TABLE I
$\langle 1 \rangle < S_2 < S_3 < S_4 < S_5 < S_6 < G_6$

Channel	Message Words	Minimum Distance Squared			
		$F = 1.1$	$F = 2$	$F = 10$	Single Receiver
1	46080	0.0225	0.0186	0.0080	0.0252
2	23040	0.0247	0.0213	0.0127	0.0424
3	7680	0.0252	0.0244	0.0201	0.0785
4	1920	0.0257	0.0281	0.0319	0.1634
5	384	0.0262	0.0323	0.0505	0.3694
6	64	0.0267	0.0371	0.0800	0.6667

TABLE II
$\langle 1 \rangle < G_1 < G_2 < G_3 < G_4 < G_5 < G_6$

Channel	Message Words	Minimum Distance Squared			
		$f = 1.1$	$F = 2$	$F = 10$	Single Receiver
1	46080	0.0243	0.0187	0.0084	0.0252
2	23040	0.0247	0.0215	0.0133	0.0370
3	5760	0.0252	0.0247	0.0211	0.0690
4	960	0.0257	0.0283	0.0334	0.1429
5	120	0.0262	0.0325	0.0529	0.4000
6	12	0.0267	0.0374	0.0838	2.0000

We list below achievable minimum distances and number of message words for certain ratios of minimum distance. The value F is the ratio of the square of the minimum distance of the first channel to that of the last. The minimum distance squared is also given for the optimal single receiver code with the given number of message words which may be generated by G_6. Each of these is an upper bound for the minimum distance squared for the corresponding channel.

References

[1] P. P. Bergmans, "A simple converse for broadcast channels with additive white Gaussian noise," *IEEE Trans. Inform. Theory*, vol. IT-20, no. 2, Mar. 1974.

[2] C. Downey and J. Karlof, "Group codes for the Gaussian broadcast channel with two receivers," *IEEE Trans. Inform. Theory*, vol. IT-26, no. 4, July 1980.

[3] ——, "On the existence of $[M, n]$ group codes for the Gaussian channel with M and n odd," *IEEE Trans. Inform. Theory*, vol. IT-23, no. 4, July 1977.

[4] T. M. Cover, "Broadcast channels," *IEEE Trans. Inform. Theory*, vol. IT-18, no. 1, Jan. 1974.

[5] C. Heegard, H. dePedro, and J. Wolf, "Permutation codes for the Gaussian broadcast channel with two receivers," *IEEE Trans. Inform. Theory*, vol. IT-24, no. 5, Sept. 1978.

[6] D. Slepian, "Permutation modulation," in *Proc. IEEE*, vol. 53, Mar. 1965.

Ternary Sequences with Perfect Periodic Autocorrelation

TOM HØHOLDT AND JØRN JUSTESEN

***Abstract*—We construct $0, \pm 1$ sequences of length $(q^{2l+1} - 1)/(q - 1)$, where $q = 2^s$, with out-of-phase periodic autocorrelation 0, and in-phase correlation q^{2l}; such that the peak factor of radiation is $(q^{2l+1} - 1)/(q^{2l+1} - q^{2l})$, which is close to 1 as q becomes large.**

Manuscript received October 30, 1981; revised March 11, 1982. This paper was partially presented at the IEEE International Symposium on Information Theory, Les Arcs, France, June 21–25, 1982.

Tom Høholdt is with Department of Mathematics, The Technical University of Denmark, Building 303, Dk-2800 Lyngby, Denmark.

Jørn Justesen is with Department of Circuit Theory and Telecommunication, The Technical University of Denmark, Building 343, DK-2800 Lyngby, Denmark.

I. Introduction

In several applications, including estimation of impulse-responses and detection of reflected waves, it is important to have periodic sequences $\{x_i\}$ of period N, with periodic autocorrelation function

$$\sum_{i=1}^{N} x_i x_{i+k} = \begin{cases} M, & \text{if } k \equiv 0 \pmod N; \\ 0, & \text{if } k \not\equiv 0 \pmod N. \end{cases}$$

We shall say that such sequences have perfect autocorrelation. Further it is desirable that the peak factor N/M be as large as possible when the amplitudes are restricted to $|x_i| \leqslant 1$. It is well-known that binary maximum length shift register sequences which have $|x_i| = 1$ achieve a small out-of-phase correlation, but that it is not exactly 0. However, by allowing $x_i \in \{0, 1, -1\}$, it is possible to obtain sequences with perfect autocorrelation and a large peak factor.

