Equation (17) is equivalent to the recursion

$$a_n^2 - a_{n-1}^2 = \frac{(\mathrm{SNR})_i}{N} a_{n-1}^2 \tag{18}$$

whose solution is

$$a_n^2 = a_1^2 \left[1 + \frac{(\mathrm{SNR})_i}{N}\right]^{n-1}. \tag{19}$$

Just as in Schalkwijk[2] we generate the estimates recursively, i.e.,

$$\hat{\theta}^k(n) = \left[1 + \frac{(\mathrm{SNR})_i}{N}\right]\hat{\theta}^k(n-1) + \frac{\dfrac{\sigma_a^2 (\mathrm{SNR})_i}{N}}{1 + \dfrac{(\mathrm{SNR})_i}{N}} u_n. \tag{20}$$

J. P. M. Schalkwijk
L. I. Bluestein
Communication Systems Laboratories
Sylvania Electronic Systems
Div. of Sylvania Elec. Prods., Inc.
Waltham, Mass. 02154

References

[1] T. J. Goblick, "Theoretical limitations on the transmission of data from analog sources," *IEEE Trans. Information Theory*, vol. IT-11, pp. 558–567, October 1965.
[2] J. P. M. Schalkwijk, "A coding scheme for additive noise channels with feedback, Part II: Band-limited signals," *IEEE Trans. Information Theory*, vol. IT-12, pp. 183–189, April 1966.
[3] T. Kailath, "An application of Shannon's rate-distortion theory to analog communication over feedback channels," *Proc. Princeton Symp. on System Science*, March 1967.
[4] T. J. Cruise, "Achievement of rate-distortion bound over additive white noise channel utilizing a noiseless feedback channel," *Proc. IEEE (Letters)*, vol. 55, pp. 583–584, April 1967.

Optimal Binary Sequences for Spread Spectrum Multiplexing

I. Introduction

Linear shift register sequences (see Zierler[1] and Gold[2]) have found extensive applications in spread spectrum communication systems. The binary sequences generated by shift register devices serve as the encoding mechanism of such systems which, when added to the baseband information, results in a wideband low-power-density signal which has statistical properties similar to noise. The casual listener is thus denied access to the baseband information which can be recovered from the wideband signal only through correlation with a stored reference sequence in the receiver which is an exact replica of the original encoding sequence.

The usefulness of the maximal linear sequences in spread spectrum communications depends in large part on their ideal autocorrelation properties. The autocorrelation function of a binary sequence h is defined as $\theta_h(\tau)$ = (number of agreements − number of disagreements) when the sequence h is compared with a cyclic shift of itself. It is well known that for maximal linear sequences $\theta_h(0)$ = period of the sequence and $\theta_h(\tau) = -1$ for $\tau \not\equiv 0$. The detection by the receiver of the high in-phase correlation value $\theta_h(0)$ determines the synchronization between transmitter and receiver necessary for the removal of the encoding sequence and the recovery of the baseband information. In multiplexing applications many systems will be operating in the same neighborhood and each communication link will employ a different maximal encoding sequence. In general, the cross-correlation function between different maximal sequences may be relatively large. Thus different systems operating in the same environment can interfere with the successful attainment and maintenance of proper synchronization by having the receiver of one communication link lock onto the cross-correlation peaks obtained by correlating with the encoding sequence of a different communication link. Thus the successful use of spread spectrum communication systems in multiplexing applications depends upon the construction of large families of encoding sequences with uniformly low cross-correlation values. In this paper we present an analytical technique for the construction of such families of linear binary encoding sequences.

Manuscript received July 22, 1966; revised February 4, 1967.

