propriate choice of λ) is

$$F(\rho) = \rho, \tag{17}$$

and for $S_N(2\Delta') < 1$, $E_s/N_0 \gg 1$:

$$F(\rho) = 1. \tag{18}$$

Similarly, from (16), for $E_s/N_0 \ll 1$ and arbitrary $S_N(2\Delta')$,

$$F(\rho) = \rho^m. \tag{19}$$

The primary advantage of using these monomial approximations of F is that no measurement of E_s/N_0 is necessary.

For $E_s/N_0 \gg 1$, the optimal nonlinearity is dependent on the frequency offset (see (17) and (18)), whereas at low E_s/N_0 it is not. This can be understood heuristically by noting that, in the limit as $E_s/N_0 \to 0$, the phase errors due to the frequency offset are negligible with respect to those due to the noise. At high E_s/N_0, however, the opposite is true and a dependence on Δ' appears.

V. Performance of Monomial Nonlinearities for Moderate E_s/N_0

To compare the performance of monomial nonlinearities to that of the optimal, (12) is integrated numerically for $m = 4$(QPSK) (quadrature phase shift keying), $\Delta f = 0$, and $F(\rho) = q(\rho)/h(\rho)$, the optimal nonlinearity. The performance (relative to the Cramer–Rao bound [1]) of the optimal and several monomial nonlinearities as a function of energy per bit divided by the one-sided spectral noise density is shown in Fig. 3. The fact that the performance of the nonlinearity $F(\rho) = \rho^2$ is very close to the optimal is important. Although a small gain in performance occurs when the optimal nonlinearity is used near $E_b/N_0 = 4$, the optimal nonlinearity requires E_b/N_0 dependent scaling of the received signal and is therefore sensitive to automatic gain control levels. From (3) we can see for monomial $F(\rho)$ that any scaling of ρ simply cancels in the numerator and denominator. This is a very nice property and a strong motivation for using the ρ^2 nonlinearity. We can conclude that for the $m = 4$ case (QPSK), ρ^2 is an excellent choice of nonlinearity in agreement with the claims of [1].

VI. Conclusion

Using the intermediate result of [1] we have derived an optimal nonlinearity for the estimator in Fig. 1. This nonlinearity is dependent on E_s/N_0 so that the signal-to-noise ratio must be estimated if optimal phase estimation is required at all noise levels. However, if it is known that E_s/N_0 is extreme, high or low, then there are monomial approximations for the nonlinearity which (asymptotically) do not depend on the signal-to-noise ratio. For the $m = 4$, $\Delta f = 0$ case we have shown that ρ^2, the nonlinearity proposed in [1], nearly achieves the upper bound in performance given by the optimal nonlinearity, and for practical reasons it is ideal for implementation.

Acknowledgment

The author would like to thank Audrey M. Viterbi and Andrew J. Viterbi for suggesting this problem and for their comments on the manuscript. The comments of the reviewers are also appreciated.

References

[1] A. J. Viterbi and A. M. Viterbi, "Nonlinear estimation of PSK-modulated carrier chase with applications to burst digital transmission," *IEEE Trans. Inform. Theory*, July 1983.

[2] M. Abramowitz and I. A. Stegun, Eds., *Handbook of Mathematical Functions*. Washington, DC: National Bureau of Standards, 1964.

[3] A. J. Viterbi, *Principles of Coherent Communication*. New York: McGraw-Hill, 1966.

On the Distribution of de Bruijn CR-Sequences

T. ETZION

***Abstract*—It is shown that the number of de Bruijn sequences of order n and linear complexity c is not a multiple of four for every n and c.**

In [1] de Bruijn sequences and their complexities are presented, and in [2] and [3] de Bruijn CR-sequences are investigated. Chan *et al.* [1] proved that the linear complexity c of a de Bruijn sequence of order n is an integer between $2^{n-1} + n$ and $2^n - 1$. They conjectured that the number of de Bruijn sequences of order $n > 3$ and linear complexity c, $\gamma(c, n)$, is a multiple of four, i.e., $\gamma(c, n) \equiv 0$ (modulo 4).