A large class of such ternary sequences was constructed by Ipatov [1], [2] using shift register sequences over $GF(q^r)$ for q odd. These sequences have length $(q^{2l+1} - 1)/(q - 1)$, but the construction depends heavily on the fact that q is odd. Moharir [3] has given necessary conditions for the existence of perfect ternary sequences and has observed that a construction based on difference sets is sometimes possible. Shedd and Sarwate [4] have constructed perfect ternary sequences of length $2^n - 1$, based on earlier work of Kasami, Gold, and Helleseth [5], using cross correlation of binary maximum length sequences. Sarwate and Pursley [6] have written an excellent survey on the subject.

In this correspondence we combine ideas of [3] and [4] and use some facts on quadrics in $PG(2l, 2^s)$, the projective geometry of dimension $2l$ over $GF(2^s)$, to construct perfect ternary sequences of length

$$\frac{(2^s)^{2l+1} - 1}{2^s - 1}, \qquad \text{with peak factor } \frac{(2^s)^{2l+1} - 1}{(2^s)^{2l+1} - (2^s)^{2l}}.$$

The details of our construction are more difficult than those of [1], but the sequences may be generated more simply. The calculation of the correlation between a received signal and the ternary sequence is also facilitated by the use of a binary ground field.

In Section II we present the construction of ternary sequences with perfect autocorrelation. The proofs of certain properties of projective geometries over $GF(2^s)$ are postponed to Section III. In Section IV we present examples of the most important sequences and details of their construction.

II. The Construction

For basic facts on difference sets, the reader is referred to [7]. Let $D = \{i_1, i_2, \cdots, i_k\}$ be a Singer difference set with parameters

$$v = \frac{q^{2l+1} - 1}{q - 1}, \quad k = \frac{q^{2l} - 1}{q - 1}, \quad \lambda = \frac{q^{2l-1} - 1}{q - 1},$$

where q is a prime power. Let x_D denote the characteristic vector of D, that is

$$x_D = (x_1, x_2, \cdots, x_v), \quad x_i = \begin{cases} 1, & i \in D; \\ 0, & i \notin D. \end{cases}$$

It is well-known that the periodic autocorrelation

$$R(j) = \sum_{i=1}^{v} x_{i+j} x_i$$

satisfies

$$R(j) = \begin{cases} k, & j \equiv 0 \pmod v; \\ \lambda, & j \not\equiv 0 \pmod v. \end{cases} \tag{1}$$

Let $\hat{D}$ denote another Singer difference-set, with the same parameters as D, and let θ denote the sequence obtained by cross correlation of x_D and $x_{\hat{D}}$. The periodic autocorrelation of θ is then ([4])

$$R_\theta(j) = \begin{cases} k^2 + (v-1)\lambda^2, & j \equiv 0 \pmod v; \\ 2k\lambda + (v-2)\lambda^2, & j \not\equiv 0 \pmod v. \end{cases} \tag{2}$$

The fact that makes our construction work is the following theorem.

Theorem 1: Let D be a Singer difference set with parameters

$$v = \frac{q^{2l+1}-1}{q-1}, \quad k = \frac{q^{2l}-1}{q-1}, \quad \lambda = \frac{q^{2l-1}-1}{q-1}, \quad q = 2^s,$$

then there exists another Singer difference set $\hat{D}$ with the same parameters, such that if θ denotes the sequence obtained by cross correlating the characteristic vectors x_D and $x_{\hat{D}}$ of D and $\hat{D}$, θ takes on only three values, namely,

$$\begin{aligned} &\frac{(q^l+1)(q^{l-1}-1)}{q-1} && \text{which appears} && \frac{q^l(q^l-1)}{2} && \text{times,} \\ &\frac{q^{2l-1}-1}{q-1} && \text{which appears} && \frac{q^{2l}-1}{q-1} && \text{times,} \\ &\frac{(q^l-1)(q^{l-1}+1)}{q-1} && \text{which appears} && \frac{q^l(q^l+1)}{2} && \text{times.} \end{aligned} \tag{3}$$

