direct construction method, it can be used to give many different families of $(\mathscr{G},\mathscr{F})$-KDPs and can be generalised, to give many more constructions.

We finally note the third approach to $(\mathscr{G},\mathscr{F})$-KDP constructions. This third approach is the use of probabilistic techniques. In [26], Dyer *et al.* give non-constructive existence results for (t,w)-KDPs. However, we do not pursue the probabilistic approach in this thesis, instead we shall restrict ourselves to deterministic constructions.

The main results in the chapter are:

1. Theorem 5.1.12 - In this theorem we characterise when an incidence structure is a $(\mathscr{G},\mathscr{F})$-KDP in terms of its internal structures.

2. Theorem 5.1.25 - In this theorem we correct Mitchell and Piper's result [60, Lemma 3.4] and characterise when an incidence structure is a $(\mathscr{G},\mathscr{F})$-KDP in terms of its external structures.

3. Theorem 5.1.31 - In this theorem we show that the complement of a $(\mathscr{G},\mathscr{F})$-KDP is a $(\mathscr{F},\mathscr{G})$-KDP. This simple, yet powerful result proves to be useful in Chapter 6, when calculating bounds for $(\mathscr{G},\mathscr{F})$-KDPs.

4. Theorem 5.3.7 - In this theorem we construct a family of $(\mathscr{G},\mathscr{F})$-KDPs directly from a finite convex structure. From this construction we are able to precisely calculate $|\mathscr{G}|$, $|\mathscr{F}|$ and the block size. We also suggest a generalisation that will potentially give rise to many more such families of $(\mathscr{G},\mathscr{F})$-KDPs.

5.1 Constructions from a Single KDP

If $\mathscr{K}$ is a finite incidence structure, then there are several established ways in which $\mathscr{K}$ can be used to construct new incidence structures. For example, internal, external, complement and dual structures. In this section we will use some definitions and results from [38], in order to investigate the internal structure, the external structure, the complement and the dual of an existing $(\mathscr{G}, \mathscr{F})$-KDP. However, first we shall consider two general, yet simple, constructions.

Our first theorem takes an existing $(\mathscr{G}, \mathscr{F})$-KDP and constructs a new $(\mathscr{G}, \mathscr{F}')$-KDP with more forbidden subsets.

Theorem 5.1.1. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then for each $n \in \mathbb{N}$, there exists a finite incidence structure $\mathscr{K}_n = (\mathscr{P}_n, \mathscr{B}_n, \mathscr{I}_n)$ with $\mathscr{P}_n = \mathscr{P}$, and $|\mathscr{B}_n| \leq \sum_{j=1}^{m} \binom{|\mathscr{B}|}{j}$ where $m = \min\{n, |\mathscr{B}|\}$, such that $\mathscr{K}_n$ is a $(\mathscr{G}, \mathscr{F}_n)$-KDP where*

$$\mathscr{F}_n = \Big\{ \bigcup_{1 \leq j \leq n} F_j : F_j \in \mathscr{F} \textit{ for } 1 \leq j \leq n \Big\}.$$

Proof. Let $\mathscr{K}^S = (\mathscr{P}^S, \mathscr{B}^S, \mathscr{I}^S)$ be the standard representation of $\mathscr{K}$. Then, from Corollary 3.4.4 we know that $\mathscr{K}^S$ is a $(\mathscr{G}, \mathscr{F})$-KDP. Let $n \in \mathbb{N}$ and define $\mathscr{P}_n = \mathscr{P}$ and

$$\mathscr{B}_n = \left\{ \bigcap_{j=1}^{m} B_j : B_j \in \mathscr{B}^S \text{ for } 1 \leq j \leq m \text{ and } \bigcap_{j=1}^{m} B_j \neq \varnothing \right\}.$$

Also define $\mathscr{I}_n \subseteq \mathscr{P}_n \times \mathscr{B}_n$ by, $(P, B) \in \mathscr{I}_n$ if, and only if, $P \in B$.

We claim that the incidence structure $\mathscr{K}_n = (\mathscr{P}_n, \mathscr{B}_n, \mathscr{I}_n)$ is a $(\mathscr{G}, \mathscr{F}_n)$-KDP where

$$\mathscr{F}_n = \Big\{ \bigcup_{1 \leq j \leq n} F_j : F_j \in \mathscr{F} \text{ for } 1 \leq j \leq n \Big\}.$$

To prove this, suppose that $G \in \mathscr{G}$, $F \in \mathscr{F}_n$ and $G \cap F = \varnothing$. Since $F \in \mathscr{F}_n$ there exists $F_j \in \mathscr{F}$, for $1 \leq j \leq n$, such that $F = \bigcup_{j=1}^{n} F_j$.

Now, since $\mathscr{K}^S$ is a $(\mathscr{G},\mathscr{F})$-KDP, for each $1 \leq j \leq n$ there exists a block $B_j \in \mathscr{B}^S$ such that $B_j \in \bigcap_{P\in G}(P) \setminus \bigcup_{Q\in F_j}(Q)$, that is, $G \subseteq B_j$ and $B_j \cap F_j = \varnothing$. Let $B = \bigcap_{j=1}^{n} B_j \in \mathscr{B}_n$. Then, $G \subseteq \bigcap_{j=1}^{n} B_j = B$ and

$$B \cap F = B \cap \left[\bigcup_{j=1}^{n} F_j\right] = \bigcup_{j=1}^{n}[F_j \cap B] \subseteq \bigcup_{j=1}^{n}[F_j \cap B_j] = \varnothing.$$

Therefore, $B \in \bigcap_{P\in G}(P) \setminus \bigcup_{Q\in F}(Q)$ and hence $\mathscr{K}_n$ is a $(\mathscr{G},\mathscr{F}_n)$-KDP. □

An immediate consequence of this theorem is the following.

Corollary 5.1.2. *If a finite incidence structure $\mathscr{K} = (\mathscr{P},\mathscr{B},\mathscr{I})$ is a $(\mathscr{G},w)$-KDP, then for each $n < |\mathscr{P}|/w$, there exists a finite incidence structure $\mathscr{K}_n = (\mathscr{P}_n,\mathscr{B}_n,\mathscr{I}_n)$ with $\mathscr{P}_n = \mathscr{P}$ and $|\mathscr{B}_n| \leq \sum_{j=1}^{m}\binom{|\mathscr{B}|}{j}$ where $m = \min\{n, |\mathscr{B}|\}$, such that $\mathscr{K}_n$ is a $(\mathscr{G},wn)$-KDP.*

Remark 5.1.3. If $\mathscr{K} = (\mathscr{P},\mathscr{B},\mathscr{I})$ is a $(\mathscr{G},1)$-KDP, then using Corollary 5.1.2 we can construct an incidence structure $\mathscr{K}' = (\mathscr{P},\mathscr{B}',\mathscr{I}')$ such that $\mathscr{K}'$ is a $(\mathscr{G},2)$-KDP and $|\mathscr{B}'| \leq \binom{|\mathscr{B}|+1}{2}$.

The following theorem is similar to Theorem 5.1.1, but takes an existing $(\mathscr{G},\mathscr{F})$-KDP and constructs a new $(\mathscr{G}',\mathscr{F})$-KDP with more privileged subsets.

Theorem 5.1.4. *If a finite incidence structure $\mathscr{K} = (\mathscr{P},\mathscr{B},\mathscr{I})$ is a $(\mathscr{G},\mathscr{F})$-KDP, then for each $n \in \mathbb{N}$, there exists a finite incidence structure $\mathscr{K}_n = (\mathscr{P}_n,\mathscr{B}_n,\mathscr{I}_n)$ with $\mathscr{P}_n = \mathscr{P}$, and $|\mathscr{B}_n| \leq \sum_{j=1}^{m}\binom{|\mathscr{B}|}{j}$ where $m = \min\{n, |\mathscr{B}|\}$, such that $\mathscr{K}_n$ is a $(\mathscr{G}_n,\mathscr{F})$-KDP where*

$$\mathscr{G}_n = \Big\{ \bigcup_{1\leq j\leq n} G_j : G_j \in \mathscr{G} \text{ for } 1 \leq j \leq n \Big\}.$$

Proof. Let $\mathscr{K}^S = (\mathscr{P}^S,\mathscr{B}^S,\mathscr{I}^S)$ be the standard representation of $\mathscr{K}$. Then, from Corollary 3.4.4 we know that $\mathscr{K}^S$ is a $(\mathscr{G},\mathscr{F})$-KDP.
Let $n \in \mathbb{N}$ and define $\mathscr{P}_n = \mathscr{P}$ and

$$\mathscr{B}_n = \left\{ \bigcup_{j=1}^{m} B_j : B_j \in \mathscr{B}^S \text{ for } 1 \leq j \leq m \text{ and } \bigcup_{j=1}^{m} B_j \neq \varnothing \right\}.$$

Also define $\mathscr{I}_n \subseteq \mathscr{P}_n \times \mathscr{B}_n$ by, $(P, B) \in \mathscr{I}_n$ if, and only if, $P \in B$.

We claim that the incidence structure $\mathscr{K}_n = (\mathscr{P}_n, \mathscr{B}_n, \mathscr{I}_n)$ is a $(\mathscr{G}_n, \mathscr{F})$-KDP where $\mathscr{G}_n = \{\bigcup_{1 \leq j \leq n} G_j : G_j \in \mathscr{G} \text{ for } 1 \leq j \leq n\}$. To prove this, suppose that $G \in \mathscr{G}_n$, $F \in \mathscr{F}$ and $G \cap F = \varnothing$. Since $G \in \mathscr{G}_n$ there exists $G_j \in \mathscr{G}$, for $1 \leq j \leq n$, such that $G = \bigcup_{j=1}^{n} G_j$ and since $G \cap F = \varnothing$, $G_j \cap F = \varnothing$, for $1 \leq j \leq n$.

Now, since $\mathscr{K}^S$ is a $(\mathscr{G}, \mathscr{F})$-KDP, for each $1 \leq j \leq n$ there exists a block $B_j \in \mathscr{B}^S$ such that $B_j \in \bigcap_{P \in G_j}(P) \setminus \bigcup_{Q \in F}(Q)$, that is, $G_j \subseteq B_j$ and $B_j \cap F = \varnothing$. Let $B = \bigcup_{j=1}^{n} B_j \in \mathscr{B}_n$. Then,

$$G = \bigcup_{j=1}^{n} G_j \subseteq \bigcup_{j=1}^{n} B_j = B \text{ and } B \cap F = \bigcup_{j=1}^{n} B_j \cap F = \varnothing.$$

Therefore, $B \in \bigcap_{P \in G}(P) \setminus \bigcup_{Q \in F}(Q)$ and hence $\mathscr{K}_n$ is a $(\mathscr{G}_n, \mathscr{F})$-KDP. □

Not surprisingly this theorem has consequences for $(t, \mathscr{F})$-KDPs.

Corollary 5.1.5. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(t, \mathscr{F})$-KDP, then for each $n < |\mathscr{P}|/t$, there exists a finite incidence structure $\mathscr{K}_n = (\mathscr{P}_n, \mathscr{B}_n, \mathscr{I}_n)$ with $\mathscr{P}_n = \mathscr{P}$ and $|\mathscr{B}_n| \leq \sum_{j=1}^{m} \binom{|\mathscr{B}|}{j}$ where $m = \min\{n, |\mathscr{B}|\}$, such that $\mathscr{K}_n$ is a $(tn, \mathscr{F})$-KDP.*

Remark 5.1.6. If $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(1, \mathscr{F})$-KDP, then using Corollary 5.1.5 we can construct an incidence structure $\mathscr{K}' = (\mathscr{P}, \mathscr{B}', \mathscr{I}')$ such that $\mathscr{K}'$ is a $(2, \mathscr{F})$-KDP and $|\mathscr{B}'| \leq \binom{|\mathscr{B}|+1}{2}$.

The constructions given so far are quite general, as they contain no constraints at all, on either the set of privileged subsets, or the set of forbidden subsets. The price one pays for this generality is that the number of blocks required for their construction is not as small as could be achieved if the families of privileged and forbidden subsets had more structure. However, the constructions in this section may still prove to be useful. For example, in Section 7.2, we are able to use Theorem 5.1.1 in order to estimate lower bounds on the number of blocks in “reasonably” general $(\mathscr{G}, \mathscr{F})$-KDPs.

5.1.1 Internal Structures

We begin with the following fundamental definition.

Definition 5.1.7. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. Then, for each point $P \in \mathscr{P}$ we define $\mathscr{K}_P$, the* ***internal structure*** *of $\mathscr{K}$ at P, to be $\mathscr{K}_P = (\mathscr{P}_P, \mathscr{B}_P, \mathscr{I}_P)$, where*

$$\mathscr{B}_P = (P),\ \ \mathscr{P}_P = (\mathscr{B}_P) \setminus \{P\} \ \textit{and}$$

$$\textit{for any } Q \in \mathscr{P}_P \textit{ and } x \in \mathscr{B}_P,\ (Q, x) \in \mathscr{I}_P \textit{ if, and only if, } (Q, x) \in \mathscr{I}.$$

That is, the point set of the internal structure of a finite incidence structure $\mathscr{K}$ at a point P consists of all the points incident with any block that is incident with P, except the point P itself. The block sets consists of all the blocks incident with P and the incidence relation follows naturally from the incidence structure $\mathscr{K}$.

For convenience, we introduce some new notation representing the blocks incident with a point and the points incident with a block in an internal structure. For a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ and a point $P \in \mathscr{P}$ we define $(Q)_P = (Q) \cap \mathscr{B}_P$ and $(x)_P = (x) \cap \mathscr{P}_P$ for every $Q \in \mathscr{P}_P$ and every $x \in \mathscr{B}_P$.

We demonstrate the definition of an internal structure with the following illustrative example.

Example 5.1.1. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be an incidence structure determined by the following binary matrix:

$$\begin{array}{cccccc}
 & x_1 & x_2 & x_3 & x_4 & x_5 \\
P_1 & 0 & 0 & 1 & 0 & 1 \\
P_2 & 0 & 1 & 1 & 1 & 0 \\
P_3 & 1 & 0 & 1 & 1 & 0 \\
P_4 & 1 & 1 & 0 & 1 & 0 \\
P_5 & 1 & 1 & 1 & 0 & 1
\end{array}$$

The matrix representation of the internal structure of $\mathscr{K}$ at point P_1 is:

$$\begin{array}{ccc} & x_3 & x_5 \\ P_2 & 1 & 0 \\ P_3 & 1 & 0 \\ P_5 & 1 & 1 \end{array}$$

The following result from [38] shows that the internal structure of a $t-(v,k,\lambda)$ design is again a design.

Result 5.1.8. *Let $\mathscr{K}$ be a $t-(v,k,\lambda)$ design with $t \geq 2$ and let P be a point of $\mathscr{K}$, then $\mathscr{K}_P$ is a $(t-1)-(v-1,k-1,\lambda)$ design.*

The corresponding result for $(\mathscr{G},\mathscr{F})$-KDPs is given next.

Theorem 5.1.9. *If a finite incidence structure $\mathscr{K}=(\mathscr{P},\mathscr{B},\mathscr{I})$ is a $(\mathscr{G},\mathscr{F})$-KDP, then for each $P \in \mathscr{P}$, $\mathscr{K}_P= (\mathscr{P}_P,\mathscr{B}_P,\mathscr{I}_P)$ is a $(\mathscr{G}_P,\mathscr{F}_P)$-KDP, where*

$$\mathscr{G}_P = \{G \setminus \{P\} : P \in G \in \mathscr{G} \text{ and } \varnothing \neq G \setminus \{P\} \subseteq \mathscr{P}_P\} \text{ and}$$

$$\mathscr{F}_P = \{F \cap \mathscr{P}_P : P \notin F \in \mathscr{F} \text{ and } \mathscr{P}_P \cap F \neq \varnothing\}.$$

Proof. Suppose that $\mathscr{K}$ is a $(\mathscr{G},\mathscr{F})$-KDP and $P \in \mathscr{P}$. Consider $G_P \in \mathscr{G}_P$ and $F_P \in \mathscr{F}_P$, such that $G_P \cap F_P = \varnothing$. Then $G_P = G \setminus \{P\} \subseteq P_P$ for some $P \in G \in \mathscr{G}$ and $F_P = F \cap \mathscr{P}_P \neq \varnothing$ for some $P \notin F \in \mathscr{F}$. Now, since $P \notin F$ and $G_P \cap F_P = \varnothing$, $G \cap F = \varnothing$. Therefore, if $\bigcap\limits_{Q_1 \in G_P} (Q_1)_P \subseteq \bigcup\limits_{Q_2 \in F_P} (Q_2)_P$, then

$$\begin{aligned} \bigcap_{Q_1 \in G} (Q_1) &= \bigcap_{Q_1 \in G_P} (Q_1) \cap (P) = \bigcap_{Q_1 \in G_P} (Q_1)_P \\ &\subseteq \bigcup_{Q_2 \in F_P} (Q_2)_P \subseteq \bigcup_{Q_2 \in F} (Q_2)_P \subseteq \bigcup_{Q_2 \in F} (Q_2). \end{aligned}$$

This contradicts the fact that $\mathscr{K}$ is a $(\mathscr{G},\mathscr{F})$-KDP and hence $\mathscr{K}_P$ is a $(\mathscr{G}_P,\mathscr{F}_P)$-KDP. □

Note that, if we include the additional assumption in Theorem 5.1.9 that $|G| \geq 2$ and $\bigcap_{Q \in G}(Q) \neq \varnothing$ for all $G \in \mathscr{G}$, then our set of privileged subsets simplifies to $\mathscr{G}_P = \{G \setminus \{P\} : P \in G \in \mathscr{G}\}$.

We have the following corollary for the special case when $\mathscr{F}$ consists of all subsets of $\mathscr{P}$ of cardinality at most w. Corollary 5.1.10 will be used later, in the proof of Theorem 5.1.15.

Corollary 5.1.10. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP, then for each $P \in \mathscr{P}$, $\mathscr{K}_P = (\mathscr{P}_P, \mathscr{B}_P, \mathscr{I}_P)$ is a $(\mathscr{G}_P, w)$-KDP where $\mathscr{G}_P = \{G \setminus \{P\} : P \in G \in \mathscr{G}$ and $\varnothing \neq G \setminus \{P\} \subseteq \mathscr{P}_P\}$.*

Proof. This follows from Theorem 5.1.9, since if $\mathscr{F} = \{F \in 2^{\mathscr{P}} : 0 < |F| \leq w\}$, then for any $P \in \mathscr{P}$,
$\mathscr{F}_P = \{F \cap \mathscr{P}_P : P \notin F \in \mathscr{F}$ and $F \cap \mathscr{P} \neq \varnothing\} = \{F \in 2^{\mathscr{P}_P} : 0 < |F| \leq w\}$. □

In a similar way to Theorem 5.1.9, if we include an additional condition in Corollary 5.1.10 and specify that $2 \leq |G| < |\mathscr{P}|$ for all $G \in \mathscr{G}$, then our set of privileged subsets simplifies to $\mathscr{G}_P = \{G \setminus \{P\} : P \in G \in \mathscr{G}\}$.

A natural case of Corollary 5.1.10 is the situation when $\mathscr{G}$ consists of all the subsets of $\mathscr{P}$ of cardinality at most t.

Corollary 5.1.11. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a (t, w)-KDP with $2 \leq t \leq |\mathscr{P}| - w$, then for each $P \in \mathscr{P}$, $\mathscr{K}_P = (\mathscr{P}_P, \mathscr{B}_P, \mathscr{I}_P)$ is a $(t-1, w)$-KDP.*

Proof. This is a special case of Corollary 5.1.10.
For $\mathscr{G} = \{T \in 2^{\mathscr{P}} : 1 < |T| \leq t\}$ it follows that

$$\mathscr{G}_P = \{T' \in 2^{\mathscr{P}_P} : 0 < |T'| \leq t - 1\}, \text{ for any } P \in \mathscr{P}.$$

□

We can now obtain a characterisation for an incidence structure being a $(\mathscr{G}, \mathscr{F})$-KDP in terms of its internal structures.

Theorem 5.1.12. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{G}$ and $\mathscr{F}$ be families of non-empty subsets of $\mathscr{P}$ such that $|G| \geq 2$ and*

$\bigcap_{Q\in G}(Q) \neq \varnothing$ for all $G \in \mathscr{G}$. Then, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, for each $P \in \mathscr{P}$, $\mathscr{K}_P$= $(\mathscr{P}_P, \mathscr{B}_P, \mathscr{I}_P)$ is a $(\mathscr{G}_P, \mathscr{F}_P)$-KDP, where

$$\mathscr{G}_P = \{G \setminus \{P\} : P \in G \in \mathscr{G}\} \textit{ and}$$

$$\mathscr{F}_P = \{F \cap \mathscr{P}_P : P \notin F \in \mathscr{F} \textit{ and } \mathscr{P}_P \cap F \neq \varnothing\}.$$

Proof. It follows directly from Theorem 5.1.9 that if $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP then for each $P \in \mathscr{P}$, $\mathscr{K}_P$ is a $(\mathscr{G}_P, \mathscr{F}_P)$-KDP, so we shall consider the converse. In order to obtain a contradiction, suppose that $\mathscr{K}$ is not a $(\mathscr{G}, \mathscr{F})$-KDP. That is, suppose that there is some $G \in \mathscr{G}$ and some $F \in \mathscr{F}$ such that $G \cap F = \varnothing$ and $\bigcap_{Q_1\in G}(Q_1) \subseteq \bigcup_{Q_2\in F}(Q_2)$.

Fix some point $P \in G$, then note that:

1. $P \notin F$;

2. $G \setminus \{P\} \subseteq \mathscr{P}_P$, since $(P) \cap \bigcap_{Q\in G\setminus\{P\}}(Q) = \bigcap_{Q\in G}(Q) \neq \varnothing$;

3. $F \cap \mathscr{P}_P \neq \varnothing$, because of the following

$$\begin{aligned} \varnothing \neq \bigcap_{Q_1\in G}(Q_1) = (P) \cap \bigcap_{Q_1\in G}(Q_1) &\subseteq (P) \cap \bigcup_{Q_2\in F}(Q_2) \\ &\subseteq \bigcup_{Q_2\in F}\left[(Q_2) \cap (P)\right]. \end{aligned}$$

Therefore, if we set $G_P = G \setminus \{P\}$ and $F_P = F \cap \mathscr{P}_P$ then $G_P \in \mathscr{G}_P$, $F_P \in \mathscr{F}_P$ and

$$\begin{aligned} \bigcap_{Q_1\in G}(Q_1) \subseteq \bigcup_{Q_2\in F}(Q_2) \implies & \bigcap_{Q_1\in G}(Q_1) \cap (P) \subseteq \bigcup_{Q_2\in F}(Q_2) \cap (P) \\ & = \bigcup_{Q_2\in F_P}(Q_2) \cap (P) \quad (\text{since } F_P = F \cap \mathscr{P}_P) \\ \implies & \bigcap_{Q_1\in G\setminus\{P\}}(Q_1)_P \subseteq \bigcup_{Q_2\in F_P}(Q_2)_P \\ \implies & \bigcap_{Q_1\in G_P}(Q_1)_P \subseteq \bigcup_{Q_2\in F_P}(Q_2)_P. \end{aligned}$$

Hence, $\mathscr{K}_P$ is not a $(\mathscr{G}_P, \mathscr{F}_P)$-KDP and the proof is complete. □

Corollary 5.1.13 is the special case of Theorem 5.1.12 in the situation when $\mathscr{F}$ consists of all subsets of $\mathscr{P}$ of cardinality at most w.

Corollary 5.1.13. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{G}$ be a family of subsets of $\mathscr{P}$ such that $|G| \geq 2$ and $\bigcap_{Q \in G}(Q) \neq \varnothing$ for all $G \in \mathscr{G}$. Then $\mathscr{K}$ is a $(\mathscr{G}, w)$-KDP if, and only if, for each $P \in \mathscr{P}$, $\mathscr{K}_P$ is a $(\mathscr{G}_P, w)$-KDP for $\mathscr{G}_P = \{G \setminus \{P\} : P \in G \in \mathscr{G}\}$.*

Proof. Since $\mathscr{F} = \{F \in 2^{\mathscr{P}} : 0 < |F| \leq w\}$, it follows that

$$\mathscr{F}_P = \{F_P \in 2^{\mathscr{P}_P} : 0 < |F_P| \leq w\}, \text{ for any } P \in \mathscr{P}. \qquad \square$$

A natural case of Corollary 5.1.13 is the situation when $\mathscr{G}$ consists of all subsets of $\mathscr{P}$ of cardinality at most t.

Corollary 5.1.14. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure, let $2 \leq t < |\mathscr{P}|$ and let $w \leq |\mathscr{P}| - t$. If $\bigcap_{Q \in G}(Q) \neq \varnothing$ for each $G \in 2^{\mathscr{P}}$ with $|G| = t$, then, $\mathscr{K}$ is a (t, w)-KDP if, and only if, for each $P \in \mathscr{P}$, $\mathscr{K}_P$ is a $(t-1, w)$-KDP .*

Proof. Since $\mathscr{G} = \{G \in 2^{\mathscr{P}} : 0 < |G| \leq t\}$, it follows from Corollary 5.1.13 that $\mathscr{G}_P = \{G_P \in 2^{\mathscr{P}_P} : 0 < |G_P| \leq t - 1\}$, for any $P \in \mathscr{P}$. □

As an application of our results on internal structures we can deduce some crude estimates for the number of blocks incident with any point (that is, the number of subkeys held by any user).

Theorem 5.1.15. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP where $2 \leq |G| < |\mathscr{P}|$ for each $G \in \mathscr{G}$, then*

$$\log_2 |\{G \in \mathscr{G} : P \in G\}| < |(P)|, \textit{ for any } P \in \mathscr{P}.$$

Proof. Let $P \in \mathscr{P}$ and let $\mathscr{G}_P = \{G \setminus \{P\} \subseteq \mathscr{P}_P : P \in G \in \mathscr{G}\} = \{G \setminus \{P\} : P \in G \in \mathscr{G}\}$, since $\left[\bigcap_{Q \in G \setminus \{P\}}(Q)\right] \cap (P) = \bigcap_{Q \in G}(Q) \neq \varnothing$ for each $G \in \mathscr{G}$ containing P.

Then, by Corollary 5.1.10, $\mathscr{K}_P$ is a $(\mathscr{G}_P, w)$-KDP. Hence, by Remark 3.3.13, the mapping $G_P \mapsto \bigcap_{Q\in G_P}(Q)_P$, from $\mathscr{G}_P$ into non-empty subsets of $\mathscr{B}_P$, is 1-to-1. Therefore,

$$|\mathscr{G}_P| = \left| \left\{ \bigcap_{Q\in G} (Q)_P \in 2^{\mathscr{B}_P} \setminus \{\varnothing\} : G \in \mathscr{G}_P \right\} \right| \leq 2^{|\mathscr{B}_P|} - 1.$$

Hence, $\log_2 |\mathscr{G}_P| \leq \log_2 \left(2^{|\mathscr{B}_P|} - 1\right) < \log_2 \left(2^{|\mathscr{B}_P|}\right) = |\mathscr{B}_P| = |(P)|$. □

In Section 5.1.2 we combine Theorem 5.1.15 with Theorem 5.1.28, (a similar result for external structures) in order to estimate the number of blocks incident with each point of a $(\mathscr{G}, \mathscr{F})$-KDP. We then revisit this combined result in Chapter 6.

5.1.2 External Structures

Again, we begin with a fundamental definition.

