the information processing system has already been designed, when we come to design the cryptosystem, and we would struggle with the expanded bits. Suppose we implement the cryptosystem on a disc drive system which has 1024 bytes per sector, and we encrypt a plaintext of 1024 bytes on it. In this case, one bit expansion doubles the time for reading/writing a plaintext. Furthermore, if the time for an RSA operation is shorter than the disc read/write time per sector ('fast' RSA hardware makes it possible), the proposed scheme could improve the performance of the disc drive system. This shows that the one bit saving is not always trivial.

We should emphasise that the proposed scheme of Reference 1 is usable in many circumstances.

M. SHIMADA

9th October 1989

Satellite Communications Systems Development Department
Microwave & Satellite Communications Division
NEC Corporation
4035 Ikebe-cho, Midoriku, Yokohama 213, Japan

K. TANAKA

Information Basic Research Laboratory
C&C Information Technology Research Laboratories
NEC Corporation
1-1 Miyazaki 4-chome, Miyamae-ku, Kawasaki, Kanagawa 213, Japan

References

1 SHIMADA, M., and TANAKA, K.: 'Blocking method for RSA cryptosystem without expanding cipher length', *Electron. Lett.*, 1989, **25**, pp. 773–774

2 RIVEST, R. L., SHAMIR, A., and ADLEMAN, L.: 'A method of obtaining digital signatures and public key cryptosystems', *Commun. ACM*, 1978, **21**, pp. 120–126

DISTANCE-INVARIANT ERROR CONTROL CODES FROM COMBINATORIAL DESIGNS

Indexing terms: Codes and coding, Information theory, Error-detection codes

Recently proposed techniques for constructing nonlinear distance-invariant codes from combinatorial designs are generalised. Such codes are of particular interest among nonlinear codes because their decoding error probabilities can be readily calculated.

Introduction: A recent letter[1] described methods of construction for distance-invariant (DI) codes from combinatorial designs. As defined by Delaney and Farrell[1] a code is distance-invariant if the number of codewords at distance i from a codeword (N_i) is independent of the choice of codeword. If a code is DI (and the values of N_i are known) then the probability of undetected errors can easily be computed. This makes DI codes of interest. Note that all linear codes are DI; in a linear code N_i is simply the number of codewords of weight i.

In this letter I give general constructions for DI codes from combinatorial designs which include all the examples of Delaney and Farrell[1] as special cases. For notation and results about designs see Beth *et al.*[2] or Hughes and Piper.[3]

Construction method: Suppose A is the $v \times b$ incidence matrix of a $2-(v, k, \lambda)$ design with b blocks and r blocks incident with every point, where

$$bk = vr \tag{1}$$

and

$$\lambda(v-1) = r(k-1) \tag{2}$$

Then, by definition of design, every row of the incidence matrix contains r ones (and $b-r$ zeros) and every pair of rows has exactly λ ones in the same positions (i.e. the logical AND of the two rows will contain exactly λ ones). Note that we assume that $v > k > 0$ and $\lambda > 0$, and hence $r \neq b/2$.

Following Reference 1, we derive three codes from A:

(1) *Type 1:* Take as codewords the rows of A.

(2) *Type 2:* The codewords of type 1 with their complements.

(3) *Type 3:* The codewords of type 2 with the all-zero and all-one codewords.

If we define an (N, M, d)-code to be one which has M codewords of length N and minimum distance d, then the next result follows immediately from the definition of a 2-design. Note that the main result of Reference 1 corresponds precisely to theorem 1 for the case $v = b$ (and hence $r = k$).

Theorem 1: Type 1 codes have parameters $[b, v, 2(r-\lambda)]$, with equal energy codewords, and are DI with $N_0 = 1$ and $N_{2(r-\lambda)} = v - 1$. Type 2 codes have parameters $\{b, 2v, \min[b-2(r-\lambda), 2(r-\lambda)]\}$, and are DI with $N_0 = 1$, $N_{2(r-\lambda)} = v-1$, $N_{b-2(r-\lambda)} = v-1$ and $N_b = 1$. If $(b-r) = 2(r-\lambda)$ then type 3 codes have parameters $[b, 2v+2, \min(r, b-r)]$, and are DI with $N_0 = 1$, $N_{2(r-\lambda)} = v$, $N_{b-2(r-\lambda)} = v$ and $N_b = 1$.

In fact, when the condition for type 3 codes (namely that $(b-r) = 2(r-\lambda)$) is combined with eqns. 1 and 2, it simplifies to either $k = v$ (a trivial case) or $k = (v-1)/2$. In the square ($v = k$) case this means that the set of nontrivial designs satisfying the type 3 condition is precisely the well known family of Hadamard designs. Delaney and Farrell[1] pointed out that the Hadamard designs satisfy the type 3 code conditions, but they do not note the converse. In fact, the type 3 codes obtained from the Hadamard designs correspond precisely to the Hadamard codes B_n described on p. 49 of Reference 4.