Let $\delta(c, n)$ denote the number of de Bruijn CR-sequences of order n and of linear complexity c. It is well-known that $\gamma(c, n) \equiv 0$ (modulo 4) if and only if $\delta(c, n) \equiv 0$ (modulo 4). Since for even $n \geq 4$ there are no de Bruijn CR-sequences, we have $\gamma(c, n) \equiv 0$ (modulo 4) for even n. For odd n there exist de Bruijn CR-sequences, and the following results have been obtained. Etzion and Lempel [2] showed that for even c $\delta(c, n) = 0$, and therefore $\gamma(c, n) \equiv 0$ (modulo 4). For $n \geq 4$, $\gamma(2^n - 1, n) \equiv 0$ (modulo 8) and for $k \geq 3$, $\gamma(2^{2k} - 1, 2k) \equiv 0$ (modulo 16). Etzion [3] showed that, if $2^{n-1} < c < 2^{n-1} + 2^{n-2}$, then $\delta(c, n) \equiv 0$ (modulo 4), and therefore $\gamma(c, n) \equiv 0$ (modulo 4).

The two de Bruijn sequences of order 3 are CR-sequences.

The complexities distribution of de Bruijn CR-sequences of order 5 were easily obtained:

c	$\delta(c, 5)$
23	4
25	8
27	12
29	8
31	32

For any other c not in the table, $\delta(c, 5) = 0$.

For $n = 7$, the characterization of de Bruijn CR-sequences [2], [3] and the Games and Chan [4] algorithm for computing the complexity of a sequence of length 2^n were used for a computer computation of $\delta(c, 7)$:

c	$\delta(c,7)$	c	$\delta(c,7)$	c	$\delta(c,7)$	c	$\delta(c,7)$
71	448	85	236	99	11802	113	1102220
73	8	87	284	101	20258	115	2116456
75	168	89	844	103	31144	117	4210074
77	24	91	1620	105	72250	119	8328830
79	88	93	2560	107	143238	121	16875998
81	40	95	6424	109	285742	123	33706580
83	224	97	7488	111	559216	125	67480984
						127	131815424

For any other c, $\delta(c, 7) = 0$.

It is now clear that for $c = 99$, 101, 105, 107, 109, 117, 119, and 121, $\delta(c, 7)$ is not a multiple of four and hence $\gamma(c, 7)$ is not a multiple of four.

References

[1] A. H. Chan, R. A. Games, and E. L. Key, "On the complexities of de Bruijn sequences," *J. Comb. Theory*, Ser. A, vol. 33, pp. 233–246, Nov. 1982.

[2] T. Etzion and A. Lempel, "On the distribution of de Bruijn sequences of given complexity," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 611–614, July 1984.

Manuscript received April 23, 1984; revised September 16, 1985.

The author is with the Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089, on leave from the Computer Science Department, Technion, Haifa, Israel.

IEEE Log Number 8406949.

[3] T. Etzion, "On the distribution of de Bruijn sequences of low complexity," *J. Comb. Theory*, Ser. A, vol. 38, pp. 241–253, Mar. 1985
[4] R. A. Games and A. H. Chan, "A fast algorithm for determining the complexity of a binary sequence with a period 2^n," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 144–146, Jan. 1983.