II. Notation

Following the notation of Zierler[1] we denote by $V(f)$ the vector space of linear sequences generated by the recursion relation corresponding to the polynomial f of degree n and further identify the members of $V(f)$ with binary $2^n - 1$ tuples. If f is a primitive polynomial over the field $K = \{0, 1\}$ then $h \in V(f)$ implies h is a maximal linear sequence. We denote by $||h||$ the number of ones in the sequence h and by $\bar{h}$ the sequence such that $\bar{h}(i) = h(i) + 1$. The correlation function θ of two binary sequences a, b has been defined as

$$\theta(\tau) = \sum_{i=0}^{2^n-1} \chi a(i)\chi b(i + \tau)$$

where χ is the unique isomorphism of the additive group $\{0, 1\}$ onto the multiplicative group $\{1, -1\}$. We note that $\theta(a, b)$ (τ) is simply described as the number of agreements − number of disagreements of the sequences a and b for each τ and that

$$\theta(a, b) = 2^n - 1 - 2\,||a + b||.$$

In what follows α will always denote a primitive $2^n - 1$ root of unity in a splitting field of $x^{2^n-1} + 1$ and the minimal polynomial of α^i will be denoted by f_i. Finally, we note the following result of Bose and Chaudhuri.[3]

Theorem 1

Let α be any primitive element of the splitting field of $x^{2^n-1} + 1$. Let f_i be the minimal polynomial of α^i. Let

$$g = \frac{x^{2^n-1} + 1}{\mathrm{lcm}\,\{f_1, f_2, \cdots f_{2k}\}}$$

Then $a, b \in V(g)$ implies $||a + b|| > 2k$.

III. Statement and Proof of Result

Our techniques for the construction of large families of encoding sequences with uniformly low cross-correlation values is based on the following result.

Theorem 2

Let α be any primitive element of $GF(2^n)$. Let f_1 be the minimal polynomial of α. Let f_t be the minimal polynomial of α^t where

$$t = \begin{cases} (2^{(n+1)/2}) + 1 & (n \text{ odd}) \\ (2^{(n+2)/2}) + 1 & (n \text{ even}). \end{cases}$$

Then $a \in V(f_1)$ and $b \in V(f_t)$ implies $|\theta(a, b)| \leq t$.

The significance of this theorem is that it tells how to select shift register tap connections which will generate maximal linear sequences with a known bound on the cross-correlation function. Since α is primitive, the sequence generated by the shift register corresponding to f_1 is maximal. Since

$$2^{(n+1)/2} + 1 \quad \text{and} \quad 2^{(n+2)/2} + 1$$

are both relatively prime to $2^n - 1$ for $n \not\equiv 0 \bmod 4$ the sequence corresponding to the polynomial f_t is also maximal in these cases. Theorem 2 thus permits the selection of pairs of maximal sequences with known bound on the cross-correlation function. This result is of practical importance since, for example, for $n = 13$ there are 630 maximal sequences and there exist pairs of these sequences

whose correlation values are as high as $\theta = 703$ while Theorem 2 guarantees the selection of pairs of sequences such that $|\theta| \leq 129$.

This result is a special case of the more general theorem stated in the following which has been obtained independently by Gold[5] and Kasami,[4] and is related to the weight distribution of error-correcting codes.

Theorem

Let a and b be maximal linear sequences given by

$$a(i) = T(\alpha^{-i}) \quad \text{and} \quad b(i) = T((\alpha^{2^l+1})^{-i})$$

where α is a primitive $2^n - 1$ root of unity (n odd), l is any integer such that $(l, k) = 1$, and T is the trace of $GF(2^n)$. Then $\theta(a, b)(n) = -1$ when $a(\tau) = 0$ and

$$\theta(a, b)(\tau) = \begin{cases} -(2^{(n+1)/2} + 1) \\ \quad \text{or} \qquad \text{when} \quad a(\tau) = 1. \\ (2^{(n+1)/2} - 1) \end{cases}$$

The proof of this theorem is contained in Gold[5].

In the remainder of this section, we proceed to the proof of Theorem 2 by means of a series of lemmas.