Further generalisations:

(*a*) A 't-class association scheme' is defined as a set V of v elements and a mapping f from the 2-subsets of V into $\{1, 2, \ldots, t\}$ with the following properties:

(i) There exist constants $v_1, v_2, \ldots, v_t$ such that, for any element P of V, there are precisely v_i other elements Q of V such that $f(\{P, Q\}) = i$ (and hence $v_1 + v_2 + \ldots + v_t = v - 1$).

(ii) There exist constants w_{ijk}, such that if P and Q are any elements of V satisfying $f(\{P, Q\}) = k$ then the number of other elements R in V satisfying $f(\{P, R\}) = i$ and $f(\{Q, R\}) = j$ is w_{ijk}.

Note that if $f(\{P, Q\}) = i$, then we say that P and Q are ith associates.

Observe that 2-class association schemes correspond precisely to strongly regular graphs.

(*b*) A 'partially balanced design with t associate classes' [PBD(t)] is then a $1-(v, k, r)$ design with a t-class association scheme defined on its v points, such that if any two points are ith associates they are commonly incident with $\lambda(i)$ blocks, for some constant $\lambda(i)$. In incidence matrix terms this means that, if A is the $v \times b$ incidence matrix of a PBD(t), then if two rows correspond to points which are ith associates, then these two rows have $\lambda(i)$ positions in which they both contain a one. Note that many examples of PBD(t) designs are known to exist.

If we derive type 1, type 2 and type 3 codes from A as we did previously (and we assume that each point has v_i ith associates) then we obtain the following.

Theorem 2: Type 1 codes have parameters $\langle b, v, \min_i\{2[r-\lambda(i)]\}\rangle$, with equal energy codewords, and are DI with $N_0 = 1$ and $N_{2[r-\lambda(i)]} = v_i$. Type 2 codes have parameters $\langle b, 2v, \min_i\{b-2[r-\lambda(i)], 2[r-\lambda(i)]\}\rangle$, and are DI with $N_0 = 1$, $N_{2[r-\lambda(i)]} = v_i$, $N_{b-2[r-\lambda(i)]} = v_i$ and $N_b = 1$. If $(b-r) = 2[r-\lambda(j)]$ for some j, then type 3 codes have parameters $\langle b, 2v+2, \min_i\{b-2[r-\lambda(i)], 2[r-\lambda(i)]\}\rangle$, and are DI with $N_0 = 1$, $N_{2[r-\lambda(i)]} = v_i$ $(i \neq j)$, $N_{2[r-\lambda(j)]} = v_j + 1$, $N_{b-2[r-\lambda(i)]} = v_i$ $(i \neq j)$, $N_{b-2[r-\lambda(j)]} = v_j + 1$ and $N_b = 1$.

We now show how the type 1 codes of theorem 2 generalise the remaining examples given by Delaney and Farrell.[1] First consider the trivial $k-(v, k, 1)$ design obtained by taking as blocks all the k-subsets of the v points (and hence $b = {}_vC_k$, the binomial coefficient). Then the dual of this design (obtained by reversing the roles of points and blocks) is a PBD(k) with $\lambda(i) = k - i$ and $v_i = {}_kC_{k-i} \cdot {}_{v-k}C_i$; we define two blocks as being ith associates if they have $k - i$ points in common. It should now be clear that the DI code of Delaney and Farrell[1] is simply the type 1 code obtained from this 'trivial' design.

Conclusion: I have shown how the DI codes of Delaney and Farrell[1] may be obtained from more general constructions. Many other DI codes may be obtained from combinatorial designs; the interested reader is referred to Cameron and van Lint.[5]

C. J. MITCHELL *17th August 1989*

Hewlett-Packard Laboratories
Filton Road, Stoke Gifford, Bristol BS12 6QZ, United Kingdom

References

1 DELANEY, F. A., and FARRELL, P. G.: 'Calculation of error probabilities for distance-invariant nonlinear error control codes', *Electron. Lett.*, 1989, **25**, pp. 497–498
2 BETH, T., JUNGNICKEL, D., and LENZ, H.: 'Design theory' (Bibliographisches Institut, Mannheim, 1985)
3 HUGHES, D. R., and PIPER, F. C.: 'Design theory' (Cambridge University Press, 1985)
4 MACWILLIAMS, F. J., and SLOANE, N. J. A.: 'The theory of error-correcting codes' (North Holland, 1977)
5 CAMERON, P. J., and VAN LINT, J. H.: 'Graphs, codes and designs' (LMS Lecture Note Series **43**, Cambridge University Press, 1980)

SUBMICRON AlGaAs/GaAs HETEROSTRUCTURE BIPOLAR TRANSISTOR WITH HIGH GAIN

Indexing terms: Semiconductor devices and materials, Bipolar devices, Transistors, Epitaxy

We describe the realisation of self-aligned AlGaAs/GaAs heterostructure bipolar transistors with submicron emitter stripe width, current gain of 120 and a maximum operating current density greater than $10^5\,A\,cm^{-2}$. The high current gain was achieved by passivating the extrinsic base region with thin AlGaAs.