Definition 5.1.16. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. Then, for each point $P \in \mathscr{P}$ we define $\mathscr{K}^P$, the* ***external structure*** *of $\mathscr{K}$ at P, to be $\mathscr{K}^P = (\mathscr{P}^P, \mathscr{B}^P, \mathscr{I}^P)$, where*

$$\mathscr{B}^P = \mathscr{B} \setminus (P),\ \ \mathscr{P}^P = (\mathscr{B}^P) \text{ and}$$

$$\text{for any } Q \in \mathscr{P}^P \text{ and } x \in \mathscr{B}^P,\ (Q,x) \in \mathscr{I}^P \text{ if, and only if, } (Q,x) \in \mathscr{I}.$$

That is, the point set of the external structure of a finite incidence structure $\mathscr{K}$ at a point P consists of all points incident with any block that is not incident with P. The block set consists of all the blocks not incident with the point P and the incidence relation follows naturally from the incidence structure $\mathscr{K}$.

As with internal structures, we introduce some new notation representing the blocks incident with a point and the points incident with a block in an external structure. For a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ and a point $P \in \mathscr{P}$ we define $(Q)^P = (Q) \cap \mathscr{B}^P$ and $(x)^P = (x) \cap \mathscr{P}^P$ for every $Q \in \mathscr{P}^P$ and every $x \in \mathscr{B}^P$.

We demonstrate this definition with the following illustrative example.

Example 5.1.2. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be an incidence structure determined by the following binary matrix:

$$\begin{array}{cccccc} & x_1 & x_2 & x_3 & x_4 & x_5 \\ P_1 & 0 & 0 & 1 & 0 & 1 \\ P_2 & 0 & 1 & 1 & 1 & 0 \\ P_3 & 1 & 0 & 1 & 1 & 0 \\ P_4 & 1 & 1 & 0 & 1 & 0 \\ P_5 & 1 & 1 & 1 & 0 & 1 \end{array}$$

The external structure of $\mathscr{K}$ at point P_1 is

$$\begin{array}{cccc} & x_1 & x_2 & x_4 \\ P_2 & 0 & 1 & 1 \\ P_3 & 1 & 0 & 1 \\ P_4 & 1 & 1 & 1 \\ P_5 & 1 & 1 & 0 \end{array}$$

The following result for external structures, taken from [38], is analogous to Result 5.1.8.

Result 5.1.17. *Let $\mathscr{K}$ be a $t-(v, k, \lambda)$ design with $t \geq 2$ and let P be a point of $\mathscr{K}$. Then $\mathscr{K}^P$ is a $(t-1)-(v-1, k, \lambda_{t-1}-\lambda)$ design, where $\lambda_{t-1} = \lambda\frac{(v-t+1)}{(k-t+1)}$.*

A similar result for key distribution patterns can be found in [60], where Mitchell and Piper state the following.

Result 5.1.18. [60, Lemma 3.4] Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. For $w \geq 2$, $\mathscr{K}$ is a $(2, w)$-KDP if and only if $\mathscr{K}^P$ is a $(2, w-1)$-KDP for every $P \in \mathscr{P}$.

Unfortunately, in the proof of Result 5.1.18, Mitchell and Piper assume that for a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ the point set of the external structure of $\mathscr{K}$, taken at any point $P \in \mathscr{P}$, is given by $\mathscr{P}^P = \mathscr{P} \setminus \{P\}$.

However, as can be seen by considering the external structure of $\mathscr{K}$ at the point P_5, in Example 5.1.2, this assumption is not true in general, for any incidence structure $\mathscr{K}$. In fact, Result 5.1.18 as stated, is false and the following example demonstrates this.

Example 5.1.3. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be an incidence structure determined by the following binary matrix:

$$\begin{array}{cccccccc}
 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 \\
P_1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
P_2 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
P_3 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
P_4 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
P_5 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}$$

In this example, $\mathscr{K}$ is not a $(2,2)$-KDP, (in fact, not even a $(1,1)$-KDP), however $\mathscr{K}^P$ is a $(2,1)$-KDP for every $P \in \mathscr{P}$.

Out of interest, we note that Example 5.1.3 is consistent with our earlier characterisation of an incidence structure being a $(\mathscr{G}, \mathscr{F})$-KDP in terms of its internal structures (Theorem 5.1.12). In fact, one can check that the internal structure of $\mathscr{K}$ at any of the points P_1, P_2, P_3 or P_4, fails to be a $(1,2)$-KDP.

We shall correct and generalise Result 5.1.18 for $(\mathscr{G}, \mathscr{F})$-KDPs. However, before we do this, we first make an observation involving Sperner systems.

Observation 5.1.19. *If $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a finite incidence structure such that for any two distinct points $P_1, P_2 \in \mathscr{P}$, $(P_1) \nsubseteq (P_2)$, (that is, $\{(P) : P \in \mathscr{P}\}$ forms a Sperner system over the set of all blocks) then $\mathscr{P}^P = \mathscr{P} \setminus \{P\}$ for every $P \in \mathscr{P}$.*

For some specific $(\mathscr{G}, \mathscr{F})$-KDPs, the family of subsets of blocks incident with each point in the point set will always form a Sperner System. In particular, we have the following remark.

Remark 5.1.20. It follows from Observation 5.1.19 that, if $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a (t, w)-KDP and $t \leq |\mathscr{P}| - w$, then $\{(P) : P \in \mathscr{P}\}$ forms a Sperner system and so $\mathscr{P}^P = \mathscr{P} \setminus \{P\}$ for every $P \in \mathscr{P}$.

Next, we shall consider a partial generalisation of Result 5.1.18. We delay our full generalisation until we have overcome some technical details.

Theorem 5.1.21. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then for each $P \in \mathscr{P}$, $\mathscr{K}^P = (\mathscr{P}^P, \mathscr{B}^P, \mathscr{I}^P)$ is a $(\mathscr{G}^P, \mathscr{F}^P)$-KDP where,*

$$\mathscr{G}^P = \{G \in \mathscr{G} : G \subseteq \mathscr{P}^P\} \text{ and}$$

$$\mathscr{F}^P = \{F \cap \mathscr{P}^P : P \in F \in \mathscr{F} \text{ and } F \cap \mathscr{P}^P \neq \varnothing\}.$$

Proof. Suppose, in order to obtain a contradiction, that for some $P \in \mathscr{P}$ there exists a $G' \in \mathscr{G}^P$ and an $F' \in \mathscr{F}^P$ such that $G' \cap F' = \varnothing$ and

$$\bigcap_{P' \in G'} (P')^P \subseteq \bigcap_{Q' \in F'} (Q')^P.$$

Now, by the definition of $\mathscr{F}^P$, there exists an $F \in \mathscr{F}$ such that $P \in F$ and $F' = F \cap \mathscr{P}^P$. Hence,

$$\begin{aligned} \bigcap_{P' \in G'} (P') &\subseteq \bigcap_{P' \in G'} \Big[[(P') \cap \mathscr{B}^P] \cup (P) \Big] = \left[\bigcap_{P' \in G'} (P') \cap \mathscr{B}^P \right] \cup (P) \\ &= \left[\bigcap_{P' \in G'} (P')^P \right] \cup (P) \subseteq \bigcup_{Q' \in F'} (Q')^P \cup (P) \subseteq \bigcup_{Q \in F} (Q). \end{aligned}$$

This contradicts the fact that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP, since $G' \cap F = \varnothing, G' \in \mathscr{G}$ and $F \in \mathscr{F}$, and the proof is complete. □

As before, with Corollary 5.1.10 we shall consider the special case when $\mathscr{F}$ consists of all the subsets of $\mathscr{P}$ of cardinality at most w.

Corollary 5.1.22. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP for $w \geq 2$, then for each $P \in \mathscr{P}$, $\mathscr{K}^P = (\mathscr{P}^P, \mathscr{B}^P, \mathscr{I}^P)$ is a $(\mathscr{G}^P, w-1)$-KDP, where $\mathscr{G}^P = \{G \in \mathscr{G} : G \subseteq \mathscr{P}^P\}$.*

Proof. This follows from Theorem 5.1.21. If $\mathscr{F} = \{F \in 2^{\mathscr{P}} : 0 < |F| \leq w\}$, then $\mathscr{F}^P = \{F^P \in 2^{\mathscr{P}^P} : 0 < |F^P| \leq w-1\}$, for any $P \in \mathscr{P}$. □

A natural case of Corollary 5.1.22 is the situation when $\mathscr{G}$ consists of all the subsets of $\mathscr{P}$ of cardinality at most t.

Corollary 5.1.23. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a (t,w)-KDP with $t \leq |\mathscr{P}| - w$ and $w \geq 2$, then for each $P \in \mathscr{P}$, $\mathscr{K}^P = (\mathscr{P}^P, \mathscr{B}^P, \mathscr{I}^P)$ is a $(t, w-1)$-KDP.*

Proof. This is a special case of Corollary 5.1.22.
For $\mathscr{G} = \{T \in 2^{\mathscr{P}} : 0 < |T| \leq t\}$ it follows that

$$\mathscr{G}^P = \{T' \in 2^{\mathscr{P}^P} : 0 < |T'| \leq t\}, \text{ for any } P \in \mathscr{P}.$$ □

We shall extend Theorem 5.1.21 to obtain a characterisation for $(\mathscr{G}, \mathscr{F})$-KDPs. However, we first require a result concerning the cardinality of the point set of an external structure. Within Lemma 5.1.24 we refer to repeated points and the smallest point in an incidence structure, (see Definition 2.1.1 and Definition 2.1.3 from Chapter 2).

Lemma 5.1.24. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure without repeated points and without a smallest point. Let $\mathscr{G}$ and $\mathscr{F}$ be families of non-empty subsets of $\mathscr{P}$ such that for every three distinct points $P_1, P_2, P_3 \in \mathscr{P}$ there exists a $G \in \mathscr{G}$ and $F \in \mathscr{F}$ such that $P_1 \in G$, $P_2, P_3 \in F$ and $G \cap F = \varnothing$.*

If for each $P \in \mathscr{P}$, $\mathscr{K}^P = (\mathscr{P}^P, \mathscr{B}^P, \mathscr{I}^P)$ is a $(\mathscr{G}^P, \mathscr{F}^P)$-KDP where

$$\mathscr{G}^P = \{G \in \mathscr{G} : G \subseteq \mathscr{P}^P\} \quad \text{and}$$
$$\mathscr{F}^P = \{F \cap \mathscr{P}^P : P \in F \in \mathscr{F} \text{ and } F \cap \mathscr{P}^P \neq \varnothing\},$$

then $\mathscr{P}^P = \mathscr{P} \setminus \{P\}$ for every $P \in \mathscr{P}$.

Proof. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure and let $\mathscr{G}$ and $\mathscr{F}$ be families of non-empty subsets of $\mathscr{P}$ that satisfy all the properties from the statement of the lemma. Now, suppose, in order to obtain a contradiction, that for some $Q \in \mathscr{P}$, $\mathscr{P}^Q \neq \mathscr{P} \setminus \{Q\}$. Then there exists $P_1 \in \mathscr{P}$ such that $P_1 \neq Q$ and $(P_1) \subseteq (Q)$.

Since there is no smallest point in $\mathscr{P}$, we know that there exists a point $P_2 \in \mathscr{P}$ such that $(P_1) \nsubseteq (P_2)$ and, in particular, $P_2 \notin \{P_1, Q\}$. Without loss of generality we can choose P_2 so that $(P_1) \nsubseteq (P_2)$ and $|(P_2)| = \min\{|P| : P \in \mathscr{P}$ and $(P_1) \nsubseteq (P)\}$. (Note that since $\mathscr{K}$ does not have any repeated points, $\mathscr{P}^{P_2} = \mathscr{P} \setminus \{P_2\}$.)

Now choose $G \in \mathscr{G}$ and $F \in \mathscr{F}$, where $G \cap F = \varnothing$, such that $P_1 \in G$ and $P_2, Q \in F$.
Then, $G \in \mathscr{G}^{P_2}$ and $F \setminus \{P_2\} \in \mathscr{F}^{P_2}$. However,

$$\bigcap_{P' \in G} (P') \subseteq (P_1) \subseteq (Q) \subseteq \bigcup_{Q' \in F \setminus \{P_2\}} (Q') \text{ and so } \bigcap_{P' \in G} (P') \subseteq \bigcup_{Q' \in F \setminus \{P_2\}} (Q').$$

That is, $\mathscr{K}^{P_2}$ is not a $(\mathscr{G}^{P_2}, \mathscr{F}^{P_2})$-KDP and the proof is complete. □

We may now give the previously alluded to characterisation, concerning when an incidence structure is a $(\mathscr{G}, \mathscr{F})$-KDP in terms of its external structure.

Theorem 5.1.25. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure without repeated points and without a smallest point. Let $\mathscr{G}$ and $\mathscr{F}$ be families of non-empty subsets of $\mathscr{P}$ such that:*

1. *for every three distinct points $P_1, P_2, P_3 \in \mathscr{P}$ there exists a $G \in \mathscr{G}$ and $F \in \mathscr{F}$ such that $P_1 \in G$, $P_2, P_3 \in \mathscr{F}$ and $G \cap F = \varnothing$;*

2. *$|F| \geq 2$ for every $F \in \mathscr{F}$.*

Then, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP if, and only if, for each $P \in \mathscr{P}$, $\mathscr{K}^P = (\mathscr{P}^P, \mathscr{B}^P, \mathscr{I}^P)$ is a $(\mathscr{G}^P, \mathscr{F}^P)$-KDP where $\mathscr{G}^P = \{G \in \mathscr{G} : G \subseteq \mathscr{P}^P\}$ and $\mathscr{F}^P = \{F \cap \mathscr{P}^P : P \in F \in \mathscr{F}$ and $F \cap \mathscr{P}^P \neq \varnothing\}$.

Proof. Suppose that $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a finite incidence structure and that $\mathscr{G}$ and $\mathscr{F}$ are families of non-empty subsets of $\mathscr{P}$ that satisfy the properties *1.* and *2.* from the statement of the theorem.

Now suppose that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP. From Theorem 5.1.21 we know that $\mathscr{K}^P$ is a $(\mathscr{G}^P, \mathscr{F}^P)$-KDP for every $P \in \mathscr{P}$.

Conversely, suppose that for every $P \in \mathscr{P}, \mathscr{K}^P$ is a $(\mathscr{G}^P, \mathscr{F}^P)$-KDP. Take any $G \in \mathscr{G}$ and any $F \in \mathscr{F}$ such that $G \cap F = \varnothing$. Then choose $P_1 \in F$. We know from Lemma 5.1.24 that $\mathscr{P}^{P_1} = \mathscr{P} \setminus \{P_1\}$, so $G \in \mathscr{G}^{P_1}$ and $F \setminus \{P_1\} \in \mathscr{F}^{P_1}$ because $|F| \geq 2$.

Since $\mathscr{K}^{P_1}$ is a $(\mathscr{G}^{P_1}, \mathscr{F}^{P_1})$-KDP,

$$\begin{aligned}
\varnothing \neq & \bigcap_{P\in G}(P)^{P_1} \setminus \bigcup_{Q\in F\setminus\{P_1\}} (Q)^{P_1} = \bigcap_{P\in G}(P)\cap \mathscr{B}^{P_1} \setminus \bigcup_{Q\in F\setminus\{P_1\}} (Q)\cap \mathscr{B}^{P_1} \\
= & \bigcap_{P\in G}(P)\cap \mathscr{B}^{P_1} \setminus \bigcup_{Q\in F}(Q)\cap \mathscr{B}^{P_1} \\
= & \left[\bigcap_{P\in G}(P)\cap \mathscr{B}^{P_1}\right] \cap \bigcap_{Q\in F} [\mathscr{B}\setminus(Q)\cup(P_1)] \quad \text{(by De Morgan's Law)} \\
= & \left[\bigcap_{P\in G}(P)\cap \mathscr{B}^{P_1} \bigcap_{Q\in F} \mathscr{B}\setminus(Q)\right] \cup \left[\bigcap_{P\in G}(P)\cap \mathscr{B}^{P_1}\cap(P_1)\right] \\
= & \bigcap_{P\in G}(P)\cap \mathscr{B}^{P_1} \bigcap_{Q\in F} \mathscr{B}\setminus(Q) \ \text{ since } \bigcap_{P\in G}(P)\cap \mathscr{B}^{P_1}\cap(P_1) = \varnothing \\
= & \bigcap_{P\in G}(P)\cap \mathscr{B}^{P_1} \setminus \bigcup_{Q\in F}(Q) \quad \text{(by De Morgan's Law)} \\
\subseteq & \bigcap_{P\in G}(P) \setminus \bigcup_{Q\in F}(Q).
\end{aligned}$$

Therefore, $\varnothing \neq \bigcap_{P\in G}(P) \setminus \bigcup_{Q\in F}(Q)$.

Hence, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP and the proof is complete. □

A canonical case of Theorem 5.1.25 is when $\mathscr{G}$ consists of all the subsets of $\mathscr{P}$ of cardinality at most t and $\mathscr{F}$ includes all subsets of $\mathscr{P}$ of cardinality at most $w + 1$.

Corollary 5.1.26. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure without repeated points and without a smallest point. Then, for any $t \leq |\mathscr{P}| - (w+1)$,*

$\mathscr{K}$ is a $(t, w+1)$-KDP if, and only if, for each $P \in \mathscr{P}$, $\mathscr{K}^P = (\mathscr{P}^P, \mathscr{B}^P, \mathscr{I}^P)$ is a (t, w)-KDP.

Proof. This is a special case of Theorem 5.1.25.
Let $\mathscr{G} = \{G \in 2^{\mathscr{P}} : 0 < |G| \leq t\}$ and $\mathscr{F} = \{F \in 2^{\mathscr{P}} : 1 < |F| \leq w+1\}$, then $\mathscr{K}$ satisfies properties *1.* and *2.* from Theorem 5.1.25. So $\mathscr{K}$ is a $(t, \mathscr{F})$-KDP and by Proposition 3.3.10, $\mathscr{K}$ is a $(t, w+1)$-KDP. □

Remark 5.1.27. Note that Example 5.1.3 (our earlier counterexample to Result 5.1.18) is consistent with Corollary 5.1.26, since point P_5 in Example 5.1.3 is actually a smallest point. If we were to remove point P_5 from Example 5.1.3 then we would be left with a finite incidence structure $\mathscr{K}_1 = (\mathscr{P}_1, \mathscr{B}_1, \mathscr{I}_1)$ such that $\mathscr{K}_1$ is a trivial 2-KDP on 4 points (and hence a $(2, 2)$-KDP) and $\mathscr{K}_1^P$ is a trivial 2-KDP on 3 points (and hence a $(2, 1)$-KDP) for every $P \in \mathscr{P}_1$.

As with internal structures we can apply our results on external structures to deduce some crude estimates for the number of blocks incident with any point.

Theorem 5.1.28. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP for $w \geq 2$ then,*

$$|(P)| < |\mathscr{B}| - \log_2 |\{G \in \mathscr{G} : P \notin G\}| \quad \textit{for any } P \in \mathscr{P}.$$

Proof. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a $(\mathscr{G}, w)$-KDP for $w \geq 2$ and let P be a point of $\mathscr{K}$. Note that since $\mathscr{K}$ is 1-secure for each $G \in \mathscr{G}^P = \{G' \in \mathscr{G} : P \notin G'\}$,

$$\bigcap_{Q \in G} (Q)^P \neq \varnothing \quad \text{and in particular} \quad \mathscr{G}^P = \{G \in \mathscr{G} : G \subseteq \mathscr{P}^P\}.$$

We know from Corollary 5.1.22 that because $\mathscr{K}$ is 2-secure, $\mathscr{K}^P$ is 1-secure. Therefore, by Observation 3.3.12, the mapping $G \mapsto \bigcap_{Q \in G} (Q)^P$ from $\mathscr{G}^P$ into non-empty subsets of $\mathscr{B}^P$ is 1-to-1. Thus,

$$|\mathscr{G}^P| = \left| \left\{ \bigcap_{Q \in G} (Q)^P \in 2^{\mathscr{B}^P} \setminus \{\varnothing\} : G \in \mathscr{G}^P \right\} \right| \leq 2^{|\mathscr{B}^P|} - 1.$$

Hence, $\log_2 |\mathscr{G}^P| \leq \log_2(2^{|\mathscr{B}^P|} - 1) < \log_2(2^{|\mathscr{B}^P|}) = |\mathscr{B}^P| = |\mathscr{B}| - |(P)|$.

That is, $|(P)| < |\mathscr{B}| - \log_2 |\{G \in \mathscr{G} : P \notin G\}|$ and the proof is complete. □

By combining Theorem 5.1.15 and Theorem 5.1.28 we obtain the following estimate for the number of blocks incident with a given point.

Corollary 5.1.29. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP where $2 \leq |G| < |\mathscr{P}|$ for all $G \in \mathscr{G}$ and $w \geq 2$, then for each $P \in \mathscr{P}$*

$$\log_2 |\{G \in \mathscr{G} : P \in G\}| < |(P)| < |\mathscr{B}| - \log_2 |\{G \in \mathscr{G} : P \notin G\}|.$$

We shall revisit this result later, in Chapter 6, when we estimate the number of blocks incident with a given point in an incidence structure.

Next we consider another way of creating new incidence structures from old ones.

5.1.3 Complement $(\mathscr{G}, \mathscr{F})$-KDPs

We begin with the fundamental definition of the *complement* of an incidence structure.

Definition 5.1.30. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. We define the **complement** of $\mathscr{K}$ denoted $C(\mathscr{K}) = (C(\mathscr{P}), C(\mathscr{B}), C(\mathscr{I}))$ such that $C(\mathscr{P}) = \mathscr{P}$, $C(\mathscr{B}) = \mathscr{B}$ and $(P, x) \in C(\mathscr{I})$ if and only if $(P, x) \notin \mathscr{I}$.*

That is, the point and block sets of the complement of an incidence structure $\mathscr{K}$ coincide with those of $\mathscr{K}$. The only thing to change is the incidence relation itself, which is replaced by the complement relation, i.e. $C(\mathscr{I}) = (\mathscr{P} \times \mathscr{B} \setminus \mathscr{I})$.

We can visualise the effect of taking the complement of an incidence structure by considering its matrix representation. We already know from Observation 1.5.3 that an incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ can be represented by a $v \times b$ binary matrix $A = (a_{i,j})$ defined as follows:

$$a_{i,j} = \begin{cases} 1 & \text{if } (P_i, x_j) \in \mathscr{I} \\ 0 & \text{otherwise.} \end{cases}$$

From this it is easy to see that $C(\mathscr{K})$ can be represented by the $v \times b$ matrix $C(A) = (a'_{i,j})$ defined as follows:

$$a'_{i,j} = \begin{cases} 0 & \text{if } (P_i, x_j) \in \mathscr{I} \\ 1 & \text{otherwise.} \end{cases}$$

As with internal structures and external structures, we now introduce some new notation representing the blocks incident with a point and the points incident with a block in a complement structure. For a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$, we let $(P)^C = \{x \in C(\mathscr{B}) : (P, x) \in C(\mathscr{I})\}$ for each $P \in C(\mathscr{P})$ and we let $(x)^C = \{P \in C(\mathscr{P}) : (P, x) \in C(\mathscr{I})\}$ for each $x \in C(\mathscr{B})$. Note that $(P)^C = \mathscr{B} \setminus (P)$ and $(x)^C = \mathscr{P} \setminus (x)$.

For $(\mathscr{G}, \mathscr{F})$-KDPs, taking the complement has the effect of interchanging the roles of $\mathscr{G}$ and $\mathscr{F}$. This is shown precisely in the following theorem.

Theorem 5.1.31. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then the complement of $\mathscr{K}, C(\mathscr{K})$ is an $(\mathscr{F}, \mathscr{G})$-KDP.*

Proof. Suppose that $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP and that $C(\mathscr{K}) = (C(\mathscr{P}), C(\mathscr{B}), C(\mathscr{I}))$. Consider $G' \in \mathscr{F}$ and $F' \in \mathscr{G}$ such that $G' \cap F' = \varnothing$. Then,

$$\bigcap_{P \in G'} (P)^C = \bigcap_{P \in G'} \mathscr{B} \setminus (P) = \mathscr{B} \setminus \bigcup_{P \in G'} (P)$$
$$\bigcup_{Q \in F'} (Q)^C = \bigcup_{Q \in F'} \mathscr{B} \setminus (Q) = \mathscr{B} \setminus \bigcap_{Q \in F'} (Q).$$

Therefore,

$$\begin{aligned} \bigcap_{P \in G'} (P)^C \subseteq \bigcup_{Q \in F'} (Q)^C \quad &\Longleftrightarrow \quad \mathscr{B} \setminus \bigcup_{P \in G'} (P) \subseteq \mathscr{B} \setminus \bigcap_{Q \in F'} (Q) \\ &\Longleftrightarrow \quad \bigcap_{Q \in F'} (Q) \subseteq \bigcup_{P \in G'} (P). \end{aligned}$$

However, since $F' \in \mathscr{G}, G' \in \mathscr{F}$ and $F' \cap G' = \varnothing$, $\bigcap_{Q \in F'} (Q) \nsubseteq \bigcup_{P \in G'} (P)$ and so $\bigcap_{P \in G'} (P)^C \nsubseteq \bigcup_{Q \in F'} (Q)^C$, which completes the proof. □

An interesting case concerning (t, w)-KDPs follows from Theorem 5.1.31.

Corollary 5.1.32. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a (t, w)-KDP for any $t \leq |\mathscr{P}| - w$, then the complement of $\mathscr{K}$, $C(\mathscr{K})$ is a (w, t)-KDP.*

Theorem 5.1.31 and Corollary 5.1.32 will be used later in Chapter 6 to calculate upper bounds for the number of blocks incident with a given point.

We conclude our discussion of complement $(\mathscr{G}, \mathscr{F})$-KDPs with a simple observation concerning trivial $\mathscr{G}$-KDPs.

Observation 5.1.33. *If $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a trivial $\mathscr{G}$-KDP such that $1 \leq |G| < |\mathscr{P}|$ for every $G \in \mathscr{G}$, then the complement of $\mathscr{K}$ is a trivial $\mathscr{G}'$-KDP for $G' = \{\mathscr{P} \setminus G : G \in \mathscr{G}\}$.*

Proof. Firstly, let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a trivial $\mathscr{G}$-KDP with the block set $\mathscr{B} = \{x_1, x_2, \ldots, x_b\}$ and $\mathscr{G} = \{G_i : i \in J \subseteq \{1, \ldots, b\}\}$. Then, for each $i \in J$, $(P, x_i) \in \mathscr{I}$ if, and only if, $P \in G_i$.

Now let $C(\mathscr{K})= (C(\mathscr{P}), C(\mathscr{B}), C(\mathscr{I}))$ be the complement of $\mathscr{K}$ such that $C(\mathscr{P}) = \mathscr{P}, C(\mathscr{B}) = \mathscr{B}$ and $(P, x_i) \in C(\mathscr{I})$ if, and only if, $(P, x_i) \notin \mathscr{I}$. Also, let $\mathscr{G}' = \{G'_i : i \in J \subseteq \{1, \ldots, b\}\}$, where $G'_i = \mathscr{P} \setminus G_i$.
For $i \in J$,

$$\begin{aligned} (P, x_i) \in C(\mathscr{I}) \quad &\Longleftrightarrow \quad (P, x_i) \notin \mathscr{I} \iff P \notin G_i \\ &\Longleftrightarrow \quad P \in \mathscr{P} \setminus G_i \iff P \in G'_i. \end{aligned}$$

Given that $1 \leq |G| < |\mathscr{P}|$ for every $G \in \mathscr{G}$, it follows that $1 \leq |G'| < |\mathscr{P}|$ for every $G' \in \mathscr{G}'$ and so $C(\mathscr{K})$ is a trivial $\mathscr{G}'$-KDP. □

An alternative proof of Observation 5.1.33 follows from Theorem 5.1.31, by applying Observation 3.2.2 and Theorem 3.2.5, which were the first results that we presented for trivial $\mathscr{G}$-KDPs. We finally note, as a special case of Observation 5.1.33, that the complement of a trivial t-KDP is a trivial $(|\mathscr{P}| - t)$-KDP for any $t < |\mathscr{P}|$.