The Geometry of Quadrics and Correlations of Sequences

RICHARD A. GAMES

***Abstract*—Nondegenerate quadrics of $\mathrm{PG}(2l, 2^s)$ have been used to construct ternary sequences of length $(2^{2sl+1}-1)/(2^s-1)$ with perfect autocorrelation function. The same construction can be used for degenerate quadrics for this case as well as quadrics of $\mathrm{PG}(N, q)$, with N arbitrary and $q = p^s$, for any prime p. This is possible because it is shown that if $Q \subseteq \mathrm{PG}(N, q)$ is a quadric, possibly degenerate, that has the same size as a hyperplane, then, provided Q itself is not a hyperplane, the hyperplanes of $\mathrm{PG}(N, q)$ intersect Q in three sizes. These sizes depend on whether N is even or odd and the degeneracy of Q. Finally, a connection to maximum period linear recursive sequences is made.**

I. Introduction

In [1] it was shown how nondegenerate quadrics in the finite projective geometry $\mathrm{PG}(2k, 2^s)$ can be used to construct ternary sequences with perfect periodic autocorrelations. In fact, the quadrics involved in the construction of [1] can be degenerate, and so this correspondence considers this possibility. In addition, the construction works for arbitrary prime power q, and because degenerate quadrics are allowed, the projective dimension N may be odd, giving a variety of resulting sequence lengths. These extensions of [1] are possible because, as is shown, if $Q \subseteq \mathrm{PG}(N, q)$ is a quadric the same size as a hyperplane but is not a hyperplane, then the hyperplanes of $\mathrm{PG}(N, q)$ intersect Q in sets of three sizes.

Now the setting of this correspondence is given and the results of [1] reviewed. Regard $\mathrm{GF}(q^{N+1})$ as an $(N+1)$-dimensional vector space over $\mathrm{GF}(q)$. If α is a primitive element of $\mathrm{GF}(q^{N+1})^* = \{x \in \mathrm{GF}(q): x \neq 0\}$, then the points of $\mathrm{PG}(N, q)$, which are the one-dimensional subspaces of the vector space $\mathrm{GF}(q^{N+1})$, are represented by $\{\alpha^i: i = 0, 1, 2, \cdots, v-1\}$, where $v = (q^{N+1}-1)/(q-1)$. A further identification with the integers modulo v, $\mathbb{Z}_v$, can be made by $\alpha^i \leftrightarrow i$. A set $X \subseteq \mathrm{PG}(N, q)$ corresponds to $D(X) = \{i: \alpha^i \in X\} \subseteq \mathbb{Z}_v$, and both X and $D(X)$ correspond to the periodic sequence $s(X)$ whose one period is given by the characteristic vector $s(X) = (x_0, x_1, \cdots, x_{v-1})$, where $x_i = 1$ when $i \in D(X)$ and $x_i = 0$ otherwise.

If $H \subseteq \mathrm{PG}(N, q)$ is a hyperplane, then $D(H) \subseteq \mathbb{Z}_v$ is a Singer difference set with parameters [2, p. 128]

$$v = \frac{q^{N+1}-1}{q-1} \qquad k = \frac{q^N-1}{q-1} \qquad \lambda = \frac{q^{N-1}-1}{q-1}.$$

That H and its translates $\alpha^i H = \{\alpha^i x: x \in H\}$, $i = 0, 1, \cdots, v-1$, form a symmetric block design on the points of $\mathrm{PG}(N, q)$ corresponds to the fact that the sequence $s(H) = (x_0, x_1, \cdots, x_{v-1})$ has a two-valued periodic autocorrelation

$$(s(H) * s(H))_j = \sum_{i=0}^{v-1} x_{i+j} x_i = \begin{cases} k, & j \equiv 0 \pmod v \\ \lambda, & j \not\equiv 0 \pmod v \end{cases}.$$

If r is relatively prime to v, then $x \mapsto x^r$ is a permutation of the points of $\mathrm{PG}(N, q)$ which corresponds to the permutation $i \mapsto ri$ of $\mathbb{Z}_v$. Then $H^r = \{x^r: x \in H\}$ corresponds to $rD(H) = \{ri: i \in D(H)\}$, and it follows that $rD(H)$ is still a (v, k, λ)-difference set, that is, $s(H^r)$ also has a two-valued periodic autocorrelation. The idea of [1] is to find values of r such that the sequences $s(H) = (x_0, x_1, \cdots, x_{v-1})$ and $s(H^r) = (y_0, y_1, \cdots, y_{v-1})$ have a periodic cross correlation

$$\theta_j = (s(H) * s(H^r))_j = \sum_{i=0}^{v-1} x_{i+j} y_i$$

with few distinct values. Then it follows [3] that the integer sequence $\boldsymbol{\theta}$ has a two-valued periodic autocorrelation given by