The proof of this theorem is given in Section III. Since

$$\frac{(q^l+1)(q^{l-1}-1)}{q-1} = \frac{q^{2l-1}-1}{q-1} - q^{l-1}$$

and

$$\frac{(q^l-1)(q^{l-1}+1)}{q-1} = \frac{q^{2l-1}-1}{q-1} + q^{l-1},$$

we obtain, by subtracting $(q^{2l-1}-1)/(q-1)$ from each element of θ, and then dividing all the elements by q^{l-1}, a sequence $\hat{\theta}$ with elements 0 and ± 1.

Moreover the periodic autocorrelation of $\hat{\theta}$ is

$$R_{\hat{\theta}}(j) = \begin{cases} q^{2l}, & j \equiv 0 \pmod v; \\ 0, & j \not\equiv 0 \pmod v. \end{cases} \tag{4}$$

This follows from

$$R_{\hat{\theta}}(j) = \frac{R_\theta(j) + a^2 v - 2a(A(a-x) + Ba + C(a+x))}{x^2},$$

where

$$a = \frac{q^{2l-1}-1}{q-1}, \quad x = q^{l-1},$$

$$A = \frac{q^l(q^l-1)}{2}, \quad B = \frac{q^{2l}-1}{q-1}, \quad C = \frac{q^l(q^l+1)}{2}$$

and a straightforward calculation.

Theorem 1 contains an existence statement, but the proof is by construction of the desired $\hat{D}$. Some examples are given in Section IV.

III. Proof of Theorem 1

The proof of Theorem 1 consists of two parts, which are formulated as follows.

Theorem 2: Let $D = \{i_1, i_2, \cdots, i_k\}$ be a Singer difference set with parameters

$$v = \frac{q^{2l+1}-1}{q-1}, \quad k = \frac{q^{2l-1}}{q-1}, \quad \lambda = \frac{q^{2l-1}-1}{q-1}, \quad q = 2^s,$$

then there exists $r \in \{1, 2, \cdots, v\}$ such that if we construct (the hyperplanes of) $\mathrm{PG}(2l, q)$ by cyclic shifts of D, the points corresponding to rD constitute a nondegenerate quadric in $\mathrm{PG}(2l, q)$.

Theorem 3: Let Q be a nondegenerate quadric of $\mathrm{PG}(2l, q)$, $q = 2^s$. The hyperplanes of $\mathrm{PG}(2l, q)$ is then divided into 3 classes; namely $q^l(q^l-1)/2$ which have $(q^l+1)(q^{l-1}-1)/(q-1)$ points in common with Q, $(q^{2l}-1)/(q-1)$ which have $(q^{2l-1}-1)/(q-1)$ points in common with Q, $q^l(q^l+1)/2$ which have $(q^l-1)(q^{l-1}+1)/(q-1)$ points in common with Q.

Proof of Theorem 3: let Q be a nondegenerate quadric of $\mathrm{PG}(2l, q)$ $q = 2^s$. Following Dickson [8], we can choose coordinates such that Q has the equation $x_0^2 + x_1x_2 + \cdots + x_{2l-1}x_{2l} = 0$, and the equation of a hyperplane is

$$a_0x_0 + a_1x_1 + \cdots + a_{2l}x_{2l} = 0, \qquad a_i \in \mathrm{GF}(q),\ a \neq 0.$$

Now we consider two cases.