5.1.4 Dual $(\mathscr{G}, \mathscr{F})$-KDPs

As in the previous subsections, we will begin with a fundamental definition.

Definition 5.1.34. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. We define the* **dual** *of $\mathscr{K}$, denoted $\mathscr{K}^T = (\mathscr{P}^T, \mathscr{B}^T, \mathscr{I}^T)$ such that $\mathscr{P}^T = \mathscr{B}$, $\mathscr{B}^T = \mathscr{P}$ and $(x, P) \in \mathscr{I}^T$ if and only if $(P, x) \in \mathscr{I}$.*

That is, the dual of an incidence structure is constructed by interchanging the roles of the points and blocks of the original structure. If A is an incidence matrix for a structure $\mathscr{K}$, then the transpose of A, A^T, is an incidence matrix for $\mathscr{K}^T$.

Our first and only result in this section investigates the families of privileged and forbidden subsets in the dual of a $(\mathscr{G}, \mathscr{F})$-KDP.

Theorem 5.1.35. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then $\mathscr{K}^T = (\mathscr{P}^T, \mathscr{B}^T, \mathscr{I}^T)$ is a $(\mathscr{G}^T, \mathscr{F}^T)$-KDP where*

$$\mathscr{G}^T = \Big\{ \bigcap_{P \in J} (P) : J \subseteq \mathscr{P} \text{ and } \bigcap_{P \in J} (P) \neq \varnothing \Big\} \text{ and}$$

$$\mathscr{F}^T = \big[2^{\mathscr{B}} \backslash \{\varnothing\}\big] \backslash \Big\{ F \in 2^{\mathscr{B}} : \exists\, G^T \in \mathscr{G}^T, \bigcap_{P \in G^T} (P) \subseteq \bigcup_{Q \in F^T} (Q) \text{ and } G^T \cap F^T = \varnothing \Big\}.$$

Theorem 5.1.35 is not a natural result. The description of $\mathscr{G}^T$ and $\mathscr{F}^T$ could essentially be applied to any incidence structure. We have simply specified that $\mathscr{G}^T$ be the largest set of privileged subsets such that $\mathscr{F}^T \supseteq \{F^T \in 2^{\mathscr{B}} : 1 \leq |F| \leq w\}$ and that $\mathscr{F}^T$ be the largest set of forbidden subsets for $\mathscr{G}^T$ with respect to $\mathscr{K}$.

However, Theorem 5.1.35 is the best that we have been able to obtain. This is because there is no obvious correspondence between the original families of privileged and forbidden subsets and those corresponding to the dual $(\mathscr{G}, \mathscr{F})$-KDP. As such, we are unable to find any natural results for $(\mathscr{G}, \mathscr{F})$-KDPs concerning duals and therefore we do not consider duals further in this thesis.

5.2 Constructions from Multiple KDPs

In [60], Mitchell and Piper consider three ways in which two $(2, w)$-KDPs may be joined to give a new $(2, w)$-KDP that provides pair-wise secure communication for a larger network of users. In this section we generalise these techniques for $(\mathscr{G}, \mathscr{F})$-KDPs.

Our first result generalises [60, Construction 1.5]. We essentially take the union of the two point sets and the cross product of the two block sets.

Theorem 5.2.1. *Let the finite incidence structures $\mathscr{K}_1 = (\mathscr{P}_1, \mathscr{B}_1, \mathscr{I}_1)$ and $\mathscr{K}_2 = (\mathscr{P}_2, \mathscr{B}_2, \mathscr{I}_2)$, where $\mathscr{P}_1 \cap \mathscr{P}_2 = \varnothing$, be a tight $(\mathscr{G}_1, \mathscr{F}_1)$-KDP and a tight $(\mathscr{G}_2, \mathscr{F}_2)$-KDP, respectively.*
Let $\mathscr{P} = \mathscr{P}_1 \cup \mathscr{P}_2$, $\mathscr{B} = \mathscr{B}_1 \times \mathscr{B}_2$ and the incidence relation $\mathscr{I}$ be defined by:
(i) For $P \in \mathscr{P}_1$, (x, y) is incident with P if, and only if, $(P, x) \in \mathscr{I}_1$;
(ii) For $P \in \mathscr{P}_2$, (x, y) is incident with P if, and only if, $(P, y) \in \mathscr{I}_2$.
Then $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP with

$$\begin{aligned} \mathscr{G} &= \mathscr{G}_1 \cup \mathscr{G}_2 \cup \{G_1 \cup G_2 : G_1 \in \mathscr{G}_1, G_2 \in \mathscr{G}_2\} \\ \textit{and} \quad \mathscr{F} &= \mathscr{F}_1 \cup \mathscr{F}_2 \cup \{F_1 \cup F_2 : F_1 \in \mathscr{F}_1, F_2 \in \mathscr{F}_2\}. \end{aligned}$$

Proof. Suppose that $\mathscr{P} = \mathscr{P}_1 \cup \mathscr{P}_2$, $\mathscr{B} = \mathscr{B}_1 \times \mathscr{B}_2$ and that the incidence relation is defined as in the statement of the theorem. Moreover, for each $P \in \mathscr{P}$ we define $(P)'$ to be the set of all blocks in $\mathscr{B}_1 \times \mathscr{B}_2$ incident with P with respect to $\mathscr{I}$. Then $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP, with $\mathscr{G}$ and $\mathscr{F}$ defined as in the statement of the theorem, if $\bigcap_{P \in G}(P)' \nsubseteq \bigcup_{Q \in F}(Q)'$ for all $G \in \mathscr{G}$ and $F \in \mathscr{F}$ such that $G \cap F = \varnothing$.
To show this we shall consider three cases:

1. when $G \in \mathscr{G}_1$ and $F \in \mathscr{F}$;
2. when $G \in \mathscr{G}_2$ and $F \in \mathscr{F}$; and
3. when $G \in \{G_1 \cup G_2 : G_1 \in \mathscr{G}_1$ and $G_2 \in \mathscr{G}_2\}$ and $F \in \mathscr{F}$.

[Case 1] $G \in \mathscr{G}_1$ and $F \in \mathscr{F}$.

We break Case 1 down into three further subcases.

[1a] Suppose that $G \in \mathscr{G}_1$, $F \in \mathscr{F}_1$ and $G \cap F = \varnothing$. Since $G \in \mathscr{G}_1$ and $F \in \mathscr{F}_1$, $\bigcap_{P \in G}(P) \not\subseteq \bigcup_{Q \in F}(Q)$ and so $\bigcap_{P \in G}(P)' \not\subseteq \bigcup_{Q \in F}(Q)'$.

[1b] Suppose that $G \in \mathscr{G}_1$, $F \in \mathscr{F}_2$ and $G \cap F = \varnothing$. Since $\mathscr{F}_2$ is tight, there exists a block $y_1 \in \mathscr{B}_2$ such that $(x, y_1) \notin \bigcup_{Q \in F}(Q)'$ for all $x \in \mathscr{B}_1$. Also, since $\mathscr{G}_1$ is tight there exists a block $x_1 \in \mathscr{B}_1$ such that $(x_1, y) \in \bigcap_{P \in G}(P)'$ for all $y \in \mathscr{B}_2$. Therefore, $(x_1, y_1) \in \bigcap_{P \in G}(P)' \setminus \bigcup_{Q \in F}(Q)'$ and hence $\bigcap_{P \in G}(P)' \not\subseteq \bigcup_{Q \in F}(Q)'$.

[1c] Suppose that $G \in \mathscr{G}_1$ and $F \in \{F_1 \cup F_2 : F_1 \in \mathscr{F}_1 \text{ and } F_2 \in \mathscr{F}_2\}$ such that $G \cap F = \varnothing$. We know that there exists a block $x_1 \in \mathscr{B}_1$ such that $(x_1, y) \in \bigcap_{P \in G}(P)' \setminus \bigcup_{Q_1 \in F_1}(Q_1)'$ for all $y \in \mathscr{B}_2$. Also, there exists a block $y_1 \in \mathscr{B}_2$ such that $(x, y_1) \notin \bigcup_{Q_2 \in F_2}(Q_2)'$ for all $x \in \mathscr{B}_1$. Therefore, $(x_1, y_1) \in \bigcap_{P \in G}(P)' \setminus \left[\bigcup_{Q_1 \in F_1}(Q_1)' \cup \bigcup_{Q_2 \in F_2}(Q_2)'\right]$ and hence $\bigcap_{P \in G}(P)' \not\subseteq \bigcup_{Q \in F}(Q)'$.

[Case 2] $G \in \mathscr{G}_2$ and $F \in \mathscr{F}$.

The proof of this case is identical to that of Case 1.

[Case 3] $G \in \{G_1 \cup G_2 : G_1 \in \mathscr{G}_1 \text{ and } G_2 \in \mathscr{G}_2\}$ and $F \in \mathscr{F}$.

Again we break this down into three further subcases.

[3a] Suppose that $G \in \{G_1 \cup G_2 : G_1 \in \mathscr{G}_1 \text{ and } G_2 \in \mathscr{G}_2\}$, $F \in \mathscr{F}_1$ and $G \cap F = \varnothing$. We know that there exists a block $x_1 \in \mathscr{B}_1$ such that $(x_1, y) \in \bigcap_{P_1 \in G_1}(P_1)' \setminus \bigcup_{Q \in F}(Q)'$ for all $y \in \mathscr{B}_2$. Also, since $\mathscr{G}_2$ is tight there exists a block $y_1 \in \mathscr{B}_2$ such that $(x, y_1) \in \bigcap_{P_2 \in G_2}(P_2)'$ for all $x \in \mathscr{B}_1$. Therefore, $(x_1, y_1) \in [\bigcap_{P_1 \in G_1}(P_1)' \cap \bigcap_{P_2 \in G_2}(P_2)'] \setminus \bigcup_{Q \in F}(Q)'$ and hence $\bigcap_{P \in G}(P)' \not\subseteq \bigcup_{Q \in F}(Q)'$.

[3b] Suppose that $G \in \{G_1 \cup G_2 : G_1 \in \mathscr{G}_1 \text{ and } G_2 \in \mathscr{G}_2\}$, $F \in \mathscr{F}_2$ and $G \cap F = \varnothing$. The proof of this case is similar to that of Case 3a.

[3c] Suppose that $G \in \{G_1 \cup G_2 : G_1 \in \mathscr{G}_1 \text{ and } G_2 \in \mathscr{G}_2\}$, $F \in \{F_1 \cup F_2 : F_1 \in \mathscr{F}_1 \text{ and } F_2 \in \mathscr{F}_2\}$ and $G \cap F = \varnothing$. We know that there exists a block $x_1 \in \mathscr{B}_1$ such that $(x_1, y) \in \bigcap_{P_1 \in G_1}(P_1)' \setminus \bigcup_{Q_1 \in F_1}(Q_1)'$ for all $y \in \mathscr{B}_2$. We also know that there exists a block $y_1 \in \mathscr{B}_2$ such that $(x, y_1) \in \bigcap_{P_2 \in G_2}(P_2)' \setminus \bigcup_{Q_2 \in F_2}(Q_2)'$ for all $x \in \mathscr{B}_1$. Therefore,

$$(x_1, y_1) \in \left[\bigcap_{P_1 \in G_1}(P_1)' \cap \bigcap_{P_2 \in G_2}(P_2)'\right] \setminus \left[\bigcup_{Q_1 \in F_1}(Q_1)' \cup \bigcup_{Q_2 \in F_2}(Q_2)'\right] = \bigcap_{P \in G}(P)' \setminus \bigcup_{Q \in F}(Q)$$

$$\text{and hence } \bigcap_{P \in G}(P)' \not\subseteq \bigcup_{Q \in F}(Q)'.$$

That is, $\bigcap_{P \in G}(P)' \not\subseteq \bigcup_{Q \in F}(Q)'$ for any $G \in \mathscr{G}$ and $F \in \mathscr{F}$ such that $G \cap F = \varnothing$. This completes the proof. □

We now consider Theorem 5.2.1 in the special case of (t, w)-KDPs.

Corollary 5.2.2. *Let the finite incidence structures $\mathscr{K}_1 = (\mathscr{P}_1, \mathscr{B}_1, \mathscr{I}_1)$ and $\mathscr{K}_2 = (\mathscr{P}_2, \mathscr{B}_2, \mathscr{I}_2)$, where $\mathscr{P}_1 \cap \mathscr{P}_2 = \varnothing$, be (t, w)-KDPs for $t \leq \min(|\mathscr{P}_1| - w, |\mathscr{P}_2| - w)$. Let $\mathscr{P} = \mathscr{P}_1 \cup \mathscr{P}_2, \mathscr{B} = \mathscr{B}_1 \times \mathscr{B}_2$ and the incidence relation $\mathscr{I}$ be defined as in Theorem 5.2.1. Then $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is also a (t, w)-KDP.*

Although Theorem 5.2.1 is a natural construction, it produces $(\mathscr{G}, \mathscr{F})$-KDPs with relatively large numbers of blocks, compared to the numbers of blocks in the component $(\mathscr{G}, \mathscr{F})$-KDPs. That is, any $(\mathscr{G}, \mathscr{F})$-KDPs produced using Theorem 5.2.1 will not be particularly efficient. For example, if we begin with a tight $(\mathscr{G}_1, \mathscr{F}_1)$-KDP with six blocks and a tight $(\mathscr{G}_2, \mathscr{F}_2)$-KDP with sx blocks, then the resultant $(\mathscr{G}, \mathscr{F})$-KDP will have 36 blocks.

Using Theorem 5.2.1 it is possible to combine two trivial $\mathscr{G}$-KDPs (or cotrivial $\mathscr{F}$-KDPs) in order to construct a much larger non-trivial $(\mathscr{G}', \mathscr{F}')$-KDP. Thus, the problem of constructing a "large" non-trivial $(\mathscr{G}, \mathscr{F})$-KDP reduces to constructing two "small" trivial $\mathscr{G}$-KDPs.

Our second result in this section generalises [60, Construction 1.6]. Here we do not simply take the cross product of the two original block sets. Instead, we first reduce the size of one of those block sets before taking the cross product. In this way, we reduce the number of blocks in the resultant $(\mathscr{G}, \mathscr{F})$-KDP.

Theorem 5.2.3. *Let the finite incidence structures $\mathscr{K}_1 = (\mathscr{P}_1, \mathscr{B}_1, \mathscr{I}_1)$, where $P^* \in \mathscr{P}_1$, and $\mathscr{K}_2 = (\mathscr{P}_2, \mathscr{B}_2, \mathscr{I}_2)$, where $\mathscr{P}_1 \cap \mathscr{P}_2 = \varnothing$, be a tight $(\mathscr{G}_1, \mathscr{F}_1)$-KDP and a tight $(\mathscr{G}_2, \mathscr{F}_2)$-KDP, respectively.*
Let $\mathscr{P} = \mathscr{P}_1 \cup \mathscr{P}_2, \mathscr{B} = [\mathscr{B}_1 \setminus (P^*)] \cup [(P^*) \times \mathscr{B}_2]$ and the incidence relation $\mathscr{I}$ be defined by:
(i) For $P \in \mathscr{P}_1$ and $x \in \mathscr{B}_1 \setminus (P^*)$, x is incident with P if, and only if, $(P, x) \in \mathscr{I}_1$;
(ii) For $P \in \mathscr{P}_1$ and $(x, y) \in (P^*) \times \mathscr{B}_2$, (x, y) is incident with P if, and only if, $(P, x) \in \mathscr{I}_1$;
(iii) For $P \in \mathscr{P}_2$, $(x, y) \in (P^*) \times \mathscr{B}_2$ is incident with P if, and only if, $(P, y) \in \mathscr{I}_2$.
Then $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP with

$$\mathscr{G} = \mathscr{G}_1 \cup \mathscr{G}_2 \cup \{G_1 \cup G_2 : P^* \in G_1 \in \mathscr{G}_1 \text{ and } G_2 \in \mathscr{G}_2\} \text{ and}$$
$$\mathscr{F} = \mathscr{F}_1^* \cup \mathscr{F}_2 \cup \{F_1 \cup F_2 : F_1 \in \mathscr{F}_1^* \text{ and } F_2 \in \mathscr{F}_2\}$$
$$\text{where } \mathscr{F}_1^* = \left\{F \in \mathscr{F}_1 : (P^*) \not\subseteq \textstyle\bigcup_{Q \in F}(Q)\right\}.$$

Proof. Suppose that $\mathscr{P} = \mathscr{P}_1 \cup \mathscr{P}_2, \mathscr{B} = [\mathscr{B}_1 \setminus (P^*)] \cup [(P^*) \times \mathscr{B}_2]$ and that the incidence relation is defined as in the statement of the theorem. Moreover, for each $P \in \mathscr{P}$ we define $(P)'$ to be the set of all blocks in $[\mathscr{B}_1 \setminus (P^*)] \cup [(P^*) \times \mathscr{B}_2]$ incident with P with respect to $\mathscr{I}$. Then $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP, with $\mathscr{G}$ and $\mathscr{F}$ defined as in the statement of the theorem, if $\bigcap_{P \in G}(P)' \not\subseteq \bigcup_{Q \in F}(Q)'$ for all $G \in \mathscr{G}$ and $F \in \mathscr{F}$ such that $G \cap F = \varnothing$.
To show this we shall consider three cases:

1. when $G \in \mathscr{G}_1$ and $F \in \mathscr{F}$;

2. when $G \in \mathscr{G}_2$ and $F \in \mathscr{F}$; and

3. when $G \in \{G_1 \cup G_2 : P^* \in G_1 \in \mathscr{G}_1 \text{ and } G_2 \in \mathscr{G}_2\}$ and $F \in \mathscr{F}$.

[Case 1] $G \in \mathscr{G}_1$ and $F \in \mathscr{F}$.

We break Case 1 down into three further subcases.

[1a] Suppose that $G \in \mathscr{G}_1$, $F \in \mathscr{F}_1^*$ and $G \cap F = \varnothing$. Since $G \in \mathscr{G}_1$ and $F \in \mathscr{F}_1$, $\bigcap_{P \in G}(P) \nsubseteq \bigcup_{Q \in F}(Q)$ and so $\bigcap_{P \in G}(P)' \nsubseteq \bigcup_{Q \in F}(Q)'$.

[1b] Suppose that $G \in \mathscr{G}_1$, $F \in \mathscr{F}_2$ and $G \cap F = \varnothing$. Since $\mathscr{G}_1$ is tight, there exists a block $x_1 \in \mathscr{B}_1$ such that $x_1 \in \bigcap_{P \in G}(P)$. If $x_1 \in \mathscr{B}_1 \setminus (P^*)$ then, $x_1 \in \bigcap_{P \in G}(P)' \setminus \bigcup_{Q \in F}(Q)'$. Otherwise, $x_1 \in (P^*)$ and $(x_1, y) \in \bigcap_{P \in G}(P)'$ for all $y \in \mathscr{B}_2$ and, since $\mathscr{F}_2$ is tight, there exists a block $y_1 \in \mathscr{B}_2$ such that $(x, y_1) \notin \bigcup_{Q \in F}(Q)'$ for all $x \in (P^*)$. Therefore, $(x_1, y_1) \in \bigcap_{P \in G}(P)' \setminus \bigcup_{Q \in F}(Q)'$ and hence $\bigcap_{P \in G}(P)' \nsubseteq \bigcup_{Q \in F}(Q)'$ in both situations.

[1c] Suppose that $G \in \mathscr{G}_1$, $F \in \{F_1 \cup F_2 : F_1 \in \mathscr{F}_1^* \text{ and } F_2 \in \mathscr{F}_2\}$ and $G \cap F = \varnothing$. We know that there exists a block $x_1 \in \mathscr{B}_1$ such that $x_1 \in \bigcap_{P \in G}(P) \setminus \bigcup_{Q_1 \in F_1}(Q_1)$. If $x_1 \in \mathscr{B}_1 \setminus (P^*)$ then, $x_1 \in \bigcap_{P \in G}(P)' \setminus \bigcup_{Q \in F}(Q)'$ otherwise $x_1 \in (P^*)$ and $(x_1, y) \in \bigcap_{P \in G}(P)' \setminus \bigcup_{Q_1 \in F_1}(Q_1)'$ for all $y \in \mathscr{B}_2$. Also, there exists a block $y_1 \in \mathscr{B}_2$ such that $(x, y_1) \notin \bigcup_{Q_2 \in F_2}(Q_2)'$ for all $x \in (P^*)$. Therefore, $(x_1, y_1) \in \bigcap_{P \in G}(P)' \setminus \left[\bigcup_{Q_1 \in F_1}(Q_1)' \cup \bigcup_{Q_2 \in F_2}(Q_2)'\right]$ and hence $\bigcap_{P \in G}(P)' \nsubseteq \bigcup_{Q \in F}(Q)'$.

[Case 2] $G \in \mathscr{G}_2$ and $F \in \mathscr{F}$.

We break Case 2 down into three further subcases.

[2a] Suppose that $G \in \mathscr{G}_2$, $F \in \mathscr{F}_1^*$ and $G \cap F = \varnothing$. Since $\mathscr{G}_2$ is tight, there exists a block $y_1 \in \mathscr{B}_2$ such that $(x, y_1) \in \bigcap_{P \in G}(P)'$ for all $x \in (P^*)$. Also, since $(P^*) \nsubseteq \bigcup_{Q \in F_1}(Q)$ for all $F_1 \in \mathscr{F}_1^*$, there exists a block $x_1 \in (P^*)$ such that $(x_1, y) \notin \bigcup_{Q \in F}(Q)'$ for all $y \in \mathscr{B}_2$. Therefore, $(x_1, y_1) \in \bigcap_{P \in G}(P)' \setminus \bigcup_{Q \in F}(Q)'$ and hence $\bigcap_{P \in G}(P)' \nsubseteq \bigcup_{Q \in F}(Q)'$.

[2b] Suppose that $G \in \mathscr{G}_2$, $F \in \mathscr{F}_2$ and $G \cap F = \varnothing$. Since $G \in \mathscr{G}_2$ and $F \in \mathscr{F}_2$, $\bigcap_{P \in G}(P) \nsubseteq \bigcup_{Q \in F}(Q)$ and so $\bigcap_{P \in G}(P)' \nsubseteq \bigcup_{Q \in F}(Q)'$.

[2c] Suppose that $G \in \mathscr{G}_2$, $F \in \{F_1 \cup F_2 : F_1 \in \mathscr{F}_1^* \text{ and } F_2 \in \mathscr{F}_2\}$ and $G \cap F = \varnothing$. We know that there exists a block $y_1 \in \mathscr{B}_2$ such that $(x, y_1) \in \bigcap_{P \in G}(P)' \setminus \bigcup_{Q_2 \in F_2}(Q_2)'$ for all $x \in (P^*)$. Also, since $(P^*) \not\subseteq \bigcup_{Q \in F_1}(Q)$ for all $F_1 \in \mathscr{F}_1$, there exists a block $x_1 \in (P^*)$ such that $(x_1, y) \notin \bigcup_{Q_1 \in F_1}(Q_1)'$ for all $y \in \mathscr{B}_2$. Therefore, $(x_1, y_1) \in \bigcap_{P \in G}(P)' \setminus \left[\bigcup_{Q_1 \in F_1}(Q_1)' \cup \bigcup_{Q_2 \in F_2}(Q_2)'\right]$ and hence $\bigcap_{P \in G}(P)' \not\subseteq \bigcup_{Q \in F}(Q)'$.

[Case 3] $G \in \{G_1 \cup G_2 : P^* \in G_1 \in \mathscr{G}_1 \text{ and } G_2 \in \mathscr{G}_2\}$ and $F \in \mathscr{F}$.
We break Case 3 down into three further subcases.

[3a] Suppose that $G \in \{G_1 \cup G_2 : P^* \in G_1 \in \mathscr{G}_1 \text{ and } G_2 \in \mathscr{G}_2\}$, $F \in \mathscr{F}_1^*$ and $G \cap F = \varnothing$. Since $P^* \in G_1$, there exists a block $x_1 \in (P^*)$ such that $(x_1, y) \in \bigcap_{P_1 \in G_1}(P)' \setminus \bigcup_{Q \in F}(Q)'$ for all $y \in \mathscr{B}_2$. Also, since $\mathscr{G}_2$ is tight there exists a block $y_1 \in \mathscr{B}_2$ such that $(x, y_1) \in \bigcap_{P_2 \in G_2}(P_2)'$ for all $x \in (P^*)$. Therefore, $(x_1, y_1) \in \left[\bigcap_{P_1 \in G_1}(P_1)' \cap \bigcap_{P_2 \in G_2}(P_2)'\right] \setminus \bigcup_{Q \in F}(Q)'$ and hence $\bigcap_{P \in G}(P)' \not\subseteq \bigcup_{Q \in F}(Q)'$.

[3b] Suppose that $G \in \{G_1 \cup G_2 : P^* \in G_1 \in \mathscr{G}_1 \text{ and } G_2 \in \mathscr{G}_2\}$, $F \in \mathscr{F}_2$ and $G \cap F = \varnothing$. We know that there exists a block $x_1 \in (P^*)$ such that $(x_1, y) \in \bigcap_{P_1 \in G_1}(P)'$ for all $y \in \mathscr{B}_2$. Also, there exists a block $y_1 \in \mathscr{B}_2$ such that $(x, y_1) \in \bigcap_{P_2 \in G_2}(P_2)' \setminus \bigcup_{Q \in F}(Q)'$ for all $x \in (P^*)$. Therefore, $(x_1, y_1) \in \left[\bigcap_{P_1 \in G_1}(P_1)' \cap \bigcap_{P_2 \in G_2}(P_2)'\right] \setminus \bigcup_{Q \in F}(Q)'$ and hence $\bigcap_{P \in G}(P)' \not\subseteq \bigcup_{Q \in F}(Q)'$.

[3c] Suppose that $G \in \{G_1 \cup G_2 : P^* \in G_1 \in \mathscr{G}_1 \text{ and } G_2 \in \mathscr{G}_2\}$, $F \in \{F_1 \cup F_2 : F_1 \in \mathscr{F}_1^* \text{ and } F_2 \in \mathscr{F}_2\}$ and $G \cap F = \varnothing$. We know that there exists a block $x_1 \in (P^*)$ such that $(x_1, y) \in \bigcap_{P_1 \in G_1}(P_1)' \setminus \bigcup_{Q_1 \in F_1}(Q_1)'$ for all $y \in \mathscr{B}_2$. Also, there exists a $y_1 \in \mathscr{B}_2$ such that $(x, y_1) \in \bigcap_{P_2 \in G_2}(P_2)' \setminus \bigcup_{Q_2 \in F_2}(Q_2)'$ for all $x \in (P^*)$. Therefore,

$$(x_1, y_1) \in \left[\bigcap_{P_1 \in G_1}(P_1)' \cap \bigcap_{P_2 \in G_2}(P_2)'\right] \setminus \left[\bigcup_{Q_1 \in F_1}(Q_1)' \cup \bigcup_{Q_2 \in F_2}(Q_2)'\right] = \bigcap_{P \in G}(P)' \setminus \bigcup_{Q \in F}(Q)$$

$$\text{and hence } \bigcap_{P \in G}(P)' \not\subseteq \bigcup_{Q \in F}(Q)'.$$

That is, $\bigcap_{P\in G}(P)' \not\subseteq \bigcup_{Q\in F}(Q)'$ for any $G \in \mathscr{G}$ and $F \in \mathscr{F}$ such that $G \cap F = \varnothing$. This completes the proof. □

We note that the combined point set in Theorem 5.2.3 includes the point P^*. In this way Theorem 5.2.3 is not a direct generalisation of [60, Construction 1.6] as [60, Construction 1.6] excludes this point. However, using Proposition 3.1.6 we can obtain a true generalisation of [60, Construction 1.6] by deleting the point P^*.