In recent years there has been interest in using AlGaAs/GaAs heterostructure bipolar transistors (HBTs) for high-speed electronics applications.[1,2] Because integrated circuits require large numbers of transistors with low power consumption, it is important to scale down lateral device dimensions, thereby minimising the total current (power) associated with device operation. However, scaling emitter stripe widths below 1 μm significantly degrades current gain due to efficient minority carrier recombination.[3,4] It has been reported that proper surface passivation significantly reduces excess base current due to surface recombination in the extrinsic base region. This results in transistors with high current gain.[5,6] However, these workers did not address device scaling. In this letter we report fabrication of self-aligned submicron AlGaAs/GaAs HBTs with high current gain and ideal lateral scaling.

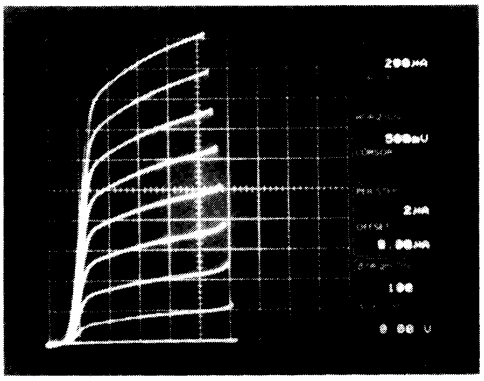
Fig. 1 shows the device layer structure which was grown by molecular beam epitaxy (MBE) on a ⟨100⟩-oriented semi-insulating GaAs substrate. First a 10000 Å-thick n-type ($1 \times 10^{19}\,cm^{-3}$ Si impurity) GaAs subcollector was grown at a temperature of 580°C, followed by a 1000 Å-thick $n = 5 \times 10^{16}\,cm^{-3}$ GaAs collector region. The base consists of a 700 Å-thick p-type ($2 \times 10^{10}\,cm^{-3}$ Be impurity) GaAs layer with a 100 Å-thick emitter/base doping setback layer. A heavily doped ($n = 1 \times 10^{18}\,cm^{-3}$) $Al_{0.35}Ga_{0.65}As$ emitter was used. A 3100 Å-thick $GaAs/Ga_{0.85}In_{0.15}As$ contact layer was necessary to facilitate a low-resistance self-aligned ohmic contact. After removal from the growth chamber the material was processed into transistor structures.

100 Å	$Ga_{0.85}In_{0.15}As$	$n > 10^{19}\,cm^{-3}$	emitter cap
3000 Å	GaAs	$n > 10^{19}\,cm^{-3}$	
500 Å	$Al_xGa_{1-x}As$	$n = 2 \times 10^{18}\,cm^{-3}$	graded, $0 < x < 0.35$
500 Å	$Al_xGa_{1-x}As$	$n = 1 \times 10^{18}\,cm^{-3}$	$x = 0.35$
100 Å	GaAs	undoped	setback
700 Å	GaAs	$p = 2 \times 10^{19}\,cm^{-3}$	base
1000 Å	GaAs	$n = 5 \times 10^{16}\,cm^{-3}$	collector
10000 Å	GaAs	$n = 1 \times 10^{19}\,cm^{-3}$	subcollector
	GaAs semi-insulating substrate		

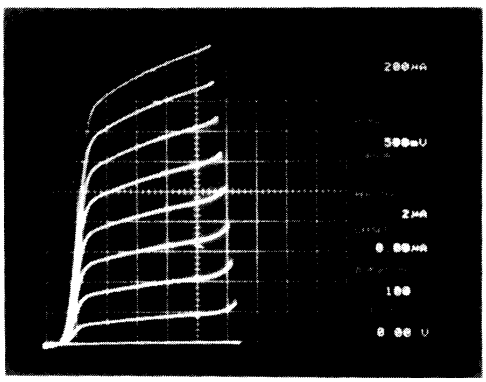
8291

Fig. 1 *Schematic diagram of epilayer structure of HBT*

Using standard contact photolithography, 1 μm-thick NiGeAu emitter strips were defined by evaporation and liftoff. Following a 10 s anneal at 400°C to alloy the emitter contact, the emitter mesa was defined using an $H_2O_2 : NH_4OH$ (pH adjusted to 7·05) spray etch. The selective etch stops 500 Å short of the base. Approximately 350 Å of AlGaAs is then removed using an $H_3PO_4 : H_2O_2 : H_2O$ (10 : 2 : 100) solution. The removal of the AlGaAs was monitored by the photocurrent between two emitter stripes. Self-aligned base contact was achieved with AuBe using the overhang of the emitter ohmic contact as a shadow mask. This resulted in a 0·4 μm base to emitter electrode spacing. The heterostructure was then annealed to facilitate the diffusion of the beryllium



a 8292



b 8292

Fig. 2
a Common-emitter current gain for device with emitter dimension $4 \times 4\,\mu m^2$
b Common-emitter current gain for device with emitter dimension $0.9 \times 11\,\mu m^2$