Case 1: $a_0 = 0$, of course there are $(q^{2l}-1)/(q-1)$ of these. We can without loss of generality assume that the hyperplane is $x_1 = a_2x_2 + \cdots + a_{2l}x_{2l}$. Now if $l = 1$ we shall find the number of common points of $x_0^2 + x_1x_2 = 0$ and $x_1 = ax_2$ and it is easy to see that only $(\sqrt{a}, a, 1)$ satisfies both equations. If $l > 1$ we shall count the number of points in the set

$$\{(x_0, x_1, \cdots, x_{2l}) | x_1 = a_2x_2 + \cdots + a_{2l}x_l \text{ and } x_0^2 + (a_2x_2 + \cdots + a_{2l}x_{2l})x_2 + \cdots + x_{2l-1}x_{2l} = 0\},$$

but for each point on the hyperplane $x_1 = a_2x_2 + \cdots + a_{2l}x_{2l}$ the last equation has exactly one solution x_0, so the number of points in the set is $(q^{2l-1}-1)/(q-1)$.

Case 2: $a_0 \neq 0$. We can assume that the hyperplane has the equation $x_0 = a_1x_1 + \cdots + a_{2l}x_{2l}$ so we shall count the number of points in the set

$$\{(x_0, x_1, \cdots, x_{2l}) | x_0 = a_1x_1 + \cdots + a_{2l}x_{2l} \text{ and } (a_1x_1 + \cdots + a_{2l}x_{2l})^2 + x_1x_2 + \cdots + x_{2l-1}x_{2l} = 0\}.$$

Here the last equation is the equation of a nondegerate quadric $\tilde{Q}$ in $\mathrm{PG}(2l-1, q)$ and obviously the number of points in the set is equal to the number of points on $\tilde{Q}$. Now in the odd-dimensional projective space there are two kinds of quadrics, namely, the elliptic ones which contain $((q^l+1)(q^{l-1}-1))/(q-1)$ points and hyperbolic ones which contain $(q^l-1)(q^{l-1}+1)/(q-1)$ points. These numbers are due to Primrose [9].

To finish the proof of the theorem we only need to count the number of elliptic (or hyperbolic) quadrics of the form

$$b_1x_1^2 + \cdots + b_{2l}x_{2l}^2 + x_1x_2 + \cdots + x_{2l-1}x_{2l} = 0.$$

If $l = 1$ this is $b_1x_1^2 + b_2x_2^2 + x_1x_2 = 0$, which has a solution for $q(q+1)/2$ choices of (b_1, b_2), this follows for instance from [10,

pp. 243–244]. If $l > 1$ the quadric is given by

$$(x_1 x_3 \cdots x_{2l-1}) \begin{pmatrix} b_1 & & & 0 \\ & b_3 & & \\ & & \ddots & \\ 0 & & & b_{2l} \end{pmatrix} \begin{pmatrix} x_1 \\ x_3 \\ \vdots \\ x_{2l-1} \end{pmatrix}$$

$$+ (x_2 x_4 \cdots x_{2l}) \begin{pmatrix} b_2 & & & 0 \\ & b_4 & & \\ & & \ddots & \\ 0 & & & b_{2l} \end{pmatrix} \begin{pmatrix} x_2 \\ x_4 \\ \vdots \\ x_{2l} \end{pmatrix}$$

$$+ (x_1 x_3 \cdots x_{2l-1}) \begin{pmatrix} x_2 \\ x_4 \\ \vdots \\ x_{2l} \end{pmatrix} = 0$$

so there is a one-to-one correspondence between these quadrics in $PG(2l-1, q)$ and the quadric $\gamma_1 z_1^2 + \gamma_2 z_2^2 + z_1 z_2$ in $PG(1, q^l)$, so by the above result the number of hyperbolic quadrics is $q^l(q^l+1)/2$. This completes the proof of Theorem 3. □

Proof of the Theorem 2: The Singer difference set D can be described by chosing a primitive element α of $GF(q^{2l+1})$ and a fixed linear mapping $L: GF(q^{2l+1}) \to GF(q)$, then $D = \{i \mid L(\alpha^i) = 0,\ i \in \{0, 1, \cdots, v-1\}\}$.