Corollary 5.2.4. *Let the finite incidence structures $\mathscr{K}_1 = (\mathscr{P}_1, \mathscr{B}_1, \mathscr{I}_1)$, where $P^* \in \mathscr{P}_1$, and $\mathscr{K}_2 = (\mathscr{P}_2, \mathscr{B}_2, \mathscr{I}_2)$, where $\mathscr{P}_1 \cap \mathscr{P}_2 = \varnothing$, be a tight $(\mathscr{G}_1, \mathscr{F}_1)$-KDP and a tight $(\mathscr{G}_2, \mathscr{F}_2)$-KDP, respectively.*
Let $\mathscr{P} = [\mathscr{P}_1 \setminus \{P^*\}] \cup \mathscr{P}_2, \mathscr{B} = [\mathscr{B}_1 \setminus (P^*)] \cup [(P^*) \times \mathscr{B}_2]$ and the incidence relation $\mathscr{I}$ be defined as in Theorem 5.2.3. Then $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP with

$$\mathscr{G} = \mathscr{G}_1^* \cup \mathscr{G}_2 \cup \{[G_1 \setminus \{P^*\}] \cup G_2 : P^* \in G_1 \in \mathscr{G}_1 \text{ and } G_2 \in \mathscr{G}_2\} \text{ and}$$
$$\mathscr{F} = \mathscr{F}_1^* \cup \mathscr{F}_2 \cup \{F_1 \cup F_2 : F_1 \in \mathscr{F}_1^* \text{ and } F_2 \in \mathscr{F}_2\}, \text{ where}$$
$$\mathscr{G}_1^* = \{G \setminus \{P^*\} : G \in \mathscr{G}_1 \text{ and } G \setminus \{P^*\} \neq \varnothing\} \text{ and } \mathscr{F}_1^* = \left\{F \in \mathscr{F}_1 : (P^*) \not\subseteq \bigcup_{Q\in F}(Q)\right\}.$$

We now give another corollary to Theorem 5.2.3 for the special case of (t, w)-KDPs.

Corollary 5.2.5. *Let the finite incidence structures $\mathscr{K}_1 = (\mathscr{P}_1, \mathscr{B}_1, \mathscr{I}_1)$, where $P^* \in \mathscr{P}_1$, and $\mathscr{K}_2 = (\mathscr{P}_2, \mathscr{B}_2, \mathscr{I}_2)$, where $\mathscr{P}_1 \cap \mathscr{P}_2 = \varnothing$, be (t, w)-KDPs for $t \leq \min(|\mathscr{P}_1| - w, |\mathscr{P}_2| - w)$. Let $\mathscr{P} = [\mathscr{P}_1 \setminus \{P^*\}] \cup \mathscr{P}_2, \mathscr{B} = [\mathscr{B}_1 \setminus (P^*)] \cup [(P^*) \times \mathscr{B}_2]$ and the incidence relation $\mathscr{I}$ be defined as in Theorem 5.2.3. Then $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is also a (t, w)-KDP.*

Our final result in this section generalises [60, Construction 1.7]. Here we reduce the size of both original block sets before taking the cross product. In this way, we reduce the number of blocks in the resultant $(\mathscr{G}, \mathscr{F})$-KDP even further.

Theorem 5.2.6. *Let the finite incidence structures $\mathscr{K}_1 = (\mathscr{P}_1, \mathscr{B}_1, \mathscr{I}_1)$, where $P^* \in \mathscr{P}_1$, and $\mathscr{K}_2 = (\mathscr{P}_2, \mathscr{B}_2, \mathscr{I}_2)$, where $Q^* \in \mathscr{P}_2$ and $\mathscr{P}_1 \cap \mathscr{P}_2 = \varnothing$, be a tight $(\mathscr{G}_1, \mathscr{F}_1)$-KDP and a tight $(\mathscr{G}_2, \mathscr{F}_2)$-KDP, respectively.*
Let $\mathscr{P} = \mathscr{P}_1 \cup \mathscr{P}_2, \mathscr{B} = [\mathscr{B}_1 \setminus (P^*)] \cup [\mathscr{B}_2 \setminus (Q^*)] \cup [(P^*) \times (Q^*)]$ and the incidence relation $\mathscr{I}$ be defined by:
(i) For $P \in \mathscr{P}_1$ and $x \in \mathscr{B}_1 \setminus (P^*)$, x is incident with P if, and only if, $(P, x) \in \mathscr{I}_1$;
(ii) For $P \in \mathscr{P}_1$ and $(x, y) \in (P^*) \times (Q^*)$, (x, y) is incident with P if, and only if, $(P, x) \in \mathscr{I}_1$;
(iii) For $P \in \mathscr{P}_2$ and $y \in \mathscr{B}_2 \setminus (Q^*)$, y is incident with P if, and only if, $(P, y) \in \mathscr{I}_2$;
(iv) For $P \in \mathscr{P}_2$ and $(x, y) \in (P^*) \times (Q^*)$, (x, y) is incident with P if, and only if, $(P, y) \in \mathscr{I}_2$.
Then $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP with

$$\mathscr{G} = \mathscr{G}_1 \cup \mathscr{G}_2 \cup \{G_1 \cup G_2 : P^* \in G_1 \in \mathscr{G}_1 \text{ and } Q^* \in G_2 \in \mathscr{G}_2\} \text{ and}$$
$$\mathscr{F} = \mathscr{F}_1^* \cup \mathscr{F}_2^* \cup \ \{F_1 \cup F_2 : F_1 \in \mathscr{F}_1^* \text{ and } F_2 \in \mathscr{F}_2^*\}, \text{ where}$$
$$\mathscr{F}_1^* = \left\{ F_1 \in \mathscr{F}_1 : (P^*) \not\subseteq \bigcup_{Q \in F_1} (Q) \right\} \text{ and } \mathscr{F}_2^* = \left\{ F_2 \in \mathscr{F}_2 : (Q^*) \not\subseteq \bigcup_{Q \in F_2} (Q) \right\}.$$

Proof. The proof of this theorem is similar to that of Theorem 5.2.3. □

In a similar way to Theorem 5.2.3 we note that the combined point set in Theorem 5.2.6 includes the points P^* and Q^*. In order to give a true generalisation of [60, Construction 1.7] we again use Proposition 3.1.6 to get the following corollary.

Corollary 5.2.7. *Let the finite incidence structures $\mathscr{K}_1 = (\mathscr{P}_1, \mathscr{B}_1, \mathscr{I}_1)$, where $P^* \in \mathscr{P}_1$, and $\mathscr{K}_2 = (\mathscr{P}_2, \mathscr{B}_2, \mathscr{I}_2)$, where $Q^* \in \mathscr{P}_2$ and $\mathscr{P}_1 \cap \mathscr{P}_2 = \varnothing$, be a tight $(\mathscr{G}_1, \mathscr{F}_1)$-KDP and a tight $(\mathscr{G}_2, \mathscr{F}_2)$-KDP, respectively. Let $\mathscr{P} = [\mathscr{P}_1 \setminus \{P^*\}] \cup [\mathscr{P}_2 \setminus \{Q^*\}], \mathscr{B} = [\mathscr{B}_1 \setminus (P^*)] \cup [\mathscr{B}_2 \setminus (Q^*)] \cup [(P^*) \times (Q^*)]$ and the* *incidence relation $\mathscr{I}$ be defined as in Theorem 5.2.6. Then $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP with*

$$\mathscr{G} = \mathscr{G}_1^* \cup \mathscr{G}_2^* \cup \big\{[G_1 \setminus \{P^*\}] \cup [G_2 \setminus \{Q^*\}] \in 2^{\mathscr{P}} \setminus \{\varnothing\} : P^* \in G_1 \in \mathscr{G}_1,\ Q^* \in G_2 \in \mathscr{G}_2\big\}$$

$$\text{and } \mathscr{F} = \mathscr{F}_1^* \cup \mathscr{F}_2^* \cup \{F_1 \cup F_2 : F_1 \in \mathscr{F}_1^* \text{ and } F_2 \in \mathscr{F}_2^*\},$$

$$\text{where } \mathscr{G}_1^* = \{G_1 \setminus \{P^*\} : G_1 \in \mathscr{G}_1 \text{ and } G_1 \setminus \{P^*\} \neq \varnothing\},$$

$$\mathscr{G}_2^* = \{G_2 \setminus \{Q^*\} : G_2 \in \mathscr{G}_2 \text{ and } G_2 \setminus \{Q^*\} \neq \varnothing\},$$

$$\mathscr{F}_1^* = \Big\{F_1 \in \mathscr{F}_1 : (P^*) \nsubseteq \bigcup_{Q \in F_1} (Q)\Big\} \text{ and } \mathscr{F}_2^* = \Big\{F_2 \in \mathscr{F}_2 : (Q^*) \nsubseteq \bigcup_{Q \in F_2} (Q)\Big\}.$$

We now give our final corollary of this section. Corollary 5.2.8 generalises [60, Construction 1.7] for the special case of (t, w)-KDPs.

Corollary 5.2.8. *Let the finite incidence structures $\mathscr{K}_1 = (\mathscr{P}_1, \mathscr{B}_1, \mathscr{I}_1)$, where $P^* \in \mathscr{P}_1$, and $\mathscr{K}_2 = (\mathscr{P}_2, \mathscr{B}_2, \mathscr{I}_2)$, where $Q^* \in \mathscr{P}_2$ and $\mathscr{P}_1 \cap \mathscr{P}_2 = \varnothing$, be (t, w)-KDPs for $t \leq \min(|\mathscr{P}_1| - w, |\mathscr{P}_2| - w)$. Let $\mathscr{P} = [\mathscr{P}_1 \setminus \{P^*\}] \cup [\mathscr{P}_2 \setminus \{Q^*\}]$, $\mathscr{B} = [\mathscr{B}_1 \setminus (P^*)] \cup [\mathscr{B}_2 \setminus (Q^*)] \cup [(P^*) \times (Q^*)]$ and the incidence relation $\mathscr{I}$ be defined as in Theorem 5.2.3. Then $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is also a (t, w)-KDP.*

Within this section we have generalised the three constructions of Mitchell and Piper [60]. The following example demonstrates the increasing efficiency of these generalised constructions.

Example 5.2.1. Let $\mathscr{K}_1 = (\mathscr{P}_1, \mathscr{B}_1, \mathscr{I}_1)$ and $\mathscr{K}_2 = (\mathscr{P}_2, \mathscr{B}_2, \mathscr{I}_2)$ be trivial 2-KDPs on four points and six blocks. Then, $\mathscr{K}_1$ and $\mathscr{K}_2$ are both tight $(2, 2)$-KDPs. Starting with $\mathscr{K}_1$ and $\mathscr{K}_2$, Theorem 5.2.1 would construct a $(2, 2)$-KDP on eight points and 36 blocks. Theorem 5.2.3 would construct a $(2, 2)$-KDP on eight points and 21 blocks and Theorem 5.2.6 would construct a $(2, 2)$-KDP on eight points and 15 blocks.

In general, if we denote the number of blocks from $\mathscr{B}_1$ that are incident with the point P^* by $r(P^*)$ and the number of blocks from $\mathscr{B}_2$ that are incident with the point Q^* by $r(Q^*)$, then we can measure the total number of points and the total number of blocks in the $(\mathscr{G},\mathscr{F})$-KDPs resulting from each of the constructions in this section.

	Number of Points	**Number of Blocks**
Theorem 5.2.1 $(\mathscr{G},\mathscr{F})$-KDPs	$\lvert\mathscr{P}_1\rvert+\lvert\mathscr{P}_2\rvert$	$\lvert\mathscr{B}_1\rvert\lvert\mathscr{B}_2\rvert$
Corollary 5.2.2 (t,w)-KDPs	$\lvert\mathscr{P}_1\rvert+\lvert\mathscr{P}_2\rvert$	$\lvert\mathscr{B}_1\rvert\lvert\mathscr{B}_2\rvert$
Theorem 5.2.3 $(\mathscr{G},\mathscr{F})$-KDPs	$\lvert\mathscr{P}_1\rvert+\lvert\mathscr{P}_2\rvert$	$\lvert\mathscr{B}_1\rvert+r(P^*)(\lvert\mathscr{B}_2\rvert-1)$
Corollary 5.2.4 $(\mathscr{G},\mathscr{F})$-KDPs	$\lvert\mathscr{P}_1\rvert+\lvert\mathscr{P}_2\rvert-1$	$\lvert\mathscr{B}_1\rvert+r(P^*)(\lvert\mathscr{B}_2\rvert-1)$
Corollary 5.2.5 (t,w)-KDPs	$\lvert\mathscr{P}_1\rvert+\lvert\mathscr{P}_2\rvert-1$	$\lvert\mathscr{B}_1\rvert+r(P^*)(\lvert\mathscr{B}_2\rvert-1)$
Theorem 5.2.6 $(\mathscr{G},\mathscr{F})$-KDPs	$\lvert\mathscr{P}_1\rvert+\lvert\mathscr{P}_2\rvert$	$\lvert\mathscr{B}_1\rvert+\lvert\mathscr{B}_2\rvert+(r(P^*)-1)(r(Q^*)-1)-1$
Corollary 5.2.7 $(\mathscr{G},\mathscr{F})$-KDPs	$\lvert\mathscr{P}_1\rvert+\lvert\mathscr{P}_2\rvert-2$	$\lvert\mathscr{B}_1\rvert+\lvert\mathscr{B}_2\rvert+(r(P^*)-1)(r(Q^*)-1)-1$
Corollary 5.2.8 (t,w)-KDPs	$\lvert\mathscr{P}_1\rvert+\lvert\mathscr{P}_2\rvert-2$	$\lvert\mathscr{B}_1\rvert+\lvert\mathscr{B}_2\rvert+(r(P^*)-1)(r(Q^*)-1)-1$

Note that, in Theorem 5.2.3 and Theorem 5.2.6, (and the corresponding corollaries), when we choose the points P^* and Q^* from the incidence structures $\mathscr{K}_1$ and $\mathscr{K}_2$ respectively, if we choose the points incident with the least number of blocks, then we minimise the total number of blocks in the constructed incidence structure $\mathscr{K}$. That is, if we have an estimate for the number of blocks incident with each point, then we have a method for minimising the number of blocks in the constructed $(\mathscr{G},\mathscr{F})$-KDP. In Chapter 6 we investigate bounds on the number of blocks incident with a given point and, the total number of blocks in a $(\mathscr{G},\mathscr{F})$-KDP.

5.3 Direct Constructions

The origins of the family of constructions in this section stem from convex analysis [23, 35, 41]. More specifically, the separation theorems that tell us that disjoint *convex sets* can be separated by *half spaces*, (equivalent to the Hahn-Banach Theorem, [23, Page 58], [35, Page 69] and [41, Page 118]).

We begin with some basic definitions.

Definition 5.3.1. *A subset $\mathcal{C}$ of $\mathbb{R}^n$ is called* **convex** *if for each $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$ and $\lambda \in [0, 1]$,*

$$\lambda \boldsymbol{x} + (1 - \lambda)\boldsymbol{y} \in \mathcal{C}.$$

A *half space* in $\mathbb{R}^n$ essentially splits $\mathbb{R}^n$ into two disjoint convex sets.

Definition 5.3.2. *A subset $\mathcal{H}$ of $\mathbb{R}^n$ is called a* **closed half space** *if there exists a vector $\boldsymbol{a} \in \mathbb{R}^n$ and an $\alpha \in \mathbb{R}$ such that,*

$$\mathcal{H} = \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{a} \cdot \boldsymbol{x} \le \alpha\}.$$

Within this section we shall consider a discrete analogue of convexity and of the following *separation theorem.*

Result 5.3.3. *Given any two disjoint, closed and bounded convex subsets $\mathcal{A}$ and $\mathcal{B}$ of $\mathbb{R}^n$ there exists a closed half space $\mathcal{H}$ of $\mathbb{R}^n$ such that:*

$$\text{(i) } \mathcal{A} \subseteq \mathcal{H} \quad \text{and} \quad \text{(ii) } \mathcal{H} \cap \mathcal{B} = \varnothing.$$

The fact that separation theorems might be useful in this setting, emanates from the fact that there are many more pairs of disjoint convex sets than there are half spaces. We treat $\mathbb{Z}^n$ as a group under addition and, in Definition 5.3.6, we describe how to generate a finite incidence structure from any finite subset of $\mathbb{Z}^n$. For sets $A, B \subseteq \mathbb{Z}^n$ we shall set

$$A + B = \{\boldsymbol{x} \in \mathbb{Z}^n : \boldsymbol{x} = \boldsymbol{a} + \boldsymbol{b} \text{ for some } \boldsymbol{a} \in A \text{ and } \boldsymbol{b} \in B\}$$

$$\text{and } -A = \{\boldsymbol{x} \in \mathbb{Z}^n : \boldsymbol{x} = -\boldsymbol{a} \text{ for some } \boldsymbol{a} \in A\}.$$

Also, in this section, if $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ and $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)$ are elements of $\mathbb{Z}^n$, then we let "$\leq$" be the partial order on $\mathbb{Z}^n$ defined by $\boldsymbol{a} \leq \boldsymbol{b}$ if, and only if, $a_i \leq b_i$ for all $1 \leq i \leq n$. In addition to this, we define $[\boldsymbol{a}, \boldsymbol{b}] = \{\boldsymbol{x} \in \mathbb{Z}^n : \boldsymbol{a} \leq \boldsymbol{x} \leq \boldsymbol{b}\}$.

The following intuitive lemma is a natural result that probably exists in the literature. However, due to the lack of a convenient reference, we have included a complete proof of Lemma 5.3.4.

Lemma 5.3.4. *For $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d} \in \mathbb{Z}^n$, if $\boldsymbol{a} \leq \boldsymbol{b}$ and $\boldsymbol{c} \leq \boldsymbol{d}$ then*

$$[\boldsymbol{a}, \boldsymbol{b}] + [\boldsymbol{c}, \boldsymbol{d}] = [\boldsymbol{a} + \boldsymbol{c}, \boldsymbol{b} + \boldsymbol{d}].$$

Proof. It is immediate that $[\boldsymbol{a}, \boldsymbol{b}] + [\boldsymbol{c}, \boldsymbol{d}] \subseteq [\boldsymbol{a} + \boldsymbol{c}, \boldsymbol{b} + \boldsymbol{d}]$, so it only remains to show that $[\boldsymbol{a} + \boldsymbol{c}, \boldsymbol{b} + \boldsymbol{d}] \subseteq [\boldsymbol{a}, \boldsymbol{b}] + [\boldsymbol{c}, \boldsymbol{d}]$. Suppose, in order to obtain a contradiction, that $[\boldsymbol{a}, \boldsymbol{b}] + [\boldsymbol{c}, \boldsymbol{d}] \subsetneqq [\boldsymbol{a} + \boldsymbol{c}, \boldsymbol{b} + \boldsymbol{d}]$, in which case there exists $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in [\boldsymbol{a} + \boldsymbol{c}, \boldsymbol{b} + \boldsymbol{d}] \setminus ([\boldsymbol{a}, \boldsymbol{b}] + [\boldsymbol{c}, \boldsymbol{d}])$.

Let $X = \{\boldsymbol{y'} \in [\boldsymbol{a}, \boldsymbol{b}] + [\boldsymbol{c}, \boldsymbol{d}] : \boldsymbol{y'} \leq \boldsymbol{x}\}$. Then $X \neq \varnothing$, since $\boldsymbol{a} + \boldsymbol{c} \in X$. Now $(X, \leq)$ is a non-empty finite partially ordered set and so has a maximal element $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$. Then, $\boldsymbol{y} < \boldsymbol{x}$ and so $y_i \leq x_i \leq b_i + d_i$ for all $1 \leq i \leq n$, and $y_j < x_j \leq b_j + d_j$ for some $1 \leq j \leq n$.

By the definition of $\boldsymbol{y}$, there exists $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in [\boldsymbol{a}, \boldsymbol{b}]$ and $\boldsymbol{w} = (w_1, w_2, \ldots, w_n) \in [\boldsymbol{c}, \boldsymbol{d}]$ such that $\boldsymbol{y} = \boldsymbol{v} + \boldsymbol{w}$. In particular $v_j + w_j < x_j \leq b_j + d_j$. Hence, either $v_j < b_j$ or $w_j < d_j$. In either case, we can see that if $\boldsymbol{y'} = (y'_1, y'_2, \ldots, y'_n) \in [\boldsymbol{a}+\boldsymbol{c}, \boldsymbol{b}+\boldsymbol{d}]$ is defined by, $y'_i = y_i$ for $i \neq j$ and $y'_j = y_j + 1$ then $\boldsymbol{y'} \in X$ since $\boldsymbol{y'} \leq \boldsymbol{x}$ and $\boldsymbol{y'} \in [\boldsymbol{a}, \boldsymbol{b}] + [\boldsymbol{c}, \boldsymbol{d}]$. However, $\boldsymbol{y} < \boldsymbol{y'} \in X$ which contradicts the maximality of $\boldsymbol{y}$. Therefore, $[\boldsymbol{a}, \boldsymbol{b}] + [\boldsymbol{c}, \boldsymbol{d}] = [\boldsymbol{a} + \boldsymbol{c}, \boldsymbol{b} + \boldsymbol{d}]$. □

In the following lemma we will use the fact that for $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d} \in \mathbb{Z}^n$,

if $\boldsymbol{a} \leq \boldsymbol{b}$ and $\boldsymbol{c} \leq \boldsymbol{d}$, then $[\boldsymbol{a}, \boldsymbol{b}] \cap [\boldsymbol{c}, \boldsymbol{d}] = \varnothing$ if, and only if,
$\boldsymbol{0} \notin [\boldsymbol{a}, \boldsymbol{b}] - [\boldsymbol{c}, \boldsymbol{d}] = [\boldsymbol{a}, \boldsymbol{b}] + [-\boldsymbol{d}, -\boldsymbol{c}] = [\boldsymbol{a} - \boldsymbol{d}, \boldsymbol{b} - \boldsymbol{c}]$ (from Lemma 5.3.4).

Lemma 5.3.5. *Suppose that* $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d} \in \mathbb{Z}^n$ *satisfy* $\boldsymbol{a} \leq \boldsymbol{b}$ *and* $\boldsymbol{c} \leq \boldsymbol{d}$. *If* $[\boldsymbol{a}, \boldsymbol{b}] \cap [\boldsymbol{c}, \boldsymbol{d}] = \varnothing$, *then there exists* $1 \leq i \leq n$ *such that either* $d_i < a_i$ *or* $b_i < c_i$.

Proof. Since $[\boldsymbol{a}, \boldsymbol{b}] \cap [\boldsymbol{c}, \boldsymbol{d}] = \varnothing$, $\mathbf{0} \notin [\boldsymbol{a}-\boldsymbol{d}, \boldsymbol{b}-\boldsymbol{c}]$. Now, since $\mathbf{0} \notin [\boldsymbol{a}-\boldsymbol{d}, \boldsymbol{b}-\boldsymbol{c}]$, there exists $1 \leq i \leq n$ such that $0 \notin [a_i-d_i, b_i-c_i]$. Therefore, either $0 < a_i-d_i$ or $b_i - c_i < 0$. That is, either $d_i < a_i$ or $b_i < c_i$. □

In order to simplify the statement of our next theorem we introduce some preliminary notation.

Definition 5.3.6. *For any* $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}^n$, *where* $\boldsymbol{a} \leq \boldsymbol{b}$, *we let* $\mathscr{K}_{\boldsymbol{a}}^{\boldsymbol{b}} = (\mathscr{P}_{\boldsymbol{a}}^{\boldsymbol{b}}, \mathscr{B}_{\boldsymbol{a}}^{\boldsymbol{b}}, \mathscr{I}_{\boldsymbol{a}}^{\boldsymbol{b}})$ *be the finite incidence structure defined by:*

$$\mathscr{P}_{\boldsymbol{a}}^{\boldsymbol{b}} = [\boldsymbol{a}, \boldsymbol{b}],$$

$$\mathscr{B}_{\boldsymbol{a}}^{\boldsymbol{b}} = \{L_i^j : 1 \leq i \leq n \text{ and } a_i+1 \leq j \leq b_i\} \cup \{R_i^j : 1 \leq i \leq n \text{ and } a_i \leq j \leq b_i-1\}$$

where for each $1 \leq i \leq n$, $L_i^j = \{(x_1, x_2, \ldots, x_n) \in \mathscr{P}_{\boldsymbol{a}}^{\boldsymbol{b}} : x_i \geq j\}$ *for* $a_i+1 \leq j \leq b_i$ *and* $R_i^j = \{(x_1, x_2, \ldots, x_n) \in \mathscr{P}_{\boldsymbol{a}}^{\boldsymbol{b}} : x_i \leq j\}$ *for* $a_i \leq j \leq b_i-1$,

and $\mathscr{I}_{\boldsymbol{a}}^{\boldsymbol{b}} \subseteq \mathscr{P}_{\boldsymbol{a}}^{\boldsymbol{b}} \times \mathscr{B}_{\boldsymbol{a}}^{\boldsymbol{b}}$ *is defined by* $(\boldsymbol{x}, B) \in \mathscr{I}_{\boldsymbol{a}}^{\boldsymbol{b}}$ *if, and only if,* $\boldsymbol{x} \in B$.

Theorem 5.3.7. *If* $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}^n$ *and* $\boldsymbol{a} \leq \boldsymbol{b}$, *then the finite incidence structure* $\mathscr{K}_{\boldsymbol{a}}^{\boldsymbol{b}} = (\mathscr{P}_{\boldsymbol{a}}^{\boldsymbol{b}}, \mathscr{B}_{\boldsymbol{a}}^{\boldsymbol{b}}, \mathscr{I}_{\boldsymbol{a}}^{\boldsymbol{b}})$ *is a* $(\mathscr{G}, \mathscr{F})$*-KDP, where*

$$\mathscr{G} = \mathscr{F} = \{[\boldsymbol{c}, \boldsymbol{d}] : \boldsymbol{a} \leq \boldsymbol{c} \leq \boldsymbol{d} \leq \boldsymbol{b}\}.$$

Proof. Suppose that the finite incidence structure $\mathscr{K}_{\boldsymbol{a}}^{\boldsymbol{b}} = (\mathscr{P}_{\boldsymbol{a}}^{\boldsymbol{b}}, \mathscr{B}_{\boldsymbol{a}}^{\boldsymbol{b}}, \mathscr{I}_{\boldsymbol{a}}^{\boldsymbol{b}})$ is defined as above and that $\mathscr{G}$ and $\mathscr{F}$ are defined as in the statement of the theorem.