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

To obtain appropriate values of r for the case of $N = 2k$ and $q = 2^s$, it is shown in [1] that if $r^{-1} = 2^i + 2^j$ (i.e., $2^i + 2^j$ must also be relatively prime to v), then H^r is a quadric in $\mathrm{PG}(2k, 2^s)$, and furthermore, that the hyperplanes intersect a nondegenerate quadric in $\mathrm{PG}(2k, 2^s)$ in sets of three sizes—corresponding to the fact that the sequences $s(H)$ and $s(H^r)$ have a three-valued periodic cross correlation $\boldsymbol{\theta}$. The intersection sizes in this case are such that a sequence $\hat{\boldsymbol{\theta}}$ can be formed from $\boldsymbol{\theta}$ with entries 0 and ± 1 and perfect periodic autocorrelation

$$(\hat{\boldsymbol{\theta}} * \hat{\boldsymbol{\theta}})_j = \begin{cases} (2^s)^{2k}, & j \equiv 0 \pmod v \\ 0, & j \not\equiv 0 \pmod v \end{cases}.$$

In [1] it was argued that in the case that $r^{-1} = 2^i + 2^j$, then H^r is a nondegenerate quadric, which is assumed in the result on hyperplane intersections. However, this may not be the case as the example $q = 2$, $k = 4$, $N = 8$, $v = 511$, $r^{-1} = 1 + 8 = 9$, $r = 284 \pmod{511}$ shows. If $H \subseteq \mathrm{PG}(8, 2)$ is a hyperplane, then H^{284} is a quadric (by the construction in [1]). Actual computation shows that the hyperplanes of $\mathrm{PG}(8, 2)$ intersect H^{284} in sets of size 143, 127, and 111 with respective multiplicities 36, 447, and 28, instead of sizes 135, 127, and 119 with respective multiplicities 136, 255, and 120 as is predicted by [1, theorem 3.2]. The problem arises because, although H^r is a quadric, it is a degenerate quadric in this case, in fact a cone of order 2. This correspondence shows that the result on the three hyperplane intersection sizes is still true for degenerate quadrics, and so the construction of [1] is still valid. In addition, the case of odd projective dimension can also be considered now since if H^r is a quadric in this case, then it is necessarily degenerate.

Section II reviews the notion of quadrics in finite projective geometries and gives the main result on hyperplane intersections. The proof, given in the Appendix, is valid for arbitrary prime power q and projective dimension N. The work ends with a conjecture as to when $H^r \subseteq \mathrm{PG}(N, q)$ is a quadric and a suggestion that actually the cross-correlation spectra of m-sequences is involved.

II. Quadrics in $\mathrm{PG}(N, q)$ and Hyperplane Intersections

In finite projective geometry $\mathrm{PG}(N, q)$ of N dimensions based on the field $\mathrm{GF}(q)$, the points can be taken as $(N+1)$-column vectors $x^t = (x_0, x_1, \cdots, x_N)$, where $x_0, x_1, \cdots, x_N$ are elements

Manuscript received August 13, 1983; revised September 16, 1985. This work was presented in part at the IEEE International Symposium on Information Theory, St. Jovite, PQ, Canada, September 26–30, 1983.

The author was with the Department of Mathematics, Colorado State University, Fort Collins, CO. He is now with The MITRE Corporation, E020, Bedford, MA 01730.

IEEE Log Number 8406955.

0018-9448/86/0500-0423$01.00