Now define $f(x, y)$: $[GF(q^{2l+1})]^2 \to GF(q)$ by $f(x, y) = L(x^a y^b)$, where a and b are chosen such that

$$\begin{aligned} &a \equiv (2^s)^m \pmod{q^{2l+1} - 1}, \\ &b \equiv (2^s)^n \pmod{q^{2l+1} - 1}, \qquad \text{for some } m \text{ and } n, \\ &a \neq b, \end{aligned} \tag{5}$$

and such that

$$r = (a+b)^{-1} \text{ is not congruent to a power of 2} \pmod{v}. \tag{6}$$

Then it is easy to see that the mapping $f(x, y)$ is bilinear and that $\{x \mid f(x, x) = 0\}$ constitutes a nondegenerate quadric in $PG(2l, q)$ consisting of the points corresponding to rD.

The bilinearity is ensured by (5) and that the quadric is nondegenerate is ensured by (6) since r by definition then is a nonmultiplier [7, p. 118].

Moreover it is a straightforward matter to verify that there indeed are choices of a and b which satisfy (5) and (6). This completes the proof of Theorem 2. □

Theorem 1 is now easily obtained. The Singer difference set D can be arbitrary, and we can then, according to Theorem 2 find a number r such that $\hat{D} = rD$ is a quadric of $PG(2l, q)$. Using Theorem 3 we then see that the sequence θ, obtained by cross correlating the sequences corresponding to D and $\hat{D}$, has the properties claimed in the theorem.

IV. Examples

If $s = 1$, that is $q = 2$, our construction gives sequences of length $2^{2l+1} - 1$. It is worth noting that the construction here coincides with that of [4], and that the choices of D and rD, corresponds to choosing words of the first and second order Reed–Muller codes, respectively.

The first interesting new sequences are obtained by setting $l = 1$. We will now construct two examples in detail for this special case.

When $l = 1$ we are considering lines and quadrics in a projective *plane* over $GF(2^s)$; in this case, it is easy to see [7] that as the nonmultiplier r of the construction we can choose $r = -1$, so that the quadric corresponds to $-D$, where D is the difference set that gives the lines of the geometry. More specificly if $s = 2$, we can as D use the $(21, 5, 1)$-Singer difference set $\{3, 6, 7, 12, 14\}$, $-D$ is then $\{7, 9, 14, 15, 18\}$.

The description is faciliated by introducing the cyclotomic classes (mod 21) that is $C(j) = \{j \cdot 2^i \pmod{21},\ i = 0, 1, \cdots\}$ and it is seen that $D = C(3) \cup C(7)$ and $-D = C(7) \cup C(9)$.

If we crosscorrelate the sequences corresponding to D and $-D$, it can be seen that $|D + t \cap (-D)|$ is constant when t belongs to a given cyclotomic class. Moreover $|D + t \cap (-D)| = 1$ if $t \in -D$, so since $C(0)$ has size 1, $C(3)$ has size 3 and only $C(1)$ and $C(5)$ have size 6, and since we know that the cross correlation takes on the value 0 six times,the value 1 five times, and the value 2 ten times, it is an easy matter to decide whether $C(1)$ or $C(5)$ corresponds to the value 2. One gets

$$\begin{aligned} &|D + t \cap (-D)| = 0, \\ &\quad \text{if } t \in C(5) = \{5, 10, 13, 17, 19, 20\} \\ &|D + t \cap (-D)| = 1, \\ &\quad \text{if } t \in C(7) \cup C(9) = \{7, 9, 14, 15, 18\} \\ &|D + t \cap (-D)| = 2, \\ &\quad \text{if } t \in C(0) \cup C(1) \cup C(3) = \{0, 1, 2, 3, 4, 6, 8, 11, 12, 16\} \end{aligned}$$

so the perfect ternary sequence is

$$+ + + + + - + 0 + 0 - + + - 00 + - 0 - - .$$

If $s = 3$ we can, as D, use $\{9, 18, 36, 41, 57, 65, 69, 71, 72\}$, and $-D$ becomes $\{1, 2, 4, 8, 16, 32, 37, 55, 64\}$.

In this case all the cyclotomic classes except $C(0)$ have size 9, and again we have $|D + t \cap (-D)| = 1$ if $t \in -D$. Since the cross correlation will have the value 0 in 28 cases then for $t = 0$: $|D + t \cap (-D)| = 0$, which is also immediately seen from above.