Suppose also that $G \in \mathscr{G}$, $F \in \mathscr{F}$ and $G \cap F = \varnothing$. Then, $G = [\boldsymbol{c}, \boldsymbol{d}]$ and $F = [\boldsymbol{e}, \boldsymbol{f}]$ for some $\boldsymbol{a} \leq \boldsymbol{c} \leq \boldsymbol{d} \leq \boldsymbol{b}$ and $\boldsymbol{a} \leq \boldsymbol{e} \leq \boldsymbol{f} \leq \boldsymbol{b}$. Then, by Lemma 5.3.5 we know that there exists $1 \leq i \leq n$ such that either $f_i < c_i$ or $d_i < e_i$. If $f_i < c_i$, then $[\boldsymbol{c}, \boldsymbol{d}] \subseteq L_i^{c_i}$ and $L_i^{c_i} \cap [\boldsymbol{e}, \boldsymbol{f}] = \varnothing$. On the other hand, if $d_i < e_i$, then $[\boldsymbol{c}, \boldsymbol{d}] \subseteq R_i^{d_i}$ and $R_i^{d_i} \cap [\boldsymbol{e}, \boldsymbol{f}] = \varnothing$. Therefore, in either case there exists a $B \in \mathscr{B}_{\boldsymbol{a}}^{\boldsymbol{b}}$ such that $[\boldsymbol{c}, \boldsymbol{d}] \subseteq B$ and $B \cap [\boldsymbol{e}, \boldsymbol{f}] = \varnothing$. That is, $B \in \bigcap_{P \in G}(P) \setminus \bigcup_{Q \in F}(Q)$ and hence $\mathscr{K}_{\boldsymbol{a}}^{\boldsymbol{b}}$ is a $(\mathscr{G}, \mathscr{F})$-KDP. $\square$

The following one dimensional example demonstrates Theorem 5.3.7.

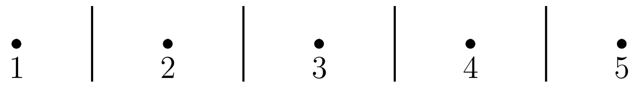
Example 5.3.1. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be the finite incidence structure defined by the following:

$$\mathscr{P} = \{1, 2, 3, 4, 5\},$$
$$\mathscr{B} = \big\{\{1\}, \{1, 2\}, \{1, 2, 3\}, \{1, 2, 3, 4\}, \{2, 3, 4, 5\}, \{3, 4, 5\}, \{4, 5\}, \{5\}\big\},$$

and for any $P \in \mathscr{P}$ and $B \in \mathscr{B}$, $(P, B) \in \mathscr{I}$ if, and only if, $P \in B$.
Then, $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP where,

$$\begin{aligned}\mathscr{G} = \mathscr{F} = \big\{&\{1\},\ \{2\},\ \{3\},\ \{4\},\ \{5\},\ \{1,2\},\ \{2,3\},\ \{3,4\},\ \{4,5\},\\ &\{1,2,3\},\ \{2,3,4\},\ \{3,4,5\},\ \{1,2,3,4\},\ \{2,3,4,5\},\ \{1,2,3,4,5\}\big\}.\end{aligned}$$

More intuitively, we can consider the points in a line, as shown below. Each point can be separated from the next, as shown by a vertical line. Every set of points to the left of a vertical line, or to the right of a vertical line, make up the blocks in the block set. The privileged and forbidden subsets are all the subsets of consecutive points.



In a similar way to Example 5.3.1, in two dimensions, the privileged and forbidden subsets are all the subsets of adjacent points that form a rectangle. Also, in three dimensions, the privileged and forbidden subsets are all the subsets of adjacent points that form a three dimensional box. That is, Theorem 5.3.7 enables secure communication for "neighbourhoods" of users. Due to this, we have a family of $(\mathscr{G}, \mathscr{F})$-KDPs that potentially lends itself to applications such as certain types of wireless sensor networks, where nodes relay data to adjacent (or “neighbouring”) nodes.

In Theorem 5.3.7, it is possible to precisely calculate $|\mathscr{G}|, |\mathscr{F}|$ and $|\mathscr{B}|$, as shown in the following remark.

Remark 5.3.8. In Theorem 5.3.7,

$$|\mathscr{G}| = |\mathscr{F}| = \prod_{i=1}^{n} \left[\frac{(b_i - a_i + 1)(b_i - a_i + 2)}{2} \right] \quad \text{and} \quad |\mathscr{B}| = \sum_{i=1}^{n} 2(b_i - a_i).$$

The fact that we can precisely calculate the number of blocks in the construction from Theorem 5.3.7 means that we have an insight into the efficiency of the construction. It is easy to see from Remark 5.3.8 that the efficiency of the construction from Theorem 5.3.7 improves as the number of dimensions increases. We can combine Theorem 5.3.7 with other results from this chapter in order to construct other $(\mathscr{G}, \mathscr{F})$-KDPs. More specifically, if we want to construct $(\mathscr{G}, w)$-KDPs or $(t, \mathscr{F})$-KDPs, then Theorem 5.3.7 can be used in conjunction with Theorem 5.1.1 or Theorem 5.1.4 respectively. Also, by considering the following definition, we can potentially extend the applicability of Theorem 5.3.7.

Definition 5.3.9. *For a set $\varnothing \neq A \subseteq [\boldsymbol{a}, \boldsymbol{b}] \subseteq \mathbb{Z}^n$ we shall let*

$$\operatorname{co}(A) = \big\{ \boldsymbol{x} \in [\boldsymbol{a}, \boldsymbol{b}] : \min\{a_i : \boldsymbol{a} \in A\} \leq x_i \leq \max\{a_i : \boldsymbol{a} \in A\} \big\}.$$

Suppose that we are given a set $\mathscr{P}$ of points and families $\mathscr{G}$ and $\mathscr{F}$ of non-empty subsets of $\mathscr{P}$, as well as a 1-to-1 mapping $\varphi : \mathscr{P} \to [\boldsymbol{a}, \boldsymbol{b}] \subseteq \mathbb{Z}^n$ such that $\operatorname{co}[\varphi(\mathrm{G})] \cap \operatorname{co}[\varphi(\mathrm{F})] = \varnothing$ whenever $G \in \mathscr{G}$, $F \in \mathscr{F}$ and $G \cap F = \varnothing$. Then, we can use $\mathscr{K}_{\boldsymbol{a}}^{\boldsymbol{b}}$ to construct an incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ that is a $(\mathscr{G}, \mathscr{F})$-KDP, in the following way:

Let $\mathscr{B} = \mathscr{B}_{\boldsymbol{a}}^{\boldsymbol{b}}$ and let $\mathscr{I} \subseteq \mathscr{P} \times \mathscr{B}$ is defined by $(P, B) \in \mathscr{I}$ if, and only if, $(\varphi(P), B) \in \mathscr{I}_{\boldsymbol{a}}^{\boldsymbol{b}}$, (i.e. $\varphi(P) \in B$). It is now routine to check that $\mathscr{K}$ is indeed a $(\mathscr{G}, \mathscr{F})$-KDP.

This raises the question of how to construct such a mapping φ, (if indeed such a mapping exists at all) given the sets $\mathscr{P}$, $\mathscr{G}$ and $\mathscr{F}$. This question is not pursued here, however it does seem worthy of further investigation.

It would also seem reasonable that other "convex structures" (see [27]) might be useful in the construction of $(\mathscr{G}, \mathscr{F})$-KDPs, where the $\mathscr{G}$'s and $\mathscr{F}$'s correspond to collections of convex sets (in the convex structure) and the blocks correspond to half spaces. All that is required is for an appropriate separation theorem to hold in the convex structure. Theorem 5.3.7 is just one example.

Chapter 6

Bounds

In this chapter we present various bounds demonstrating the efficiency levels of $(\mathscr{G}, \mathscr{F})$-KDPs. As introduced in Section 1.3.3, the network storage and user storage requirements in a KPS are the main measures of efficiency of a scheme. In a $(\mathscr{G}, \mathscr{F})$-KDP these measures correspond to the total number of blocks in the incidence structure and the number of blocks incident with each point. The fewer the blocks, the more efficient a $(\mathscr{G}, \mathscr{F})$-KDP is considered to be, and an efficient $(\mathscr{G}, \mathscr{F})$-KDP is seen as a "good" $(\mathscr{G}, \mathscr{F})$-KDP. Therefore, within this chapter, we find bounds on these efficiency measures and aim to show how efficient we can expect a $(\mathscr{G}, \mathscr{F})$-KDP to be.

Other authors have also found bounds of this type for $(\mathscr{G}, \mathscr{F})$-KDPs. In [78], Ruszinkó gives an upper bound for (t, w)-CFFs and in [26], Dyer *et al.* use probabilistic techniques to find bounds and give existence results for (t, w)-CFFs. Quinn presents several lower bounds for (t, w)-KDPs in [71] and [73] and in [85] and [86], Stinson *et al.* provide various bounds for (t, w)-CFFs. Within this chapter we are able to generalise some of these known results to $(\mathscr{G}, \mathscr{F})$-KDPs and construct some new bounds of our own.

As well as bounds indicating the efficiency of $(\mathscr{G}, \mathscr{F})$-KDPs, some generic techniques that can be applied to $(\mathscr{G}, \mathscr{F})$-KDPs in order to improve their efficiency are also considered in the literature. In [71] and [73], Quinn introduces a technique for improving the efficiency of a KDP based upon the idea of using an *information map* in order to reduce the information content of the keys. In [82] and [84], Stinson *et al.* introduce a technique based on the use of *resilient functions*. This method allows for a trade off between the level of security in a $(\mathscr{G}, \mathscr{F})$-KDP and the amount of key storage. Within this thesis we do not attempt to improve on these already strong results, instead we simply acknowledge that they can be applied to our $(\mathscr{G}, \mathscr{F})$-KDPs in order to improve their efficiency.

We begin this chapter by considering bounds for general $(\mathscr{G}, \mathscr{F})$-KDPs. Without introducing any major constraints on the sets of privileged and forbidden subsets, we are able to produce some informative results. After this, we introduce the constraint that the set of privileged subsets forms a Sperner system (which encompasses the case of (t, w)-KDPs). As a consequence of this constraint we are able to give improved bounds for $(\mathscr{G}, \mathscr{F})$-KDPs. We conclude the chapter by reviewing some bounds that we essentially get for "free". By generalising the notions of internal and external structures and using some bounds from earlier in the chapter, we are able to give some new bounds estimating (among other things) the number of blocks incident with each point in a $(\mathscr{G}, w)$-KDP.

The main results in this chapter are:

1. Theorem 6.1.4 - In this theorem we provide a lower bound on the number of blocks required for any $(\mathscr{G}, \mathscr{F})$-KDP with the property that, for every $G \in \mathscr{G}$ and for some fixed $n \in \mathbb{N}$, there exist $F_1, F_2, \ldots, F_n \in \mathscr{F}$ (not necessarily distinct) such that $\mathscr{P} \setminus G = \bigcup_{1 \le j \le n} F_j$.

2. Theorem 6.1.8 - In this theorem we take the symmetric difference of certain block sets (those incident with all points in a privileged subset) in order to find a new bound for completely general $(\mathscr{G}, w)$-KDPs.

3. Corollary 6.2.6 - In this corollary we make use of several earlier results,

(Corollary 5.1.11, Corollary 5.1.23, Corollary 6.2.4 and Theorem 6.2.5) and present our best bound for (t, t)-KDPs.

4. Theorem 6.2.9 - In this theorem we use techniques of Füredi in order to give a Quinn style bound for $(\mathscr{G}, w)$-KDPs, under the additional assumption that the set of privileged subsets forms a Sperner system. This is our best bound for $(\mathscr{G}, w)$-KDPs in the case when $|\mathscr{G}| \approx w^2$.

For a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ we use the following notation :

- $b = |\mathscr{B}|$ (the total number of blocks in $\mathscr{K}$);
- $r(P) = |(P)|$ (the number of blocks incident with the point $P \in \mathscr{P}$).

Note that if the incidence structure is indexed, as in $\mathscr{K}^* = (\mathscr{P}^*, \mathscr{B}^*, \mathscr{I}^*)$ or $\mathscr{K}_* = (\mathscr{P}_*, \mathscr{B}_*, \mathscr{I}_*)$, then we let $|\mathscr{B}^*| = b^*$ and $|\mathscr{B}_*| = b_*$.

As will be seen in Section 6.3, calculating bounds on the number of blocks incident with each point in a $(\mathscr{G}, \mathscr{F})$-KDP is equivalent to calculating bounds on the total number of blocks in another $(\mathscr{G}, \mathscr{F})$-KDP. Therefore, we shall be focusing our attention on finding bounds for the total number of blocks in a given $(\mathscr{G}, \mathscr{F})$-KDP.

6.1 General Bounds

In this section we attempt to obtain lower bounds on the total number of blocks required for the construction of a completely general $(\mathscr{G}, \mathscr{F})$-KDP (that is, a $(\mathscr{G}, \mathscr{F})$-KDP with no constraints on the sets of privileged and forbidden subsets). Unfortunately, in order to make progress, it was necessary for us to impose some natural restrictions on the set of forbidden subsets. With these added restrictions we have been able to obtain a number of lower bounds on the number of blocks required for a given $(\mathscr{G}, \mathscr{F})$-KDP. Our first result is also our most general result.

Theorem 6.1.1. *Let a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a $(\mathscr{G}, \mathscr{F})$-KDP with the property that if $G, G' \in \mathscr{G}$ and $G \neq G'$ then there exists an $F \in \mathscr{F}$ such that either (i) $G \cap F \neq \varnothing$ and $G' \cap F = \varnothing$ or (ii) $G \cap F = \varnothing$ and $G' \cap F \neq \varnothing$. Then, $b \geq \log_2 |\mathscr{G}|$.*

Proof. We know from Observation 3.3.12 that for a $(\mathscr{G}, \mathscr{F})$-KDP, as defined in the statement of the theorem, the mapping $G \to \bigcap_{P \in G}(P)$ from $\mathscr{G}$ into subsets of $\mathscr{B}$ is 1-to-1. Therefore,

$$|\mathscr{G}| = \left|\{\bigcap_{P \in G}(P) : G \in \mathscr{G}\}\right| \leq |2^{\mathscr{B}}| = 2^b$$

and so $b \geq \log_2 |\mathscr{G}|$. □

An important special case of this general theorem is given next.

Corollary 6.1.2. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP, then $b \geq \log_2 |\mathscr{G}|$.*

Next, we combine some of our results from earlier in this thesis to give a new and reasonably general approach to finding the minimum number of blocks required for the construction of a $(\mathscr{G}, \mathscr{F})$-KDP.

Definition 6.1.3. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then we define $\mathscr{K}$ to be an* **n-*cover complete*** *$(\mathscr{G}, \mathscr{F})$-KDP, for $n \in \mathbb{N}$, if for each $G \in \mathscr{G}$ there exist $F_1, F_2, \ldots, F_n \in \mathscr{F}$ (not necessarily distinct) such that $\mathscr{P} \setminus G = \bigcup_{1 \leq j \leq n} F_j$.*

Theorem 6.1.4. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. If $\mathscr{K}$ is an n-cover complete $(\mathscr{G}, \mathscr{F})$-KDP and $n \leq |\mathscr{B}|$, then*

$$|\mathscr{G}| \leq \sum_{j=1}^{n} \binom{|\mathscr{B}|}{j} < \frac{(|\mathscr{B}| + 1)^n}{n!} \quad \textit{and so} \quad \lfloor \sqrt[n]{n!\ |\mathscr{G}|}\ \rfloor \leq |\mathscr{B}|.$$

Proof. Suppose that $\mathscr{K}= (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is an n-cover complete $(\mathscr{G}, \mathscr{F})$-KDP. By Theorem 5.1.1, we know that for each $n \in \mathbb{N}$, there exists a finite incidence structure $\mathscr{K}_n= (\mathscr{P}_n, \mathscr{B}_n, \mathscr{I}_n)$ with $\mathscr{P}_n = \mathscr{P}$, and

$$|\mathscr{B}_n| \leq \sum_{j=1}^{m} \binom{|\mathscr{B}|}{j} \text{ where } m = \min\{n, |\mathscr{B}|\},$$

such that $\mathscr{K}_n$ is a $(\mathscr{G}, \mathscr{F}_n)$-KDP, where

$$\mathscr{F}_n = \left\{ \bigcup_{1\leq j\leq n} F_j : F_j \in \mathscr{F} \text{ for } 1 \leq j \leq n \right\}.$$

Now, since $\mathscr{K}$ is an n-cover complete $(\mathscr{G}, \mathscr{F})$-KDP, $\mathscr{P} \setminus G \in \mathscr{F}_n$ for each $G \in \mathscr{G}$. That is, $\mathscr{K}_n$ is a completely secure $(\mathscr{G}, \mathscr{F}_n)$-KDP and so by Theorem 3.2.5, $\mathscr{K}_n$ is a trivial $\mathscr{G}$-KDP.

Hence, as noted in Section 3.2.1,

$$|\mathscr{G}| \leq |\mathscr{B}_n| \leq \sum_{j=1}^{m} \binom{|\mathscr{B}|}{j} \leq \sum_{j=1}^{n} \binom{|\mathscr{B}|}{j}.$$

Finally, by induction (on n), we obtain the following inequality:

$$\sum_{j=1}^{n} \binom{|\mathscr{B}|}{j} < \frac{(|\mathscr{B}| + 1)^n}{n!}. \qquad \square$$

Remark 6.1.5. If a finite incidence structure $\mathscr{K}= (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a (t, w)-KDP, then $\mathscr{K}$ is $\left\lceil \frac{v - t}{w} \right\rceil$-cover complete, where $v = |\mathscr{P}|$.

In the following example, we will be referencing notation and results from Section 5.3.

Example 6.1.1. Let us begin by observing that for any $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}^n$ such that $\boldsymbol{a} \leq \boldsymbol{b}$, the incidence structure $\mathscr{K}_{\boldsymbol{a}}^{\boldsymbol{b}}= (\mathscr{P}_{\boldsymbol{a}}^{\boldsymbol{b}}, \mathscr{B}_{\boldsymbol{a}}^{\boldsymbol{b}}, \mathscr{I}_{\boldsymbol{a}}^{\boldsymbol{b}})$ is a $2n$-cover complete $(\mathscr{G}_{\boldsymbol{a}}^{\boldsymbol{b}}, \mathscr{F}_{\boldsymbol{a}}^{\boldsymbol{b}})$ -KDP, where $\mathscr{G}_{\boldsymbol{a}}^{\boldsymbol{b}} = \mathscr{F}_{\boldsymbol{a}}^{\boldsymbol{b}} = \{[\boldsymbol{c}, \boldsymbol{d}] : \boldsymbol{a} \leq \boldsymbol{c} \leq \boldsymbol{d} \leq \boldsymbol{b}\}$.

Next, we restrict our attention to the case when $\boldsymbol{a} = (1, 1)$ and $\boldsymbol{b} = (v, v)$ for some $v \in \mathbb{N}$, that is, $\mathscr{P}_{\boldsymbol{a}}^{\boldsymbol{b}} = \{1, 2, \ldots, v\} \times \{1, 2, \ldots, v\} \subseteq \mathbb{Z}^2$. In this case, we know from Remark 5.3.8 that, $|\mathscr{B}_{\boldsymbol{a}}^{\boldsymbol{b}}| = 4(v - 1)$ and $|\mathscr{G}_{\boldsymbol{a}}^{\boldsymbol{b}}| = |\mathscr{F}_{\boldsymbol{a}}^{\boldsymbol{b}}| = \binom{v+1}{2}^2$.

At the same time, by applying Theorem 6.1.4, (which in turn relies on Theorem 5.1.1), we can estimate a lower bound for the number of blocks (which we shall denote b) in any 4-cover complete $(\mathscr{G},\mathscr{F})$-KDP. Specifically we get $\lfloor \sqrt[4]{24|\mathscr{G}|}\, \rfloor \leq b$. Thus, in the case when $|\mathscr{G}| = \binom{v+1}{2}^2$, we get $\lfloor \sqrt[4]{6}v \, \rfloor < b$, which implies that $\sqrt[4]{6}(v-1) < b$.

The discrepancy between 4 and $\sqrt[4]{6}$, in this particular case, follows mainly from the fact that the block set $\mathscr{B}_4$ constructed in Theorem 5.1.1 only has $\binom{v+1}{2}^2$ blocks, rather than $\sum_{j=1}^{4}\binom{b}{j}$. This is due to the fact that some of the potential "new" blocks in $\mathscr{B}_4$ are either empty (in which case they are discarded) or else they reduce to already existing blocks. For example, the intersection of two "left" blocks is again a "left" block and, similarly, the intersection of two "right" blocks is again a "right" block. We also acknowledge that some of the inequalities used in this example are quite crude and so contribute to the discrepancy between 4 and $\sqrt[4]{6}$.

We showed in Example 6.1.1 that, to some extent, the $(\mathscr{G},\mathscr{F})$-KDPs generated from Theorem 5.3.7 are quite efficient in terms of the number of blocks required for their construction. Example 6.1.1 also demonstrates that the lower bound on the number of blocks given by Theorem 6.1.4 can be reasonably tight. On the other hand, with some more careful analysis of Theorem 6.1.4 and, in particular, Theorem 5.1.1, it should be possible to improve this lower bound for $|\mathscr{B}|$.

Although, in general, it is difficult to estimate the number of blocks in a $(\mathscr{G},\mathscr{F})$-KDP, there is a special case when this is possible. Specifically, we saw in Section 3.2.1 that for a trivial $\mathscr{G}$-KDP, $\mathscr{K} = (\mathscr{P},\mathscr{B},\mathscr{I})$, it is possible to estimate the number of blocks in $\mathscr{K}$. That is, we obtained $b = |\mathscr{B}| \geq |\mathscr{G}|$. In fact, if we remove any redundancy from $\mathscr{K}$ then we obtain $b = |\mathscr{B}| = |\mathscr{G}|$. Thus, if we are given any families $\mathscr{G}$ and $\mathscr{F}$ of non-empty subsets of a given set $\mathscr{P}$, then we can always construct an incidence structure $\mathscr{K} = (\mathscr{P},\mathscr{B},\mathscr{I})$ that is a $(\mathscr{G},\mathscr{F})$-KDP and has at most $|\mathscr{G}|$ blocks. This provides a natural upper bound on the number of blocks required for any "good" $(\mathscr{G}, \mathscr{F})$-KDP. It also suggests an approach to estimating the number of blocks in a $(\mathscr{G}, \mathscr{F})$-KDP. That is, to determine how close a given $(\mathscr{G}, \mathscr{F})$-KDP is to being trivial. This is just what we do next. More precisely, we show that for w sufficiently large relative to $|\mathscr{G}|$, every $(\mathscr{G}, w)$-KDP is "almost trivial". This is not entirely surprising, since we showed in Proposition 3.3.5 that for a $(\mathscr{G}, w)$-KDP, $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$, if $w \geq |\mathscr{B}|$ then $\mathscr{K}$ is a trivial $\mathscr{G}$-KDP and thus has at least $|\mathscr{G}|$ blocks.

Lemma 6.1.6. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP and $b < \binom{w+2}{2}$, then*

$$\big|\{G \in \mathscr{G} : G = (x) \text{ for some } x \in \mathscr{B}\}\big| \geq |\mathscr{G}| - w.$$

Proof. Let $\mathscr{G}' = \{G \in \mathscr{G} : G \neq (x) \text{ for any } x \in \mathscr{B}\}$ and for every $G \in \mathscr{G}'$ set $\bar{G} = \bigcap_{P \in G}(P)$. Our goal is to show that $|\mathscr{G}'| \leq w$, but first we need to show that for any distinct elements $G'_0, G'_1, \ldots, G'_i \in \mathscr{G}'$, where $|G'_j| \geq |G'_i|$ for all $0 \leq j \leq i \leq w$, $|\bar{G}'_i \setminus \bigcup_{0 \leq j < i} \bar{G}'_j| \geq w - i + 1$.

So suppose, in order to obtain a contradiction, that $|\bar{G}'_i \setminus \bigcup_{0 \leq j < i} \bar{G}'_j| \leq w - i$. Then we can write $\bar{G}'_i \setminus [\bar{G}'_0 \cup \bar{G}'_1 \cup \cdots \cup \bar{G}'_{i-1}] = \{x_1, x_2, \ldots, x_k\}$ for $1 \leq k \leq w - i$. Since $G'_i \in \mathscr{G}'$, for each $1 \leq j \leq k$ there exists a point $P_j \in (x_j) \setminus G'_i$. On the other hand, for each $0 \leq j < i$ there exists a point $Q_j \in G'_j \setminus G'_i$, since $|G'_j| \geq |G'_i|$ and $G'_j \neq G'_i$.

Therefore,

$$\begin{aligned} \bar{G}'_i &\subseteq [\bar{G}'_0 \cup \bar{G}'_1 \cup \cdots \cup \bar{G}'_{i-1}] \cup \bar{G}'_i \setminus [\bar{G}'_0 \cup \bar{G}'_1 \cup \cdots \cup \bar{G}'_{i-1}] \\ &= [\bar{G}'_0 \cup \bar{G}'_1 \cup \cdots \cup \bar{G}'_{i-1}] \cup \{x_1, x_2, \ldots, x_k\} \\ &\subseteq (Q_0) \cup (Q_1) \cup \cdots \cup (Q_{i-1}) \cup (P_1) \cup (P_2) \cup \cdots \cup (P_k), \end{aligned}$$

which is not possible since $\{Q_0, Q_1, \ldots, Q_{i-1}, P_1, P_2, \ldots, P_k\} \cap G'_i = \varnothing$ and $i + k \leq w$. Hence, $\left|\bar{G}'_i \setminus \bigcup\limits_{0 \leq j < i} \bar{G}'_j\right| \geq w - i + 1$.

Next we assume, in order to obtain a contradiction, that $|\mathscr{G}'| > w$. Then, there exist $w+1$ distinct elements $G_0, G_1, \dots, G_w \in \mathscr{G}'$ and, after possibly reordering them, we may assume that $|G_i| \geq |G_{i+1}|$ for $0 \leq i < w$. Then,

$$\Big|\bigcup_{0\leq i\leq w} \bar{G}_i\Big| = |\bar{G}_0| + |\bar{G}_1 \setminus \bar{G}_0| + |\bar{G}_2 \setminus (\bar{G}_1 \cup \bar{G}_0)| + \cdots + |\bar{G}_w \setminus (\bar{G}_{w-1} \cup \bar{G}_{w-2} \cup \cdots \cup \bar{G}_0)|$$

$$\geq (w+1) + w + (w-1) + \cdots + 2 + 1 = \frac{(w+1)(w+2)}{2} = \binom{w+2}{2}.$$

Hence, $b \geq \Big|\bigcup_{0\leq i\leq w} \bar{G}_i\Big| \geq \binom{w+2}{2}$. However, $b < \binom{w+2}{2}$ so we have a obtained a contradiction and thus $|\mathscr{G}'| \leq w$.

Therefore, $\big|\{G \in \mathscr{G} : G = (x) \text{ for some } x \in \mathscr{B}\}\big| = |\mathscr{G}| - |\mathscr{G}'| \geq |\mathscr{G}| - w$. □

We now use Lemma 6.1.6 to obtain a lower bound on the total number of blocks in a $(\mathscr{G}, w)$-KDP. The inspiration for Theorem 6.1.7 comes from [73, Theorem 3.6], where Quinn gave a lower bound of the same style for (t, w)-KDPs.

Theorem 6.1.7. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP, then*

$$b \geq \min\left\{|\mathscr{G}| - w, \binom{w+2}{2}\right\}.$$

Proof. Let a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a $(\mathscr{G}, w)$-KDP, for $w \geq 1$. In order to obtain a contradiction, suppose $b < \min\left\{|\mathscr{G}| - w, \binom{w+2}{2}\right\}$. In particular, $b < \binom{w+2}{2}$, so by Lemma 6.1.6,

$$\big|\{G \in \mathscr{G} : G = (x) \text{ for some } x \in \mathscr{B}\}\big| \geq |\mathscr{G}| - w.$$

Which gives a contradiction since

$$b \geq |\{x \in \mathscr{B} : G = (x) \text{ for some } G \in \mathscr{G}\}|$$
$$\geq |\{G \in \mathscr{G} : G = (x) \text{ for some } x \in \mathscr{B}\}| \geq |\mathscr{G}| - w.$$ □

Theorem 6.1.7 shows that if $\binom{w+2}{2} \geq |\mathscr{G}| - w$ then the number of blocks required for a $(\mathscr{G}, w)$-KDP is only w fewer than the number of blocks required for a trivial $\mathscr{G}$-KDP. So in this case we have a good estimate on the number of blocks required for a $(\mathscr{G}, w)$-KDP. However, in the case when $|\mathscr{G}| >> w^2$, Theorem 6.1.7 does not provide a good lower bound (on the total number of blocks required). We address this deficiency in our next theorem, which is completely new.

Theorem 6.1.8. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP, then $b \geq \log_2 \binom{|\mathscr{G}|}{\lceil w/2 \rceil}$.*

Proof. If $\lceil w/2 \rceil = 1$ then the result follows from Corollary 6.1.2. So we shall only consider the case when $k = \lceil w/2 \rceil \geq 2$.

Let $D = \{X \in 2^{\mathscr{G}} : |X| = k\}$, let $\bar{G} = \bigcap_{P \in G}(P)$ for every $G \in \mathscr{G}$ and let $\varphi : D \to 2^{\mathscr{B}}$ be defined by, $\varphi(\{G_1, G_2, \dots, G_k\}) = \bar{G}_1 \Delta \bar{G}_2 \Delta \cdots \Delta \bar{G}_k$ (where Δ denotes the symmetric difference). Note that φ is well-defined, since if $\{G_1, G_2, \dots, G_k\} = \{G'_1, G'_2, \dots, G'_k\} \in D$ then $\varphi(\{G_1, G_2, \dots, G_k\}) = \varphi(\{G'_1, G'_2, \dots, G'_k\})$ (essentially, this follows from the fact that $(2^{\mathscr{B}}, \Delta)$ is an Abelian group).

We claim that φ is 1-to-1 on D. To this end, let us suppose, in order to obtain a contradiction, that $\varphi(\{G_1, G_2, \dots, G_k\}) = \varphi(\{G'_1, G'_2, \dots, G'_k\})$ for some $\{G_1, G_2, \dots, G_k\} \in D$ and $\{G'_1, G'_2, \dots, G'_k\} \in D$ such that $\{G_1, G_2, \dots, G_k\} \neq \{G'_1, G'_2, \dots, G'_k\}$. Then, after cancelling out any common sets and possibly relabelling, we obtain that $\{G_1, G_2, \dots, G_j\} \cap \{G'_1, G'_2, \dots, G'_j\} = \varnothing$ and $\bar{G}_1 \Delta \bar{G}_2 \Delta \cdots \Delta \bar{G}_j = \bar{G}'_1 \Delta \bar{G}'_2 \Delta \cdots \Delta \bar{G}'_j$ for some $1 \leq j \leq k$. Note that if $j = 1$ then we are done, since if $\bar{G}_1 = \bar{G}'_1$ then $G_1 = G'_1$, by Remark 3.3.13, and so $\{G_1, G_2, \dots, G_k\} = \{G'_1, G'_2, \dots, G'_k\}$ in these cases.

So, we shall suppose that $2 \leq j$. Again, by relabelling and possibly interchanging the $G's$ with the $G''s$, we may assume that

$$|G_1| = \min\left\{|G''| : G'' \in \{G_1, G_2, \dots, G_j, G'_1, G'_2, \dots, G'_j\}\right\}.$$

Then, for every $2 \leq i \leq j$ there exist points $P_i \in G_i \setminus G_1$ and $P'_i \in G'_i \setminus G_1$.

Of course, there also exists a point $P_1' \in G_1' \setminus G_1$. Now,

$$\begin{aligned}
\bar{G}_1 &\subseteq [\bar{G}_1 \Delta (\bar{G}_2 \Delta \cdots \Delta \bar{G}_j)] \cup [\bar{G}_2 \cup \bar{G}_3 \cup \cdots \cup \bar{G}_j] \\
&= [\bar{G}_1' \Delta \bar{G}_2' \Delta \cdots \Delta \bar{G}_j'] \cup [\bar{G}_2 \cup \bar{G}_3 \cup \cdots \cup \bar{G}_j] \\
&\subseteq \bigcup_{1 \le i \le j} \bar{G}_i' \cup \bigcup_{2 \le i \le j} \bar{G}_i \\
&\subseteq (P_1') \cup (P_2') \cup \cdots \cup (P_j') \cup (P_2) \cup (P_3) \cup \cdots \cup (P_j).
\end{aligned}$$

This contradicts the fact that $\mathscr{K}$ is a $(\mathscr{G}, w)$-KDP, and therefore φ is indeed 1-to-1.

Hence, $\binom{|\mathscr{G}|}{\lceil w/2 \rceil} = |D| = |\varphi(D)| \le |2^{\mathscr{B}}| = 2^b$ and so $\log_2 \binom{|\mathscr{G}|}{\lceil w/2 \rceil} \le b$. □

Theorem 6.1.8 is the best that we can do without imposing any constraints on the set of privileged subsets.

6.2 Bounds for Sperner Systems

In this section we shall restrict our attention to the case when the families of privileged subsets form a Sperner system. We shall see that under this additional assumption, we are able to obtain better lower bounds on b than in the previous section. Note that the special case of $\mathscr{G} = \{G \in \mathscr{P} : |G| \le t\}$ fails to form a Sperner system. However, if we were to set $\mathscr{G}' = \{G \in \mathscr{P} : |G| = t\}$ then $\mathscr{G}' \subseteq \mathscr{G}$ and $\mathscr{G}'$ forms a Sperner system on $\mathscr{P}$. Moreover, if $t + w \le |\mathscr{P}|$, then we showed in Corollary 3.3.9 that if an incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}', w)$-KDP then $\mathscr{K}$ is a (t, w)-KDP. Hence, the case of (t, w)-KDPs is indeed covered within this subsection.

For the purpose of clarity, we split this section into three subsections. In the first subsection we generalise existing bounds. In the second we use a version of Stirling's approximation (Corollary 2.2.9) to further tighten these generalised bounds. Finally, in our third subsection, we consider a theorem of Füredi [34]. We use some techniques of Füredi in our own theorem and explore some similar results by other authors.

6.2.1 Generalised Bounds

The bounds that we present in this subsection are simple and explicit. Before we can introduce them, however, we require two short lemmas.

Much work has been done on inequalities associated with CFFs (see, for example [28, 78, 85] and [86]). As can be seen from the following lemma, our studies (when the set of privileged subsets forms a Sperner system) converge with those of CFFs.

Lemma 6.2.1. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP and $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$, then the set of common blocks, $\mathcal{S} = \left\{\bigcap_{P \in G}(P) : G \in \mathscr{G}\right\}$, has the property that if $S_0, S_1, \ldots, S_w \in \mathcal{S}$ and $S_0 \notin \{S_1, S_1, \ldots, S_w\}$ then $S_0 \not\subseteq \bigcup_{k=1}^{w} S_k$. (That is, $\mathcal{S}$ is a $(1, w)$-CFF.)*

Proof. Suppose, in order to obtain a contradiction that there exists $G_0 \in \mathscr{G}$ and $G_1, G_2, \ldots, G_w \in \mathscr{G} \setminus \{G_0\}$ such that

$$\bigcap_{P \in G_0}(P) \subseteq \bigcap_{P \in G_1}(P) \cup \bigcap_{P \in G_2}(P) \cup \cdots \cup \bigcap_{P \in G_w}(P).$$

Since $\mathscr{G}$ forms a Sperner system we know that for each $1 \leq k \leq w$ there exists a point $P_k \in G_k \setminus G_0$. Then,

$$\bigcap_{P \in G_0}(P) \subseteq \bigcap_{P \in G_1}(P) \cup \bigcap_{P \in G_2}(P) \cup \cdots \cup \bigcap_{P \in G_w}(P) \subseteq (P_1) \cup (P_2) \cup \cdots \cup (P_w),$$

which contradicts the fact that $\mathscr{K}$ is a $(\mathscr{G}, w)$-KDP. □

The following lemma enables us to employ Sperner's theorem to estimate the number of blocks required in a $(\mathscr{G}, w)$-KDP in the case when the family of privileged subsets $\mathscr{G}$ forms a Sperner system. Lemma 6.2.2 is implicit in [26, Theorem 6].

Lemma 6.2.2. *Let X be a set and $\mathcal{S} \subseteq 2^X$. If $\mathcal{S}$ is a $(1, w)$-CFF, then*

$$\mathcal{S}' = \left\{ \bigcup_{1 \leq k \leq w} S_k : S_1, S_2, \ldots, S_w \in \mathcal{S} \text{ and } S_i \neq S_j \text{ for } i \neq j \right\}$$

forms a Sperner system on X.

Proof. If $|\mathcal{S}| < w$ then there is nothing to prove since $\mathcal{S}' = \varnothing$ in this case. So let us assume that $|\mathcal{S}| \geq w$. Let us also assume, in order to obtain a contradiction, that $\mathcal{S}'$ is not a Sperner system on X. Then there exist distinct sets $S_1, S_2, \dots, S_w \in \mathcal{S}$ and $S_1', S_2', \dots, S_w' \in \mathcal{S}$ such that

$$\{S_1, S_2, \dots, S_w\} \neq \{S_1', S_2', \dots, S_w'\} \quad \text{and} \quad \bigcup_{1 \leq k \leq w} S_k \subseteq \bigcup_{1 \leq k \leq w} S_k'.$$

Now, there must exist some $1 \leq j \leq w$ such that $S_j \notin \{S_1', S_2', \dots, S_w'\}$ for otherwise $\{S_1, S_2, \dots, S_w\} \subseteq \{S_1', S_2', \dots, S_w'\}$ and in this case we would have $\{S_1, S_2, \dots, S_w\} = \{S_1', S_2', \dots, S_w'\}$, as both sets have cardinality w.

Then, $S_j \subseteq \bigcup_{1 \leq k \leq w} S_j'$, which contradicts the fact that $\mathcal{S}$ is a $(1, w)$-CFF. Therefore, $\mathcal{S}'$ must indeed be a Sperner system on X. □

The following theorem uses Result 2.2.7 to generalise [26, Theorem 6] and [73, Theorem 3.4] from (t, w)-KDPs to $(\mathscr{G}, w)$-KDPs where the set of privileged subsets forms a Sperner system.

Theorem 6.2.3. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP and $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$, then*

$$b \geq \log_2 \binom{|\mathscr{G}|}{w} + 1.$$

Proof. From Lemma 6.2.2 and Lemma 6.2.2 we know that

$$\mathcal{S} = \left\{ \bigcup_{1 \leq k \leq w} \bigcap_{P \in G_k} (P) : G_1, G_2, \dots, G_w \in \mathscr{G} \text{ and } G_i \neq G_j \text{ for } i \neq j \right\}$$

forms a Sperner system. Therefore, from Result 2.2.7 and Result 2.2.5 (Sperner's Theorem), we have

$$|\mathcal{S}| \leq \binom{b}{\lfloor b/2 \rfloor} \leq 2^{b-1}.$$

$$\text{So,} \quad \binom{|\mathscr{G}|}{w} \leq 2^{b-1} \quad \text{and hence,} \quad b \geq \log_2 \binom{|\mathscr{G}|}{w} + 1.$$ □

The following corollary demonstrates an immediate consequence of this theorem.

Corollary 6.2.4. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ on v points is a (t, w)-KDP and $t + w \leq v$, then*

$$b \geq \max \left\{ \log_2 \binom{\binom{v}{t}}{w}, \log_2 \binom{\binom{v}{w}}{t} \right\} + 1.$$

Proof. It follows from Theorem 6.2.3 that $b \geq \log_2 \binom{\binom{v}{t}}{w} + 1$. However, we also know from Theorem 5.1.31 that the complement of $\mathscr{K}$ is a (w, t)-KDP on b blocks. Therefore, from Theorem 5.1.31, $b \geq \log_2 \binom{\binom{v}{w}}{t} + 1$ and the result follows. □

In order to fully exploit Corollary 6.2.4 it is necessary to understand the precise relationship between $\binom{\binom{v}{t}}{w}$ and $\binom{\binom{v}{w}}{t}$.

Theorem 6.2.5. *If $1 \leq w \leq t < v$ are natural numbers, then*

$$\binom{\binom{v}{t}}{w} \leq \binom{\binom{v}{w}}{t}.$$

Despite its simplicity, the proof of Theorem 6.2.5 (also given in [61]) is long and cumbersome. However, the result is new and potentially of independent interest. Therefore, in order to avoid derailing the flow of the thesis, we have omitted the proof of Theorem 6.2.5 in favour of including it in Appendix A.

We can now deduce the following corollary, motivated by [86, Lemma 2.4].

Corollary 6.2.6. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ on v points is a (t, t)-KDP and $2t \leq v$, then*

$$b \geq 2 \log_2 \binom{\binom{v-1}{t-1}}{t} + 2.$$

Proof. Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure on v points and for some arbitrary point $P \in \mathscr{P}$, let $\mathscr{K}_P = (\mathscr{P}_P, \mathscr{B}_P, \mathscr{I}_P)$ be the internal structure of $\mathscr{K}$ at P and let $\mathscr{K}^P = (\mathscr{P}^P, \mathscr{B}^P, \mathscr{I}^P)$ be the external structure of $\mathscr{K}$ at P.

Now, $b = b_P + b^P$ and if $\mathscr{K}$ is a (t, w)-KDP on v points, then $\mathscr{K}_P$ is a $(t-1, w)$-KDP (Corollary 5.1.11) and $\mathscr{K}^P$ is a $(t, w-1)$-KDP (Corollary 5.1.23), both on $v-1$ points. Since $\mathscr{K}$ is a (t,t)-KDP, it follows from Corollary 6.2.4 and Theorem 6.2.5 that,

$$\begin{aligned} b = b_P + b^P &\geq \log_2 \binom{\binom{v-1}{t-1}}{t} + 1 + \log_2 \binom{\binom{v-1}{t-1}}{t} + 1 \\ &= 2\log_2 \binom{\binom{v-1}{t-1}}{t} + 2 \end{aligned}$$

and the proof is complete. □

6.2.2 Tightening the Bounds

Using Corollary 2.2.9 we can improve further upon our previous bounds on the total number of blocks required for a $(\mathscr{G}, w)$-KDP. For example, from Theorem 6.2.3 we know that if a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP and $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$, then

$$b \geq \log_2 \binom{|\mathscr{G}|}{w} + 1 = \log_2 \left[2 \binom{|\mathscr{G}|}{w} \right].$$

Now, using Corollary 2.2.9 we can improve upon this bound:

$$\log_2 \binom{|\mathscr{G}|}{w} \leq \log_2 \binom{b}{\lfloor b/2 \rfloor} < b - \frac{1}{2} \log_2 \left(\frac{\pi}{2} b \right).$$

Therefore,

$$\begin{aligned} b &> \log_2 \binom{|\mathscr{G}|}{w} + \frac{1}{2} \log_2 \left(\frac{\pi}{2} b \right) \\ &> \log_2 \binom{|\mathscr{G}|}{w} + \frac{1}{2} \log_2 \left[\frac{\pi}{2} \left(\log_2 \left[2 \binom{|\mathscr{G}|}{w} \right] \right) \right]. \end{aligned}$$

This new bound comes directly from substituting in the bound from Theorem 6.2.3 and it can be easily verified that if $\binom{|\mathscr{G}|}{w} \geq 4$ then we have a better bound than that from Theorem 6.2.3.

In fact, we can continue substituting in bounds for b to get better bounds at each substitution. Unfortunately, this gets messy quite quickly and the improvements to the bound diminish rapidly.

However, if we really wanted to "squeeze the pips" out of this approach, we could inductively define a sequence by

$$a_1 = \log_2 \left[2\binom{|\mathscr{G}|}{w} \right] \qquad \text{and} \qquad a_{n+1} = \log_2 \binom{|\mathscr{G}|}{w} + \frac{1}{2}\log_2\left(\frac{\pi}{2}a_n\right).$$

$$\text{Then, } \; a_2 = \log_2 \binom{|\mathscr{G}|}{w} + \frac{1}{2}\log_2\left[\frac{\pi}{2}\left(\log_2\left[2\binom{|\mathscr{G}|}{w}\right]\right)\right] \quad \text{and}$$

$$\begin{aligned} a_{n+1} - a_n &= \frac{1}{2}\left[\log_2\left(\frac{\pi}{2}a_n\right) - \log_2\left(\frac{\pi}{2}a_{n-1}\right)\right] \\ &= \frac{1}{2}\left[\log_2 \frac{a_n}{a_{n-1}}\right] \geq 0, \quad \text{if } \frac{a_n}{a_{n-1}} \geq 1. \end{aligned}$$

Clearly $a_2 \geq a_1$ if $\binom{|\mathscr{G}|}{w} \geq 4$ and, inductively, if $a_n \geq a_{n-1}$ then $a_{n+1} \geq a_n$, so the sequence is increasing for all n, and is bounded above by b, so convergent. However, for the reasons stated earlier, we have chosen not to pursue these bounds any further.

6.2.3 Bounds using Techniques of Füredi

In this subsection, we modify a proof technique of Füredi in order to improve upon some of our bounds from Subsection 6.2.1 and Subsection 6.2.2 (for $(\mathscr{G}, w)$-KDPs with $|\mathscr{G}|$ large).

As demonstrated by Lemma 6.2.1, CFFs are intimately connected to the study of $(\mathscr{G}, w)$-KDPs. Of particular interest to us is the calculation of the smallest possible cardinality of any set X that admits a w-CFF. There have been many results on this topic. However, we will focus our attention on a result of Füredi, [34], which although not the best bound in the literature, it is the simplest and easiest to apply in the setting of $(\mathscr{G}, w)$-KDPs. So, next we will present the result from [34] in the setting of $(\mathscr{G}, w)$-KDPs and give the full details of the proof. We also give an explicit formula for the error term, which is not given in [34].

Theorem 6.2.7. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP, where $2 \leq w \leq b$ and $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$, then*

$$\frac{\log_2 |\mathscr{G}|}{b} < \frac{4\log_2(w) + H(w,b)}{w^2}$$

$$\textit{where} \quad H(w,b) = \frac{w^2}{b}\left[3\log_2(w) + \log_2\left(\frac{e}{2}\right)\right] + 2\log_2\left(\frac{e}{2}\right).$$

Proof. Firstly let

$$t = \left\lceil (b-w)/\binom{w+1}{2} \right\rceil \quad \text{and note that} \quad b/2 \geq t > 0.$$

Let $\mathcal{S} = \left\{\bigcap_{P \in G}(P) : G \in \mathscr{G}\right\}$, then $|\mathscr{G}| = |\mathcal{S}|$ since the mapping $G \to \bigcap_{P \in G}(P)$ is 1-to-1 (Remark 3.3.13) and no set $S \in \mathcal{S}$ is contained in the union of w other members of $\mathcal{S}$ (Lemma 6.2.1).

Next define $\mathcal{S}_t \subseteq \mathcal{S}$ as the family of members of $\mathcal{S}$ having their own t-subset. That is, $\mathcal{S}_t = \{S \in \mathcal{S}$: there exists a t-element set $T \subseteq S$ such that $T \nsubseteq S'$ for any other $S' \in \mathcal{S}\}$.

Let $\mathcal{T}$ be the family of these t-subsets, let $\mathcal{S}_0 = \{S \in \mathcal{S} : |S| < t\}$ and let $\mathcal{R}$ be the family of t-sets containing a member of $\mathcal{S}_0$, that is,

$$\mathcal{R} = \{R \in 2^{\mathcal{B}} : |R| = t \text{ and } S \subseteq R \text{ for some } S \in \mathcal{S}_0\}.$$

Since no set $S \in \mathcal{S}$ is contained in any other member of $\mathcal{S}$ (i.e. $\mathcal{S}$ forms a Sperner system), $\mathcal{T}$ and $\mathcal{R}$ are disjoint. Moreover, from Result 2.2.6 we have $|\mathcal{S}_0| \leq |\mathcal{R}|$. From this it follows that

$$|\mathcal{S}_0 \cup \mathcal{S}_t| = |\mathcal{S}_0| + |\mathcal{S}_t| \leq |\mathcal{R}| + |\mathcal{T}| = |\mathcal{R} \cup \mathcal{T}| \leq \binom{b}{t}.$$

Let $\mathcal{S}' = \mathcal{S} \setminus (\mathcal{S}_0 \cup \mathcal{S}_t)$. We will eventually show that $|\mathcal{S}'| \leq w$, but first we will show that for any distinct elements $S'_0, S'_1, \ldots, S'_i \in \mathcal{S}'$ where $i \leq w$,

$$|S'_i \setminus \bigcup_{0 \leq j < i} S'_j| \geq t(w-i) + 1.$$

In order to obtain a contradiction, we shall suppose that $|S'_i \setminus \bigcup_{0 \leq j < i} S'_j| \leq t(w-i)$. Now, since $S'_i \notin \mathcal{S}_0$, we know that $|S'_i| \geq t$. Therefore, there exist some

t-element subsets $\{T_{i+1}, T_{1+2}, \ldots, T_w\}$ of S'_i such that $S'_i \setminus [S'_0 \cup S'_1 \cup \cdots \cup S'_{i-1}] \subseteq \bigcup_{i<j\leq w} T_j \subseteq S'_i$. Since $S'_i \notin \mathcal{S}_t$ for each $i < j \leq w$, there exists an $S_j \in \mathcal{S}$ such that $T_j \subseteq S_j$. Therefore, $S'_i \setminus [S'_0 \cup S'_1 \cup \cdots \cup S'_{i-1}] \subseteq \bigcup_{i<j\leq w} T_j \subseteq \bigcup_{i<j\leq w} S_j$ and so $S'_i \subseteq \bigcup\{S_j : 0 \leq j \leq w$ and $j \neq i\}$, which is a contradiction since no set $S \in \mathcal{S}$ is contained in the union of w other members of $\mathcal{S}$.

Next we assume, in order to obtain another contradiction, that $|\mathcal{S}'| > w$. Then, there exist $w + 1$ distinct elements $S_0, S_1, \ldots, S_w \in \mathcal{S}'$ and we have

$$\begin{aligned}\Big|\bigcup_{0\leq i\leq w} S_i\Big| &= |S_0| + |S_1 \setminus S_0| + |S_2 \setminus (S_1 \cup S_0)| + \cdots + |S_w \setminus (S_{w-1} \cup S_{w-2} \cup \cdots \cup S_0)| \\ &\geq (tw+1) + (t(w-1)+1) + (t(w-2)+1) + \cdots + (2t+1) + (t+1) \\ &= tw + t(w-1) + t(w-2) + \cdots + 2t + t + (w+1) \\ &= (w+1) + \frac{tw(w+1)}{2} = (w+1) + t\binom{w+1}{2} \\ &= (w+1) + \left\lceil (b-w)/\binom{w+1}{2} \right\rceil \binom{w+1}{2} \geq b + 1.\end{aligned}$$

So, $b \geq \Big|\bigcup_{0\leq i\leq w} S_i\Big| \geq b + 1$ and we have a contradiction, therefore $|\mathcal{S}'| \leq w$.

Now, $|\mathscr{G}| = |\mathcal{S}| = |\mathcal{S}_0 \cup \mathcal{S}_t| + |\mathcal{S}'| \leq \binom{b}{t} + w$ for $t = \lceil (b-w)/\binom{w+1}{2} \rceil$.

$$\text{So, } |\mathscr{G}| \leq w + \binom{b}{\lceil (b-w)/\binom{w+1}{2} \rceil}.$$

Also, since

1. $\log_2(w + x) \leq \log_2(w) + \log_2(x) = \log_2(wx)$, if $2 \leq w \leq x$, and
2. $(b-w)/\binom{w+1}{2} = \dfrac{2(b-w)}{w(w+1)} \leq \dfrac{2b}{w^2} \leq \dfrac{b}{2}$,

it follows that

$$\log_2 |\mathscr{G}| \leq \log_2 w + \log_2 \binom{b}{\lceil (b-w)/\binom{w+1}{2} \rceil} \leq \log_2 w + \log_2 \binom{b}{\lceil 2b/w^2 \rceil}.$$

Now, from Stirling's approximation [87, page 253], $\binom{n}{r} \leq \dfrac{n^r}{r!} < \left(\dfrac{en}{r}\right)^r$.

Therefore,

$$\begin{aligned}
\log_2 |\mathscr{G}| &< \log_2 w + \log_2 \left[\left(\frac{eb}{\lceil 2b/w^2 \rceil} \right)^{\lceil 2b/w^2 \rceil} \right] \\
&\leq \log_2 w + \log_2 \left[\left(\frac{eb}{2b/w^2} \right)^{\lceil 2b/w^2 \rceil} \right] \\
&\leq \log_2 w + \log_2 \left[\frac{e}{2} w^2 \right]^{\left(\frac{2b}{w^2} + 1 \right)} \\
&= \log_2 w + \left(\frac{2b}{w^2} + 1 \right) \left[2 \log_2 w + \log_2 \left(\frac{e}{2} \right) \right] \\
&= \log_2 w + \left(\frac{4b}{w^2} + 2 \right) \left[\log_2 w + \frac{1}{2} \log_2 \left(\frac{e}{2} \right) \right] \\
&= \frac{4b}{w^2} \log_2 w + 3 \log_2 w + \left(\frac{2b}{w^2} + 1 \right) \log_2 \left(\frac{e}{2} \right) \\
&= \frac{b}{w^2} \left[4 \log_2 w + \frac{3w^2}{b} \log_2 w + \left(2 + \frac{w^2}{b} \right) \log_2 \left(\frac{e}{2} \right) \right].
\end{aligned}$$

Hence,

$$\frac{\log_2 |\mathscr{G}|}{b} < \frac{4 \log_2(w) + H(w,b)}{w^2}$$

where $H(w,b) = \dfrac{w^2}{b} \left[3 \log_2(w) + \log_2 \left(\dfrac{e}{2} \right) \right] + 2 \log_2 \left(\dfrac{e}{2} \right)$. □

We now show that for large b, the quantity $H(w,b)$ from Theorem 6.2.7 is small.

Remark 6.2.8. For fixed $w \geq 2$,

$$\lim_{b \to \infty} H(w,b) = \lim_{b \to \infty} \frac{w^2}{b} \left[3 \log_2(w) + \log_2 \left(\frac{e}{2} \right) \right] + 2 \log_2 \left(\frac{e}{2} \right) = 2 \log_2 \left(\frac{e}{2} \right) < 1.$$

We may recall from Section 6.1 that for a $(\mathscr{G}, w)$-KDP, $\mathscr{K}$, if $|\mathscr{G}| \approx w^2/2$, then $\mathscr{K}$ is "almost" trivial. We next use the proof techniques of Füredi in order to improve upon Theorem 6.1.7, under the additional assumption that the set of privileged subsets forms a Sperner system. Note that, as with Theorem 6.1.7, Theorem 6.2.9 is written in the style of [73, Result 3.6].