What remains is to find the three cyclotomic classes, where the cross correlation is 0. One finds that this is the case for $C(11)$, $C(25)$, $C(13)$, so we get

$$|D + t \cap (-D)| = 0, \qquad \text{for } t = 0,\ 11,\ 22,\ 44,\ 15,\ 30,\ 60,\ 47,\ 21,\ 42,\ 25,\ 50,\ 27,\ 54,\ 35,\ 70,\ 67,\ 61,\ 49,\ 13,\ 26,\ 52,\ 31,\ 62,\ 51,\ 29,\ 58,\ 43,$$

and

$$|D + t \cap (-D)| = 1, \qquad \text{for } t = 1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 37,\ 55,\ 64.$$

The perfect ternary sequence is therefore

$$\begin{aligned} &-00+0+\ ++0+\ +-+-+-0+\ +++--++--- \\ &+---0+\ +-+0+\ +++--+++-+----+ \\ &-0+\ +-+---+0+\ +-++-++. \end{aligned}$$

As a concluding remark, we mention that the correlation of a received signal with the ternary sequences we have constructed can be obtained by correlating the received signal with the binary sequences given by D and $\hat{D}$, subtracting them, and then scaling the result.

References

[1] V. P. Ipatov, "Ternary sequences with ideal autocorrelation properties," *Radio Eng. Electron. Phys.*, vol. 24, pp. 75–79, Oct. 1979.

[2] ——, "Contribution to the theory of sequences with perfect periodic autocorrelation properties," *Radio Eng. Electron. Phys.*, vol. 25, pp. 31–34, Apr. 1980.

[3] P. S. Moharir, "Generalized PN sequences," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 782–784, Nov. 1977.

[4] D. A. Shedd and D. V. Sarwate, "Construction of sequences with good correlation properties," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 94–97, Jan. 1979.

[5] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, pp. 209–232, Nov. 1976.
[6] D. V. Sarwate and M. B. Pursley, "Cross correlation properties of pseudo-random and related sequences," *IEEE Proc.*, vol. 68, pp. 593–619, May 1980.
[7] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics 1982. Berlin: Springer, 1971.
[8] L. E. Dickson, *Linear Groups*. New York: Dover, 1958.
[9] E. J. F. Primrose, "Quadrics in finite geometries," in *Proc. Camb. Phil. Soc.*, vol. 47, pp. 299–304, Mar. 1951.
[10] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw Hill, 1968.

On the Characterization of PN Sequences

UNJENG CHENG, MEMBER, IEEE, AND SOLOMON W. GOLOMB, FELLOW, IEEE

***Abstract*—Balanced binary sequences of period $2^n - 1$ with the run property and the two-level autocorrelation property are not necessarily PN sequences.**

In [1] a hierarchy of classes of binary sequences of period $2^n - 1$ was presented, and several conjectures about the intersections of these classes were offered. The hierarchy is summarized in Fig. 1, where U is the class of all binary sequences of period $2^n - 1$, and PN is the class of maximum-length shift register sequences of period $2^n - 1$. The intermediate classes are R (the "run property"), M (the "multiplier property," referring to sequences which are constant on cyclotomic cosets), S (the span-n property), and C (the two-level correlation property). For detailed definitions, see [1].

The possibility that $R \cap M = \text{PN}$ is belied by numerous counter-examples, first occurring at $n = 5$. A small class of counter-examples to $S \cap M = \text{PN}$ is described in [1], with the first instance at $n = 7$.

It was conjectured in [1] (the "strong conjecture") that $R \cap C = \text{PN}$. A counter-example has been found with $n = 7$, i.e., with period 127. For this period Baumert [2] determined six types of two-level correlation sequences which he designated by the letters A, B, C, D, E, F. A member of type E, not listed explicitly in [2] (it is a decimation of the example presented there), provides the first counter-example to $R \cap C = \text{PN}$. Explicitly, the sequence is

11111011110011111110010010111010101111000110000
10011011100110001101101110100100011010000101010 0
11010010100011101100000101000000.