Theorem 6.2.9. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP and $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$, then*

$$b \geq \min\left\{|\mathscr{G}|, \binom{w+2}{2}\right\}.$$

Proof. In order to obtain a contradiction, suppose $b < \min\left\{|\mathscr{G}|, \binom{w+2}{2}\right\}$. For every $G \in \mathscr{G}$ let $\bar{G} = \bigcap_{P \in G}(P)$ and let

$$\mathscr{G}_1 = \left\{G \in \mathscr{G} : \bar{G} \setminus \bigcup\{\bar{G}' : G' \in \mathscr{G} \text{ and } G' \neq G\} \neq \varnothing\right\}.$$

Then, for each $G \in \mathscr{G}_1$ choose $x_G \in \bar{G} \setminus \bigcup\{\bar{G}' : G' \in \mathscr{G} \text{ and } G' \neq G\}$. The mapping $G \to x_G$, from $\mathscr{G}_1$ into $\mathscr{B}$ is 1-to-1, so $|\mathscr{G}_1| = |\{x_G : G \in \mathscr{G}_1\}| \leq b$. Since $b < |\mathscr{G}|$, we know that $|\mathscr{G}_1| < |\mathscr{G}|$. Hence, $\mathscr{G}' = \mathscr{G} \setminus \mathscr{G}_1 \neq \varnothing$. For each $G' \in \mathscr{G}'$, $\bar{G}' \cap \{x_G : G \in \mathscr{G}_1\} = \varnothing$ and, as we shall show next, $|\bar{G}'| \geq w + 1$.

To see that $|\bar{G}'| \geq w+1$, we proceed indirectly, that is, we suppose that $|\bar{G}'| \leq w$. Therefore, $\bar{G}' = \{x_1, x_2, \ldots, x_k\}$ for $k \leq w$. Since $G' \in \mathscr{G}'$, for each $1 \leq j \leq k$ there exists a $G_j \neq G'$ such that $x_j \in \bar{G}_j$. However, as $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$, there exists a point $P_j \in G_j \setminus G'$ for each $1 \leq j \leq k$. Therefore,

$$\bar{G}' = \{x_1, x_2, \ldots, x_k\} \subseteq \bar{G}_1 \cup \bar{G}_2 \cup \cdots \cup \bar{G}_k \subseteq (P_1) \cup (P_2) \cup \cdots \cup (P_k)$$

and we have a contradiction since $k \leq w$. Now,

$$\begin{aligned} b &\geq |\bar{G}' \cup \{x_G : G \in \mathscr{G}_1\}| = |\bar{G}'| + |\{x_G : G \in \mathscr{G}_1\}| \\ &= |\bar{G}'| + |\mathscr{G}_1| \geq (w+1) + |\mathscr{G}_1|. \end{aligned}$$

That is, $|\mathscr{G}_1| \leq b - (w+1)$ and hence

$$|\mathscr{G}'| = |\mathscr{G} \setminus \mathscr{G}_1| = |\mathscr{G}| - |\mathscr{G}_1| > b - |\mathscr{G}_1| \geq b - [b - (w+1)] = w + 1.$$

We will now show that for any distinct elements $G'_0, G'_1, \ldots, G'_i \in \mathscr{G}'$, with $i \leq w$, $|\bar{G}'_i \setminus \bigcup_{0 \leq j \leq i-1} \bar{G}'_j| \geq w - i + 1$. Suppose, in order to obtain a contradiction, that $|\bar{G}'_i \setminus \bigcup_{0 \leq j \leq i-1} \bar{G}'_j| \leq w - i$. Then, we can write

$\bar{G}'_i \setminus [\bar{G}'_0 \cup \bar{G}'_1 \cup \cdots \cup \bar{G}'_{i-1}] = \{x_1, x_2, \ldots, x_k\}$ for $1 \leq k \leq w - i$. Since $G'_1 \in \mathscr{G}'$, for $1 \leq j \leq k$ there exists a $G'_j \in \mathscr{G}$ such that $x_j \in \bar{G}'_j$. For each $1 \leq j \leq k$ choose $P_{i+j} \in G'_{i+j} \setminus G'_i$. Now, for each $0 \leq j < i$ there exists a point $P_j \in G'_j \setminus G'_i$, since $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$. Therefore,

$$\begin{aligned}
\bar{G}'_i &\subseteq [\bar{G}'_0 \cup \bar{G}'_1 \cup \cdots \cup \bar{G}'_{i-1}] \cup \bar{G}'_i \setminus [\bar{G}'_0 \cup \bar{G}'_1 \cup \cdots \cup \bar{G}'_{i-1}] \\
&= [\bar{G}'_0 \cup \bar{G}'_1 \cup \cdots \cup \bar{G}'_{i-1}] \cup \{x_1, x_2, \ldots, x_k\} \\
&\subseteq (P_0) \cup (P_1) \cup \cdots \cup (P_{i-1}) \cup (P_{i+1}) \cup (P_{i+2}) \cup \cdots \cup (P_{i+k}).
\end{aligned}$$

This gives a contradiction since $\{P_0, P_1, \ldots P_{i-1}, P_{i+1}, P_{i+2}, \ldots, P_{i+k}\} \cap G'_i = \varnothing$ and $i + k \leq w$. Therefore, $|\bar{G}'_i \setminus \bigcup_{0 \leq j \leq i-1} \bar{G}'_j| \geq w - i + 1$.

Now, from earlier we recall that $|\mathscr{G}'| > w + 1$. Therefore, there exist $w + 1$ distinct elements $G_0, G_1, \ldots, G_w \in \mathscr{G}'$ and

$$\begin{aligned}
\Big| \bigcup_{0 \leq i \leq w} \bar{G}_i \Big| &= |\bar{G}_0| + |\bar{G}_1 \setminus \bar{G}_0| + |\bar{G}_2 \setminus (\bar{G}_1 \cup \bar{G}_0)| + \cdots + |\bar{G}_w \setminus (\bar{G}_{w-1} \cup \bar{G}_{w-2} \cup \cdots \cup \bar{G}_0)| \\
&\geq (w+1) + w + (w-1) + \cdots + 2 + 1 = \frac{(w+1)(w+2)}{2} = \binom{w+2}{2}.
\end{aligned}$$

Hence, $b \geq \Big| \bigcup_{0 \leq i \leq w} \bar{G}_i \Big| \geq \binom{w+2}{2}$. However, $b < \binom{w+2}{2}$ so we have obtained a contradiction and thus $b \geq \min\left\{ |\mathscr{G}|, \binom{w+2}{2} \right\}$. □

From this latest theorem we see that if an incidence structure $\mathscr{K}$ is a $(\mathscr{G}, w)$-KDP, and $|\mathscr{G}| \leq \binom{w+2}{2}$, then the number of blocks in $\mathscr{K}$ is at least as many as in a trivial $\mathscr{G}$-KDP. Hence, in these situations, the best, (in the sense of the least number of blocks) that we can achieve is via a trivial $\mathscr{G}$-KDP.

Similar results to Theorem 6.2.7 have been obtained by other authors in the case of (t, w)-KDPs, see [25, 78, 86]. In particular, Stinson, Wei and Zhu [86] give the following bound on b for $(1, w)$-KDPs.

Result 6.2.10. [86, Theorem 1.1] *For any $(1, w)$-KDP on v points, where $w \geq 2$,*

$$b \geq c \frac{w^2}{\log_2 w} \log_2 v \quad \textit{for some constant } c.$$

In fact, Stinson *et al.* suggest that the constant c may be approximately $1/2$ for any $w \geq 2$. This compares favourably to Theorem 6.2.7 in which the error term, $H(w, b)$, is dependent upon w. However, there appears to be an oversight in Result 6.2.10, as the only non-negative constant c that makes Result 6.2.10 true for any $w \geq 2$ is $c = 0$. This is demonstrated in the following example.

Example 6.2.1. For each $b \in \mathbb{N}$, where $b \geq 3$, let $\mathscr{B}_b$ be any finite set of b elements, let $\mathscr{P}_b = \{\{x\} : x \in \mathscr{B}_b\}$ and let $(P, x) \in \mathscr{I}_b$ if, and only if, $P = \{x\}$. Then, the finite incidence structure $\mathscr{K}_b = (\mathscr{P}_b, \mathscr{B}_b, \mathscr{I}_b)$ is a $(1, w)$-KDP on v points, where $v = b$ and $w = b - 1$.
If, $b \geq c\dfrac{w^2}{\log_2 w}\log_2 v$, holds for $\mathscr{K}_b$, then

$$b \geq c\frac{(b-1)^2}{\log_2(b-1)}\log_2 b \;\Rightarrow\; b \geq c(b-1)^2 \;\Rightarrow\; c \leq \frac{b}{b^2 - 2b + 1}.$$

Therefore, $c = 0$ is the only constant for which $b \geq c\dfrac{w^2}{\log_2 w}\log_2 v$ holds for all the incidence structures $\mathscr{K}_b$, since $\displaystyle\lim_{b\to\infty} \frac{b}{b^2 - 2b + 1} = 0$.

Later, in [86, Theorem 3.2], the constant from Result 6.2.10 is used inductively. Unfortunately, $c = 0$ renders [86, Theorem 3.2] trivial. On the other hand, for v large relative to w, Theorem 6.2.10 holds and, as such (with some alterations to the proof), Theorem 3.2 in [86] can be partially resurrected.

6.3 Internal and External Bounds

In this section we use our earlier bounds on the total number of blocks in a $(\mathscr{G}, \mathscr{F})$-KDP, $\mathscr{K}$, in order to estimate, among other things, the number of blocks incident with each point of $\mathscr{K}$. The way that we accomplish this is by considering the internal and external structures of a given $(\mathscr{G}, \mathscr{F})$-KDP.

We first restate (using our new notation) a bound from Chapter 5 (Corollary 5.1.29) which was obtained by using both the internal and external structure of a given incidence structure.

Theorem 6.3.1. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP where $2 \leq |G| < |\mathscr{P}|$ for all $G \in \mathscr{G}$ and $w \geq 2$, then for each $P \in \mathscr{P}$*

$$\log_2 |\{G \in \mathscr{G} : P \in G\}| < r(P) < b - \log_2 |\{G \in \mathscr{G} : P \notin G\}|.$$

Our next result in this direction improves upon Theorem 6.3.1.

Proposition 6.3.2. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP, where $2 \leq |G| < |\mathscr{P}|$ for all $G \in \mathscr{G}$ and $w \geq 2$, then for each $P \in \mathscr{P}$,*

$$\log_2 \binom{|\mathscr{G}_P|}{\lceil w/2 \rceil} \ \leq \ r(P) \ \leq \ b - \log_2 \binom{|\mathscr{G}^P|}{\lceil (w-1)/2 \rceil},$$

where $\mathscr{G}_P = \{G \in \mathscr{G} : P \in G\}$ and $\mathscr{G}^P = \{G \in \mathscr{G} : P \notin G\}$.

Proof. We know from Corollary 5.1.10 that $\mathscr{K}_P = (\mathscr{P}_P, \mathscr{B}_P, \mathscr{I}_P)$ is a $(\mathscr{G}'_P, w)$-KDP, where $\mathscr{G}'_P = \{G \backslash \{P\} : P \in G \in \mathscr{G}\}$. We also know from Corollary 5.1.22 that $\mathscr{K}^P = (\mathscr{P}^P, \mathscr{B}^P, \mathscr{I}^P)$ is a $(\mathscr{G}^P, w-1)$-KDP, since $\mathscr{G}^P = \{G \in \mathscr{G} : G \subseteq \mathscr{P}^P\} = \{G \in \mathscr{G} : P \notin G\}$. Now, from Theorem 6.1.8 we have

$$b_P \geq \log_2 \binom{|\mathscr{G}'_P|}{\lceil w/2 \rceil} \qquad \text{and} \qquad b^P \geq \log_2 \binom{|\mathscr{G}^P|}{\lceil (w-1)/2 \rceil}.$$

Since $r(P) = b_P = b - b^P$, the result follows. □

If the set of privileged subsets forms a Sperner system then we may further improve upon this bound.

Proposition 6.3.3. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP, where $2 \leq |G| < |\mathscr{P}|$ for all $G \in \mathscr{G}$, $w \geq 2$ and $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$, then for each $P \in \mathscr{P}$,*

$$\log_2 \binom{|\mathscr{G}_P|}{w} + 1 \ \leq \ r(P) \ \leq \ b - \log_2 \binom{|\mathscr{G}^P|}{w-1} - 1,$$

where $\mathscr{G}_P = \{G \in \mathscr{G} : P \in G\}$ and $\mathscr{G}^P = \{G \in \mathscr{G} : P \notin G\}$.

Proof. As with Proposition 6.3.2, $\mathscr{K}_P$= $(\mathscr{P}_P, \mathscr{B}_P, \mathscr{I}_P)$ is a $(\mathscr{G}'_P, w)$-KDP, where $\mathscr{G}'_P = \{G\backslash\{P\} : P \in G \in \mathscr{G}\}$ and $\mathscr{K}^P$= $(\mathscr{P}^P, \mathscr{B}^P, \mathscr{I}^P)$ is a $(\mathscr{G}^P, w–1)$-KDP. Since, $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$, $\mathscr{G}_P$ forms a Sperner system on $\mathscr{P}_P$ and $\mathscr{G}^P$ forms a Sperner system on $\mathscr{P}^P$. From Theorem 6.2.3 we have

$$b_P \geq \log_2 \binom{|\mathscr{G}'_P|}{w} + 1 \quad \text{and} \quad b^P \geq \log_2 \binom{|\mathscr{G}^P|}{w-1} + 1.$$

Since $r(P) = b_P = b - b^P$, the result follows. □

By generalising the notion of an internal structure we are able to calculate lower bounds on the number of blocks incident with every point in a given set of points.

Definition 6.3.4. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. Then, for any set of points $\varnothing \neq X \subseteq \mathscr{P}$ we define $\mathscr{K}_X$, the **internal structure of $\mathscr{K}$ at X** to be $\mathscr{K}_X$= $(\mathscr{P}_X, \mathscr{B}_X, \mathscr{I}_X)$, where $\mathscr{B}_X = \bigcap_{P\in X}(P)$, $\mathscr{P}_X = (\mathscr{B}_X)\backslash X$, and for any $P \in \mathscr{P}_X$ and $x \in \mathscr{B}_X$, $(P, x) \in \mathscr{I}_X$, if, and only if, $(P, x) \in \mathscr{I}$.*

Thus, for the internal structure $\mathscr{K}_X$ of a finite incidence structure $\mathscr{K}$= $(\mathscr{P}, \mathscr{B}, \mathscr{I})$ at $\varnothing \neq X \subseteq \mathscr{P}$, $|\mathscr{B}_X| = \left|\bigcap_{P\in X}(P)\right|$. Hence, the problem of calculating the number of blocks incident with every point in a given set of points X reduces to the problem of calculating b in an appropriate internal structure. Before we can do this, we first show that the internal structure of a $(\mathscr{G}, \mathscr{F})$-KDP at a set X is a $(\mathscr{G}', \mathscr{F}')$-KDP for some $\mathscr{G}'$ and $\mathscr{F}'$. Theorem 6.3.5 is a generalisation of Theorem 5.1.9 however, its proof is completely analogous and so is not presented here.

Theorem 6.3.5. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, \mathscr{F})$-KDP, then for every $\varnothing \neq X \subseteq \mathscr{P}$, $\mathscr{K}_X$= $(\mathscr{P}_X, \mathscr{B}_X, \mathscr{I}_X)$ is a $(\mathscr{G}_X, \mathscr{F}_X)$-KDP where, $\mathscr{G}_X = \{G \setminus X : X \subseteq G \in \mathscr{G} \text{ and } \varnothing \neq G \setminus X \subseteq \mathscr{P}_X\}$ and $\mathscr{F}_X = \{F \cap \mathscr{P}_X : X \cap F = \varnothing \text{ and } F \cap \mathscr{P}_X \neq \varnothing\}$.*

The following corollary is for the special case when $\mathscr{F}$ consists of all the subsets of $\mathscr{P}$ of cardinality at most w.

Corollary 6.3.6. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP, where $w \geq 1$ and $|G| < |\mathscr{P}|$ for all $G \in \mathscr{G}$, then for every $\varnothing \neq X \subseteq \mathscr{P}$, $\mathscr{K}_X = (\mathscr{P}_X, \mathscr{B}_X, \mathscr{I}_X)$ is a $(\mathscr{G}_X, w)$-KDP where, $\mathscr{G}_X = \{G \setminus X : X \subsetneqq G \in \mathscr{G}\}$.*

We can now calculate a lower bound on the number of blocks incident with every point in a given set of points.

Theorem 6.3.7. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP, where $w \geq 1$ and $|G| < |\mathscr{P}|$ for all $G \in \mathscr{G}$, then for any $\varnothing \neq X \subseteq \mathscr{P}$,*

$$\left| \bigcap_{P \in X} (P) \right| \geq \log_2 \binom{|\mathscr{G}_X|}{\lceil w/2 \rceil}, \text{ where } \mathscr{G}_X = \{G \in \mathscr{G} : X \subsetneqq G\}.$$

Proof. We already know from Corollary 6.3.6 that $\mathscr{K}_X = (\mathscr{P}_X, \mathscr{B}_X, \mathscr{I}_X)$ is a $(\mathscr{G}'_X, w)$-KDP where, $\mathscr{G}'_X = \{G \setminus X : X \subsetneqq G \in \mathscr{G}\}$. Then, from Theorem 6.1.8 we have

$$b_X \geq \log_2 \binom{|\mathscr{G}'_X|}{\lceil w/2 \rceil}$$

and the result follows. □

If $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$, then $\mathscr{G}'_X$ forms a Sperner system on $\mathscr{P}_X$ and we can improve upon this bound using Theorem 6.2.3.

Theorem 6.3.8. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP, where $w \geq 1$, $|G| < |\mathscr{P}|$ for all $G \in \mathscr{G}$ and $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$, then for any $\varnothing \neq X \subseteq \mathscr{P}$,*

$$\left| \bigcap_{P \in X} (P) \right| \geq \log_2 \binom{|\mathscr{G}_X|}{w} + 1, \text{ where } \mathscr{G}_X = \{G \in \mathscr{G} : X \subsetneqq G\}.$$

Now, by generalising the notion of an external structure we are able to calculate upper bounds on the number of blocks incident with any point in a given set of points.

Definition 6.3.9. *Let $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ be a finite incidence structure. Then, for any set of points $\varnothing \neq X \subseteq \mathscr{P}$ we define $\mathscr{K}^X$, the **external structure***

***of* $\mathscr{K}$ *at* X** *to be* $\mathscr{K}^X = (\mathscr{P}^X, \mathscr{B}^X, \mathscr{I}^X)$*, where* $\mathscr{B}^X = \mathscr{B} \setminus \bigcup_{P\in X}(P)$*,* $\mathscr{P}^X = (\mathscr{B}^X)$*, and for any* $P \in \mathscr{P}^X$ *and* $x \in \mathscr{B}^X$*,* $(P, x) \in \mathscr{I}^X$*, if, and only if,* $(P, x) \in \mathscr{I}$*.*

Thus, for the external structure $\mathscr{K}^X$ of a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ at $\varnothing \neq X \subseteq \mathscr{P}$, $|\mathscr{B}^X| = b - \left|\bigcup_{P\in X}(P)\right|$. Hence, the problem of calculating the number of blocks not incident with any point in a given subset of points, X, reduces to the problem of calculating b in an appropriate external structure. Before we can do this, we first show that the external structure of a $(\mathscr{G}, \mathscr{F})$-KDP at a set X is a $(\mathscr{G}', \mathscr{F}')$-KDP for some $\mathscr{G}'$ and $\mathscr{F}'$. Theorem 6.3.10 is a generalisation of Theorem 5.1.21, however its proof is completely analogous and is not presented here.

Theorem 6.3.10. *If a finite incidence structure* $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ *is a* $(\mathscr{G}, \mathscr{F})$*-KDP, then for every* $\varnothing \neq X \subseteq \mathscr{P}$*,* $\mathscr{K}^X = (\mathscr{P}^X, \mathscr{B}^X, \mathscr{I}^X)$ *is a* $(\mathscr{G}^X, \mathscr{F}^X)$*-KDP, where*

$$\mathscr{G}^X = \{G \in \mathscr{G} : G \subseteq \mathscr{P}^X\} \quad \textit{and}$$
$$\mathscr{F}^X = \{F \cap \mathscr{P}^X : X \subseteq F \in \mathscr{F} \textit{ and } F \cap \mathscr{P}^X \neq \varnothing\}.$$

The following corollary is for the special case when $\mathscr{F}$ consists of all the subsets of $\mathscr{P}$ of cardinality at most w.

Corollary 6.3.11. *If a finite incidence structure* $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ *is a* $(\mathscr{G}, w)$*-KDP, then for every* $\varnothing \neq X \subseteq \mathscr{P}$*, where* $|X| < w$*,* $\mathscr{K}^X = (\mathscr{P}^X, \mathscr{B}^X, \mathscr{I}^X)$ *is a* $(\mathscr{G}^X, w - |X|)$*-KDP, where* $\mathscr{G}^X = \{G \in \mathscr{G} : G \cap X = \varnothing\}$*.*

We can now calculate an upper bound on the number of blocks incident with any point in a given set of points.

Theorem 6.3.12. *If a finite incidence structure* $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ *is a* $(\mathscr{G}, w)$*-KDP, then for any* $\varnothing \neq X \subseteq \mathscr{P}$ *where* $|X| < w$*,*

$$\left|\bigcup_{P\in X}(P)\right| \leq b - \log_2 \binom{|\mathscr{G}^X|}{\lceil \frac{w-|X|}{2} \rceil}, \quad \textit{where } \mathscr{G}^X = \{G \in \mathscr{G} : G \cap X = \varnothing\}.$$

Proof. We already know from Corollary 6.3.11 that $\mathscr{K}^X = (\mathscr{P}^X, \mathscr{B}^X, \mathscr{I}^X)$ is a $(\mathscr{G}^X, w-|X|)$-KDP, since $\mathscr{G}^X = \{G \in \mathscr{G} : G \subseteq \mathscr{P}^X\} = \{G \in \mathscr{G} : G \cap X = \varnothing\}$. Then, from Theorem 6.1.8 we have

$$b^X \geq \log_2 \binom{|\mathscr{G}^X|}{\lceil \frac{w-|X|}{2} \rceil}$$

and the result follows. □

If $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$, then $\mathscr{G}^X$ forms a Sperner system on $\mathscr{P}^X$ and we can improve upon this bound using Theorem 6.2.3.

Theorem 6.3.13. *If a finite incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ is a $(\mathscr{G}, w)$-KDP and $\mathscr{G}$ forms a Sperner system on $\mathscr{P}$, then for any $\varnothing \neq X \subseteq \mathscr{P}$ where $|X| < w$,*

$$\left| \bigcup_{P \in X} (P) \right| \leq b - \log_2 \binom{|\mathscr{G}^X|}{w - |X|} - 1, \text{ where } \mathscr{G}^X = \{G \in \mathscr{G} : G \cap X = \varnothing\}.$$

As mentioned at the beginning of Section 6.1, we have been unable to obtain any bounds on the total number of blocks in a completely general $(\mathscr{G}, \mathscr{F})$-KDP. However, throughout this chapter we have obtained several bounds on the total number of blocks in a $(\mathscr{G}, w)$-KDP. We know from Theorem 5.1.31 that the complement of a $(\mathscr{G}, \mathscr{F})$-KDP on b blocks is a $(\mathscr{F}, \mathscr{G})$-KDP on b blocks. Therefore, all our bounds on the number of blocks in a $(\mathscr{G}, w)$-KDP apply equally to a $(t, \mathscr{F})$-KDP, but we have not specified these bounds individually.

Chapter 7

Summary and Future Work

In this chapter we summarise the main contributions of this thesis and highlight areas of future study that follow from our work.

7.1 Summary

Throughout this thesis we have investigated a notion of generalised key distribution patterns, defined as $(\mathscr{G},\mathscr{F})$-KDPs in Definition 3.1.1, and studied the mathematics behind them. Our first results on $(\mathscr{G},\mathscr{F})$-KDPs were given in Chapter 3 and concerned their most basic properties. In investigating these basic properties we found some unexpected consequences. For example, it is possible that:

1. for some privileged subsets $G \in \mathscr{G}$ in a $(\mathscr{G},\mathscr{F})$-KDP there may be no shared blocks, that is, $|\bigcap_{P\in G}(P)| = 0$;

2. for some $G' \subsetneq G \in \mathscr{G}$ in a $(\mathscr{G},\mathscr{F})$-KDP there may exist an $F \in \mathscr{F}$ such that $\bigcap_{P\in G'}(P) \subseteq \bigcup_{Q\in F}(Q)$. In particular, there is a $(\mathscr{G}, w)$-KDP where $\mathscr{G} = \{G \in 2^{\mathscr{P}} : |G| = t\}$, that is not a (t, w)-KDP (see Example 3.3.1).

We also investigated the concepts of complete security and complete communication. That is, the case in which $\bigcap_{P\in G}(P) \not\subseteq \bigcup_{Q\in \mathscr{P}\setminus G}(Q)$ for every $G \in \mathscr{G}$ and the case in which $\bigcap_{P\in \mathscr{P}\setminus F}(P) \not\subseteq \bigcup_{Q\in F}(Q)$ for every $F \in \mathscr{F}$.

These cases correspond precisely to trivial $\mathscr{G}$-KDPs and cotrivial $\mathscr{F}$-KDPs respectively.

In Chapter 4 we considered a predefined incidence structure, $\mathscr{K}$, and investigated all possible sets of privileged and forbidden subsets for which $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP. Firstly, we addressed the points and blocks that play no role in a $(\mathscr{G}, \mathscr{F})$-KDP. We analysed concepts of redundancy and introduced techniques for eliminating redundancy from existing $(\mathscr{G}, \mathscr{F})$-KDPs. Secondly, we attempted to find the largest possible set of privileged and forbidden subsets for which $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP. To this end, we observed the trade-off between the size of the set of privileged subsets and the size of the set of forbidden subsets and defined a partial ordering. Finally, we showed that there is, in general (according to our ordering) no largest $(\mathscr{G}, \mathscr{F})$-KDP for a given incidence structure, instead there are many distinct maximal $(\mathscr{G}, \mathscr{F})$-KDPs.

In Chapter 5, we began by considering some of the standard operations that may be applied to incidence structures and we examined their effect on the corresponding $(\mathscr{G}, \mathscr{F})$-KDPs. In particular, we considered the operations of internal structures, external structures and complement structures. We also generalised some of the constructions of Mitchell and Piper [60], from (t, w)-KDPs to $(\mathscr{G}, \mathscr{F})$-KDPs. Lastly, we provided a new method for constructing $(\mathscr{G}, \mathscr{F})$-KDPs. Notably this method of construction gives rise to $(\mathscr{G}, \mathscr{F})$-KDPs that are far from being (t, w)-KDPs. Moreover, it appears that this construction can be generalised to apply to other abstract finite convex structures, such as those found in [27]. Since the calculations of $|\mathscr{G}|$, $|\mathscr{F}|$, $|\mathscr{B}|$ and $|\mathscr{P}|$ are straightforward for these constructions, they may be used as “test cases” for some of our theorems, particularly those concerning the number of blocks in a $(\mathscr{G}, \mathscr{F})$-KDP.

In Chapter 6 we examined the efficiency of $(\mathscr{G}, \mathscr{F})$-KDPs, more specifically, we considered the size of the block set of a $(\mathscr{G}, \mathscr{F})$-KDP. We were able to obtain several lower bounds for the number of blocks required for a given $(\mathscr{G}, \mathscr{F})$-KDP. In the cases when the set of privileged subsets in a $(\mathscr{G}, \mathscr{F})$-KDP forms a Sperner system, we were able to obtain similar results to those obtained for (t, w)-KDPs. However, in the cases when the set of privileged subsets in a $(\mathscr{G}, \mathscr{F})$-KDP do not form a Sperner system, we had to work harder in order to obtain any results. As a consequence of these investigations, we were also able to find lower bounds on the number of blocks in a given $(\mathscr{G}, \mathscr{F})$-KDP that are incident with (i) a single point, or (ii) a set of points. These results also enabled us to estimate the number of blocks in a given $(\mathscr{G}, \mathscr{F})$-KDP that are **not** incident with (i) a single point, or (ii) a set of points. Some of these estimates have consequences for other theorems, such as Theorem 5.2.3, Theorem 5.2.6, Theorem 5.1.1 and Theorem 5.1.4, (also see Section 7.2).