In [3, ch. 3], it is shown that all PN sequences have the three "randomness properties" U, R, and C (designated in [3] as the properties $R - 1$, $R - 2$, and $R - 3$, respectively), and the impression is given that any sequence with these three properties must be a PN sequence. The counter-example above shows that this is not the case.

A complete search of the cases $n \leqslant 8$, and partial searches for $n \geqslant 9$, have thus far failed to uncover any counter-examples to the "weak conjecture" $S \cap C = \text{PN}$. On the other hand, no proof of this conjecture has as yet been discovered.

Manuscript received November 8, 1982. This work was supported in part by the Army Research Office under Grant DAAG29-79-C-0054, and in part under Grant DAAG29-82-K-0142.

The authors are with the Department of Electrical Engineering, Powell Hall of Engineering, University of Southern California, Los Angeles, CA 90089-0272.

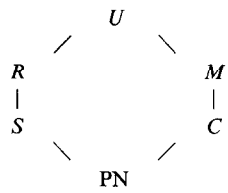

Fig. 1. Hierarchy of classes of binary sequences of period $2^n - 1$.

REFERENCES

[1] S. W. Golomb, "On the classification of balanced binary sequences of period $2^n - 1$," *IEEE Trans. Inform. Theory*, vol. IT-26, no. 6, pp. 730–732, Nov. 1980.
[2] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics. New York: Springer-Verlag, 1971.
[3] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA: Holden-Day, 1967; Revised edition. Laguna Hills, CA: Aegean Park, 1982.

A Low-Rate Bound for Asymmetric Error-Correcting Codes

J. MARTIN BORDEN, MEMBER, IEEE

***Abstract*—We prove a Plotkin-type bound for binary codes which correct asymmetric errors. This bound shows that it is possible to correct as many as 1 / 3 asymmetric errors per code symbol, and no more. The result is obtained by estimating the solution of a linear program.**

I. INTRODUCTION

Binary codes designed to correct asymmetric errors (of type $1 \rightarrow 0$ exclusively) which occur on the Z channel have been studied by a number of researchers. The asymmetric-error-correcting ability of such an "asymmetric code" is determined by its asymmetric distance d_a. This is the minimum value of the asymmetric distance $d_a(\boldsymbol{x}_i, \boldsymbol{x}_j)$ taken over all pairs of distinct codewords $\boldsymbol{x}_i$ and $\boldsymbol{x}_j$, where

$$d_a(\boldsymbol{x}_i, \boldsymbol{x}_j) = 1/2\{d_H(\boldsymbol{x}_i, \boldsymbol{x}_j) + |w(\boldsymbol{x}_i) - w(\boldsymbol{x}_j)|\}, \quad (1)$$

d_H is the familiar Hamming distance and w is the weight function. It is well-known and relatively easy to prove using the combinatorial significance of d_a that a code can correct e asymmetric errors if and only if $d_a \geqslant e + 1$ [2].

In this correspondence we prove the following low-rate bound.

Theorem: The parameters of a length n code containing M codewords and having asymmetric distance d_a satisfy $M \leqslant 4d_a/(3d_a - n)$ (provided $n < 3d_a$), or equivalently, $d_a/n \leqslant M/(3M - 4)$. On the other hand, for all values of M, there exists a code whose parameters satisfy $d_a/n \geqslant 1/3$.

It is interesting to make comparisons between bounds for asymmetric coding and bounds for the familiar "symmetric coding" (where errors of both types $1 \rightarrow 0$ and $0 \rightarrow 1$ occur). The well-known Plotkin bound shows that $d_H/n \leqslant M/(2M - 2)$; also, there are codes with arbitrarily large M such that $d_H/n \geqslant 1/2$ [9]. Thus there are arbitrarily large codes which can correct $1/3$ asymmetric errors per code letter, whereas the corresponding fraction for symmetric codes is only $1/4$ (since d_H is roughly twice the number of correctable symmetric errors).

Manuscript received May 26, 1982; September 23, 1982.

The author is with the Worcester Polytechnic Institute, Department of Mathematical Sciences, Worcester, MA 01609.

0018-9448/83/0700-0600$01.00 ©1983 IEEE