7.2 Future Work

Two of the most important problems in our study of $(\mathscr{G}, \mathscr{F})$-KDPs remain open:

1. The problem of constructing efficient $(\mathscr{G}, \mathscr{F})$-KDPs (that is, $(\mathscr{G}, \mathscr{F})$-KDPs in which the number of blocks is minimised) for given families of privileged and forbidden subsets.

2. The problem of calculating good lower bounds on the number of blocks in a general $(\mathscr{G}, \mathscr{F})$-KDP, that is, a $(\mathscr{G}, \mathscr{F})$-KDP where there are no constraints on the sets of privileged and forbidden subsets.

7.2.1 Open Problems

We now present some specific open problems that follow directly from our work. These problems are related to the two main open problems detailed above.

Problem 1. *Given a set of points $\mathscr{P}$ and families of non-empty subsets, $\mathscr{G}$ and $\mathscr{F}$ of $\mathscr{P}$, construct an incidence structure $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$ such that $\mathscr{K}$ is a $(\mathscr{G}, \mathscr{F})$-KDP and*

$$|\mathscr{B}| \;/\; \big|\{(G, F) \in \mathscr{G} \times \mathscr{F} : G \cap F = \varnothing\}\big|$$

is as small as possible.

Thus far, the only construction that we have been able to achieve that has shown any promise in this direction is Theorem 5.3.7.

Problem 2. *For a given $(\mathscr{G}, \mathscr{F})$-KDP, $\mathscr{K} = (\mathscr{P}, \mathscr{B}, \mathscr{I})$, calculate a "good" lower bound for $|\mathscr{B}|$.*

As previously mentioned, we have been unable to obtain any lower bounds on the number of blocks in a $(\mathscr{G}, \mathscr{F})$-KDP unless we impose additional constraints on the sets of privileged and forbidden subsets.

Our most general result so far was given in Theorem 6.1.1, where we showed that $|\mathscr{B}| \geq \log_2 |\mathscr{G}|$ for $(\mathscr{G}, \mathscr{F})$-KDPs that satisfy a relatively mild restriction on $\mathscr{F}$. This contrasts with the situation in Chapter 6 where we obtained good bounds for $|\mathscr{B}|$ in the case of $(\mathscr{G}, w)$-KDPs.

Problem 3. *Is it possible to extend Theorem 5.3.7 (our direct construction that uses a discrete analogue of convexity) to construct $(\mathscr{G}, \mathscr{F})$-KDPs using other finite convex geometries?*

There is a large literature on finite convex geometries, see [27] and the references within. Some of these convex geometries admit separation theorems, along the same lines as Lemma 5.3.5. For these convex geometries, it should be possible to construct $(\mathscr{G}, \mathscr{F})$-KDPs in the same way as we did in Theorem 5.3.7. It is also probably worth pursuing the question of when it is possible to embed a given $(\mathscr{G}, \mathscr{F})$-KDP into one of these convex structures, as discussed at the end of Chapter 5.

The next open problem that we consider involves some of our results from Section 6.3.

Problem 4. *Is it possible to recursively use the results from Section 6.3 on internal and external structures of* $(\mathscr{G}, \mathscr{F})$*-KDPs, to obtain lower bounds on the number of blocks?*

In [86], Stinson, Wei and Zhu recursively used results (equivalent to those of internal and external structures) on (t, w)-CFFs to determine lower bounds for the size of the ground set of a (t, w)-CFF. With some restrictions on the sets of privileged and forbidden subsets it seems possible that the approach taken by Stinson, Wei and Zhu in [86], could be applied to $(\mathscr{G}, \mathscr{F})$-KDPs.

The final open problem that we present here concerns an inequality that arose in the study of the number of blocks required in a (t, w)-KDP (see Corollary 6.2.4).

Problem 5. *Suppose that* $1 \leq w \leq t < v$*, give a combinatorial proof of the inequality*

$$\binom{\binom{v}{w}}{t} \Big/ \binom{\binom{v}{t}}{w} \geq \frac{w!(t!)^w}{t!(w!)^t}.$$

In Appendix A we present an algebraic proof of this inequality. However, the combinatorial nature of the inequality itself would strongly suggest that a combinatorial proof is possible and would more intuitively reflect the nature of the inequality.

Appendix A

Proof of Theorem 6.2.5

We begin with three inequalities that are required for our theorem.

Lemma A.0.1. [61, Lemma 1] *If* $1 \leq w < v$ *and* $1 \leq j \leq w$ *then,*

$$[v(v-1)\cdots(v-w+1) - jw!][v-w+j] \geq v(v-1)\cdots(v-w+1)(v-w).$$

Proof. Fix $1 \leq j \leq w$ then,

$$[v(v-1)\cdots(v-w+1) - jw!][(v-w)+j] =$$
$$v(v-1)\cdots(v-w+1)(v-w) + \big[jv(v-1)\cdots(v-w+1) - j^2w! - jw!(v-w)\big].$$

We claim that $jv(v-1)\cdots(v-w+1) - j^2w! - jw!(v-w) \geq 0$.
To see this, we simply do more algebra.

$$\begin{aligned} & jv(v-1)\cdots(v-w+1) - j^2w! - jw!(v-w) \geq 0 \\ \iff\ & jv(v-1)\cdots(v-w+1) \geq j^2w! + jw!(v-w) \\ \iff\ & \binom{v}{w} \geq j + (v-w). \end{aligned}$$

Now, $j + (v-w) \leq v$.
On the other hand, because $1 \leq w < v$, we know that $\binom{v}{w} \geq v$.
Therefore,
$[v(v-1)\cdots(v-w+1) - jw!][v-w+j]$

$$\geq v(v-1)\cdots(v-w+1)(v-w). \quad \square$$

Lemma A.0.2. [61, Lemma 2] *If* $1 < w < v$ *and* $1 \leq j < v$ *then,*

$$[v(v-1)\cdots(v-w+1)-jw!] \geq (v-1)(v-2)\cdots(v-w+1)(v-w) \geq (v-w)^w.$$

Proof. To prove this, we again do some algebra.

$$[v(v-1)\cdots(v-w+1)-jw!] - (v-w)(v-1)(v-2)\cdots(v-w+1) \geq 0$$

$$\begin{aligned} &\iff -jw! + w(v-1)(v-2)\cdots(v-w+1) \geq 0 \\ &\iff (v-1)(v-2)\cdots(v-w+1) \geq j(w-1)! \\ &\iff \left[\frac{v-1}{j}\right]\left[\frac{v-2}{w-1}\right]\cdots\left[\frac{v-w+1}{2}\right] \geq 1; \end{aligned}$$

which is true since $1 \leq j < v$ and $w < v$. □

Lemma A.0.3. [61, Lemma 3] *If* $1 \leq w < v$, *then*

$$\left[\prod_{j=1}^{w}[v(v-1)\cdots(v-w+1)-jw!]\right][v(v-1)\cdots(v-w+1)] \geq [v(v-1)\cdots(v-w)]^w.$$

Proof. This follows directly from Lemma A.0.1 and the fact that:

$$\left[\prod_{j=1}^{w}[v(v-1)\cdots(v-w+1)-jw!]\right][v(v-1)\cdots(v-w+1)] = \prod_{j=1}^{w}[v(v-1)\cdots(v-w+1)-jw!][v-w+j].$$ □

We are now ready to present the relationship between $\binom{\binom{v}{t}}{w}$ and $\binom{\binom{v}{w}}{t}$.

Theorem A.0.4. [61, Theorem 1] *If* $1 < w < t < v$ *are natural numbers then,*

$$\binom{\binom{v}{w}}{t} \Big/ \binom{\binom{v}{t}}{w} > \frac{w!(t!)^w}{t!(w!)^t}.$$

Proof. Suppose that $1 < w < t < v$ are natural numbers then,

$$\begin{aligned}
\binom{\binom{v}{w}}{t} &= \frac{1}{t!}\left[\prod_{j=0}^{t-1}\frac{[v(v-1)\cdots(v-w+1)-jw!]}{w!}\right] \\
&\geq \frac{1}{t!(w!)^t}\left[\prod_{j=0}^{w}[v(v-1)\cdots(v-w+1)-jw!]\right][(v-w)^w]^{t-w-1}\text{(by Lemma A.0.2)} \\
&= \frac{1}{t!(w!)^t}\left[v(v-1)\cdots(v-w+1)\prod_{j=1}^{w}[v(v-1)\cdots(v-w+1)-jw!]\right][(v-w)^{t-w-1}]^w \\
&\geq \frac{1}{t!(w!)^t}\Big([v(v-1)\cdots(v-w)]^w\cdot[(v-w)^{t-w-1}]^w\Big)\text{ (by Lemma A.0.3)} \\
&= \frac{1}{t!(w!)^t}\Big([v(v-1)\cdots(v-w)(v-w)^{t-w-1}]^w\Big) \\
&\geq \frac{1}{t!(w!)^t}\Big([v(v-1)\cdots(v-w)\cdots(v-t+1)]^w\Big) \\
&> \frac{w!(t!)^w}{t!(w!)^t}\left[\frac{1}{w!}\prod_{j=0}^{w-1}\frac{[v(v-1)\cdots(v-t+1)-jt!]}{t!}\right] \\
&= \frac{w!(t!)^w}{t!(w!)^t}\binom{\binom{v}{t}}{w}.
\end{aligned}$$

□

To understand this inequality better we need the following crude estimate.

Proposition A.0.5. [61, Proposition 2] *If* $1 \leq w \leq t$ *are natural numbers then*

$$\frac{w!(t!)^w}{t!(w!)^t} \geq \left(\frac{w+1}{2}\right)^{(t-w)} \geq 1.$$

Proof. We need only consider the case when $1 < w < t$.

$$\begin{aligned}
\frac{w!(t!)^w}{t!(w!)^t} &= \frac{(t!)^{(w-1)}}{(w!)^{(t-1)}} = \frac{(t!)^{(w-1)}}{(w!)^{(t-w)}(w!)^{(w-1)}} = \frac{[t(t-1)\cdots(w+1)]^{(w-1)}}{(w!)^{(t-w)}} \\
&= \underbrace{\left(\frac{t^{(w-1)}}{w!}\right)\left(\frac{(t-1)^{(w-1)}}{w!}\right)\cdots\left(\frac{(w+1)^{(w-1)}}{w!}\right)}_{(t-w)-\text{factors}}.
\end{aligned}$$

Now, $\dfrac{j^{(w-1)}}{w!} \geq \dfrac{w+1}{2}$ for all $(w+1) \leq j$ since,

$$\begin{aligned}
\frac{j^{(w-1)}}{w!} &= \underbrace{\left(\frac{j}{w}\right)\left(\frac{j}{w-1}\right)\cdots\left(\frac{j}{3}\right)\left(\frac{j}{2}\right)}_{(w-1)-\text{times}} \\
&\geq \underbrace{\left(\frac{j}{w}\right)\left(\frac{j}{w-1}\right)\cdots\left(\frac{j}{3}\right)\left(\frac{w+1}{2}\right)}_{(w-1)-\text{factors}} \geq \frac{w+1}{2}.
\end{aligned}$$

□

It it easy to see that Theorem 6.2.5 follows directly from Theorem A.0.4 together with Proposition A.0.5.

It should be noted that the inequality in Theorem A.0.4 is a generalisation of [36, Theorem 5] which examines the special case when $t = 3$ and $w = 2$. In [61] it is shown that in some sense the inequality in Theorem A.0.4 is sharp. Furthermore, a generalisation of this result is also given. However, as these results are not directly relevant to our study of $(\mathscr{G}, \mathscr{F})$-KDPs they are not presented here.

Bibliography

[1] D. Angluin and L. G. Valiant, *Fast probabilistic algorithms for Hamiltonian circuits and matchings*, Journal of Computer and System Sciences **18** (1979), 155–193.

[2] S. R. Blackburn, T. Etzion, K. M. Martin, and M. B. Paterson, *Efficient key predistribution for grid-based wireless sensor networks. Information Theoretic Security. Lecture Notes in Computer Science*, vol. 5155, pp. 54–69, Springer, Heidelburg, 2008.

[3] S. R. Blackburn, T. Etzion, K. M. Martin, and M. B. Paterson, *Distinct difference configurations: Multihop paths and key predistribution in sensor networks*, IEEE Transactions on Information Theory **56** (2010), 3961–3972.

[4] S. R. Blackburn and F. Piper, *Applications of combinatorics to security (proceedings from the application of combinatorial mathematics), 1994*, pp. 31–47, Oxford University Press, Oxford, 1997.

[5] R. Blom, *Non-public key distribution. Advances in Cryptology - CRYPTO '82*, pp. 231–236, Plenum Press, New York, 1983.

[6] R. Blom, *An optimal class of symmetric key generation systems. Advances in Cryptology - EUROCRYPT '84. Lecture Notes in Computer Science*, vol. 209, pp. 335–338, Springer-Verlag, Berlin, 1985.

[7] C. Blundo and P. D'Arco, *The key establishment problem. Foundations of Security Analysis and Design II. Lecture Notes in Computer Science*, vol. 2946, p. 1106, Springer-Verlag, Berlin, 2004.

[8] C. Blundo, A. DeSantis, U. Vaccaro, A. Herzberg, S. Kutten, and M. Yung, *Perfectly secure key distribution for dynamic conferences. Advances in Cryptology - CRYPTO '92. Lecture Notes in Computer Science*, vol. 740, pp. 471–486, Springer-Verlag, Berlin, 1993.

[9] B. Bollobás, *On generalized graphs*, Acta Mathematica Academiae Scientiarum Hungaricae **16** (1965), 447–452.

[10] B. Bollobás, *Random graphs*, Academic Press, London, 1985.

[11] B. Bollobás, *Combinatorics*, Cambridge University Press, Cambridge, 1986.

[12] C. Boyd and A. Mathuria, *Protocols for authentication and key establishment*, Springer-Verlag, Berlin, 2003.

[13] S. A. Camtepe and B. Yener, *Combinatorial designs of key distribution mechanisms for wireless sensor networks. Computer Security - ESORICS 2004. Lecture Notes in Computer Science*, vol. 3193, pp. 293–308, Springer-Verlag, Berlin, 2004.

[14] S. A. Camtepe and B. Yener, *Key distribution mechanisms for wireless sensor networks: A survey*, Rensselaer Polytechnic Institute, Computer Science Department, Technical Report TR-05-07, 2005.

[15] S. A. Camtepe and B. Yener, *Combinatorial designs of key distribution mechanisms for wireless sensor networks*, IEEE / ACM Transactions on Networking **15** (2007), 346–358.

[16] D. Chakrabarti, S. Maitra, and B. Roy, *A hybrid design of key predistribution scheme for wireless sensor networks. ICISS 2005. Lecture Notes in Computer Science*, vol. 3803, pp. 228–238, Springer-Verlag, Berlin, 2005.

[17] D. Chakrabarti, S. Maitra, and B. Roy, *A key predistribution scheme for wireless sensor networks: merging blocks in combinatorial design. ISC 2005. Lecture Notes in Computer Science*, vol. 3650, pp. 89–103, Springer-Verlag, Berlin, 2005.

[18] D. Chakrabarti and J. Seberry, *Combinatorial structures for design of wireless sensor networks. ACNS 2006. Lecture Notes in Computer Science*, vol. 3989, pp. 365–374, Springer-Verlag, Berlin, 2006.

[19] H. Chan, A. Perrig, and D. Song, *Random key predistribution schemes for sensor networks*, IEEE Symposium on Research in Security and Privacy (Conference Proceedings) (2003), 197–213.

[20] J. W. Dong, D. Y. Pei, and X. L. Wang, *A class of key predistribution schemes based on orthogonal arrays*, Journal of Computer Science and Technology **23** (2008), 825–831.

[21] J. W. Dong, D. Y. Pei, and X. L. Wang, *A key predistribution scheme based on 3-designs. INSCRYPT 2007. Lecture Notes in Computer Science*, vol. 4990, pp. 81–92, Springer-Verlag, Berlin, 2008.

[22] W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, and A. Khalili, *A pairwise key predistribution scheme for wireless sensor networks*, ACM Transactions on Information and System Security **8** (2005), 228–258.

[23] N. Dunford and J. T. Schwartz, *Linear operators 1: General theory*, Interscience Publishers, London, 1958.

[24] A. D'yachkov, V. Lebedev, P. Vilenkin, and S. Yekhanin, *Cover-free families and superimposed codes: Constructions, bounds and applications to cryptography and group testing*, IEEE International Symposium on Information Theory (Conference Proceedings) (2001), 117.

[25] A. G. Dyachkov and V. V. Rykov, *Bounds on the length of disjunctive codes (in Russian)*, Problemy Peredachi Informatsii **18** (1982), 7–13.

[26] M. Dyer, T. Fenner, A. Freize, and A. Thomason, *On key storage in secure networks*, Journal of Cryptology **8** (1995), 189–200.

[27] P. H. Edelman and R. E. Jamison, *The theory of convex geometries*, Geometriae Dedicata **19** (1985), 247–270.

[28] K. Engel, *Interval packing and covering in the boolean lattice*, Combinatorics, Probability & Computing **5** (1996), 373–384.

[29] P. Erdös, P. Franki, and Z. Füredi, *Families of finite sets in which no set is covered by the union of two others*, Journal of Combinatorial Theory A **33** (1982), 158–166.

[30] P. Erdös, P. Franki, and Z. Füredi, *Families of finite sets in which no set is covered by the union of r others*, Israel Journal of Mathematics **51** (1985), 75–89.

[31] L. Eschenauer and V. Gligor, *A key management scheme for distributed sensor networks*, Proceedings of 9th ACM Conference on Computer and Communication Security (2002), 41–47.

[32] A. Fiat and M. Naor, *Broadcast encryption. Advances in Cryptology - CRYPTO '93. Lecture Notes in Computer Science*, vol. 773, pp. 480–491, Springer-Verlag, Berlin, 1994.

[33] R. A. Fisher, *An examination of the different possible solutions of a problem in incomplete blocks*, Annals of Eugenics **10** (1940), 52–75.

[34] Z. Füredi, *On r-cover-free families*, Journal of Combinatorial Theory A **73** (1996), 172–173.

[35] J. R. Giles, *Convex analysis with application in the differentiation of convex functions: Research notes in mathematics 58*, Pitman Advanced Publishing Program, Boston, 1982.

[36] S. W. Golomb, *Iterated binomial coefficients*, American Mathematics Monthly **87** (1980), 719–727.

[37] M. (Jr.) Hall, *Combinatorial theory*, Blaisdell Publishing Company, Waltham, 1967.

[38] D. R. Hughes and F. C. Piper, *Design theory*, Cambridge University Press, Cambridge, 1985.

[39] C. J. A. Jansen, *On the key storage requirements for secure terminals*, Computers and Security **5** (1986), 145–149.

[40] W. H. Kautz and R. C. Singleton, *Nonrandom binary superimposed codes*, IEEE Transactions on Information Theory **10** (1964), 363–377.

[41] J. L. Kelley and I. Namioka, *Linear topological spaces*, D. Van Nostrand, Princeton, 1963.

[42] H. Kim and V. Lebedev, *On optimal superimposed codes*, Journal of Combinatorial Designs **12** (2004), 71–91.

[43] K. Kurosawa, K. Okada, H. Saido, and D. R. Stinson, *New combinatorial bounds for authentication codes and key predistribution schemes*, Designs, Codes and Cryptography **15** (1998), 87–100.

[44] J. Lee and D. R. Stinson, *A combinatorial approach to key predistribution for distributed sensor networks*, IEEE Wireless Communications and Networking Conference (WCNC 2005) **2** (2005), 1200–1205.

[45] J. Lee and D. R. Stinson, *Deterministic key predistribution schemes for distributed sensor networks. Selected Areas in Cryptography. Lecture*

Notes in Computer Science, vol. 3357, pp. 294–307, Springer-Verlag, Heidelburg, 2005.

[46] J. Lee and D. R. Stinson, *On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs*, Technical Report CACR 2005-40, Centre for Applied Cryptographic Research, University of Waterloo, 2005.

[47] J. Lee and D. R. Stinson, *Tree-based key distribution patterns. Selected Areas in Cryptography. Lecture Notes in Computer Science*, vol. 3897, pp. 189–204, Springer-Verlag, Berlin, 2006.

[48] J. Lee and D. R. Stinson, *On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs*, ACM Transactions on Information and System Security (TISSEC) **11(2)** (2008), Article 5, 1–35.

[49] J. Lee and D. R. Stinson, *Common intersection designs*, Journal of Combinatorial Designs **14(4)** (2009), 251–269.

[50] D. Liu and P. Ning, *Establishing pairwise keys in distributed sensor networks*, Proceedings of 10th ACM Conference on Computer and Communication Security (2003), 52–61.

[51] D. Lubell, *A short proof of Sperner's lemma*, Journal of Combinatorial Theory **1** (1966), 299.

[52] K. M. Martin, *The combinatorics of cryptographic key establishment*, Surveys in Combinatorics 2007, London Mathematical Lecture Notes Series **346** (2007), 223–273.

[53] K. M. Martin, *On the applicability of combinatorial designs to key predistribution for wireless sensor networks. Coding and Cryptology. Lecture Notes in Computer Science*, vol. 5557, pp. 124–145, Springer-Verlag, Berlin, 2009.

[54] K. M. Martin, M. B. Paterson, and D. R. Stinson, *Key predistribution for homogeneous wireless sensor networks with group deployment of nodes*, ACM Transactions on Sensor Networks **7(2)** (2010), Article 11, 1–27.

[55] T. Matsumoto and H. Imai, *On the key predistribution scheme: A practical solution to the key distribution problem. Advances in Cryptology - CRYPTO '87. Lecture Notes in Computer Science*, vol. 293, pp. 185–193, Springer-Verlag, Berlin, 1987.

[56] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of applied cryptography*, CRC-Press, Florida, 1996.

[57] L. D. Meshalkin, *A generalisation of Sperner's theorem on the number of subsets of a finite set (in Russian)*, Teoriya Veroyatnostei i ee Primeneniya **8** (1963), 219–220.

[58] L. D. Meshalkin, *A generalisation of Sperner's theorem on the number of subsets of a finite set (English translation)*, Theory of Probability and its Applications **8** (1964), 204–205.

[59] C. J. Mitchell and F. C. Piper, *The cost of reducing key storage requirements in secure networks*, Computers and Security **6** (1987), 339–341.

[60] C. J. Mitchell and F. C. Piper, *Key storage in secure networks*, Discrete Applied Mathematics **21** (1988), 215–228.

[61] W. B. Moors and J. C. Novak, *Order matters when choosing sets*, Mathematical Inequalities & Applications **14(2)** (2011), 439–444.

[62] C. M. O'Keefe, *Applications of finite geometries to information security*, Australian Journal of Combinatorics **7** (1993), 195–212.

[63] C. M. O'Keefe, *A comparison of key distribution patterns constructed from circle geometries. Advances in Cryptology - AUSCRIPT '92. Lecture Notes in Computer Science*, vol. 718, pp. 517–527, Springer-Verlag, Berlin, 1993.

[64] C. M. O'Keefe, *Key distribution patterns using Minkowski planes*, Designs, Codes and Cryptography **5(3)** (1995), 261–267.

[65] C. Padró, I. Gracia, S. M. Mellevi, and P. Morillo, *Linear key predistribution schemes*, Designs, Codes and Cryptography **25** (2002), 281–298.

[66] R. Palisse, *A short proof of Fisher's inequality*, Discrete Mathematics **111** (1993), 421–422.

[67] E. C. Park and I. F. Blake, *Reducing communication overhead of key distribution schemes for wireless sensor networks*, Proceedings of 16th International Conference on Computer Communications and Networking (2007), 1345–1350.

[68] M. B. Paterson and D. R. Stinson, *A unified approach to combinatorial key predistribution schemes for sensor networks*, Cryptology ePrint Archive: Report 2011/076, 2011.

[69] D. Y. Pei, J. W. Dong, and C. M. Rong, *A novel key predistribution schemes for wireless distributed sensor networks*, Science China Information Sciences **53** (2010), 288–298.

[70] F. C. Piper and S. Murphy, *Cryptography: A very short introduction*, Oxford University Press, Oxford, 2002.

[71] K. A. S. Quinn, *Combinatorial structures with applications to information theory*, Ph.D. thesis, University of London, 1991.

[72] K. A. S. Quinn, *Some constructions for key distribution patterns*, Designs, Codes and Cryptography **4(2)** (1994), 177–191.

[73] K. A. S. Quinn, *Bounds for key distribution patterns*, Journal of Cryptology **12** (1999), 227–239.

[74] G. Rinaldi, *Key distribution patterns using tangent circle structures*, Designs, Codes and Cryptography **31(3)** (2004), 289–300.

[75] K. Römer and F. Mattern, *The design space of wireless sensor networks*, IEEE Wireless Communications Magazine **11(6)** (2004), 54–61.

[76] S. Ruj and B. Roy, *Revisiting key predistribution using transversal design for grid based deployment scheme*, International Journal of Distributed Sensor Networks **5** (2008), 660–674.

[77] S. Ruj and B. Roy, *Key predistribution using combinatorial designs for a grid group deployment scheme in wireless sensor networks*, ACM Transactions on Sensor Networks **6(11)** (2009), Article 4.

[78] M. Ruszinkó, *On the upper bound of the size of the r-cover-free families*, Journal of Combinatorial Theory A **66** (1994), 302–310.

[79] H. J. Ryser, *An extension of a theorem of de Bruijn and Erdös on combinatorial designs*, Journal of Algebra **10** (1968), 246–261.

[80] J. Spencer, *Ten lectures on the probabilistic method*, SIAM: Society for Industrial and Applied Mathematics, Philadelphia, pa, 1987.

[81] E. Sperner, *Ein satz über untermengen einer endlichen lenge*, Mathematische Zeitschrift **27** (1928), 544–548.

[82] D. R. Stinson, *On some methods of unconditionally secure key distribution and broadcast encryption*, Designs, Codes and Cryptography **12(3)** (1997), 215–243.

[83] D. R. Stinson, *Cryptography: Theory and practice*, Chapman & Hall / CRC, Boca Raton, Florida, 3rd edition, 2006.

[84] D. R. Stinson and T. VanTrung, *Some new results on key distribution patterns and broadcast encryption*, Designs, Codes and Cryptography **14** (1998), 261–279.

[85] D. R. Stinson and R. Wei, *Generalised cover free families*, Discrete Mathematics **279** (2004), 463–477.

[86] D. R. Stinson, R. Wei, and L. Zhu, *Some new bounds for cover free families*, Journal of Combinatorial Theory A **90** (2000), 224–234.

[87] K. R. Stromberg, *Introduction to classical real analysis*, Wadsworth International Mathematics Series, Belmont, California, 1981.

[88] R. Wei and J. Wu, *Product construction of key distribution schemes for sensor networks. Selected Areas in Cryptography. Lecture Notes in Computer Science*, vol. 3357, pp. 280–293, Springer-Verlag, Heidelburg, 2004.

[89] L. Xu, J. Chen, and X. Wang, *Cover free family based efficient group key management strategy in wireless sensor networks*, Journal of Communications **3** (2008), 51–58.

[90] K. Yamamoto, *Logarithmic order of free distributive lattices*, Journal of the Mathematical Society of Japan **6** (1954), 343–353.