Lemma 1

Let α be any primitive $2^n - 1$ root of unity in a splitting field of

$$x^{2^n-1} + 1.$$

Let

$$g_k = \frac{x^{2^n-1} + 1}{\text{lcm } \{f_1, f_2, \cdots f_k\}}$$

where f_i is the minimal polynomial of α^i. Let f be an irreducible polynomial of degree n. Let A_f be the conjugate class of roots of f. Let $m_f = \min \{i \mid \alpha^i \in A_f\}$, the class leader of A_f. Then $m_f > k$ implies f is a factor of g_k.

Proof: f irreducible of degree n implies $f \mid x^{2^n-1} + 1$ implies $f \mid g_k$ lcm $\{f_1, f_2, \cdots f_k\}$, and $m_f > k$ implies $f_i \mid \text{lcm } \{f_1 \cdots f_k\}$ implies $f \mid g_k$.

Lemma 2

Let α be any primitive $2^n - 1$ root of unity in a splitting field of

$$x^{2^n-1} + 1.$$

Let $u = 2^{n-1} - 1$. Let

$$v = \begin{cases} 2^{n-1} - 1 - 2^{n-1/2} & \text{for } n \text{ odd} \\ 2^{n-1} - 1 - 2^{n/2} & \text{for } n \text{ even.} \end{cases}$$

Let f_u be the minimal polynomial of α^u. Let f_v be the minimal polynomial of α^v. Then $m_{f_u} = u$ and $m_{f_v} = v$.

Proof: α^r and α^s belong to the same conjugate class of $GF(2^n)$ if, and only if, there exists an integer k such that $\alpha^r = (\alpha^s)^{2^k}$ if, and only if, $r = s \cdot 2^k$ modulo $2^n - 1$ if, and only if, there exists a cyclic permutation p such that $[r(0), r(1), \cdots r(n-1)] = [s(p(0)), s(p(1)) \cdots s(p(n-1))]$ where

$$r = \sum_{i=0}^{n-1} r(i)2^i \quad \text{and} \quad s = \sum_{i=0}^{n-1} s(i)2^i.$$

Now $u = 2^n - 1 = \sum_{i=0}^{n-1} u(i)\, 2^i$ where $[u(0), u(1), \cdots u(n-1)] = [1\ 1 \cdots 1\ 0]$. Clearly any permutation of $[1\ 1 \cdots 1\ 0]$ corresponds to a larger integer and hence $m_{f_u} = u$. Now

$$v = 2^{n-1} - 1 - 2^{n-1/2} = \sum_{i=0}^{n-1} v(i)2^i$$

where

$$\left[v(0), v(1), \cdots v\left(\frac{n-3}{2}\right), v\left(\frac{n-1}{2}\right), \cdot v\left(\frac{n+1}{2}\right) \cdots v(n-2)v(n-1)\right]$$

$$= [\underbrace{1, 1, \cdots 1}_{n-1/2 \text{ ones}}, \ 0, \ \underbrace{1 \cdots 1}_{n-1/2 \text{ ones}}, \ 0].$$

Again it is clear that any cyclic permutation of $[v(0), \cdots v(n-1)]$ will result in a larger integer and hence $m_{f_v} = v$. A similar argument holds when $v = 2^{n-1} - 1 - 2(n/2)$.

Lemma 3

f_u and f_v are factors of g_{v-1} where u and v are as in Lemma 2 and

$$g_{v-1} = \frac{x^{2^{n-1}} + 1}{\text{lcm } \{f_1, f_2, \cdots f_{v-1}\}}$$

then $f_v \mid g_{v-1}$.

Proof:

$$m_{f_u} = u \text{ (by Lemma 2)} = 2^n - 1$$

$> 2^{n-1} > v - 1$ implies $f_u \mid g_{v-1}$ (by Lemma 1)

$$m_{f_v} = v \text{ (by Lemma 2)} > v - 1 \text{ implies } f_v \mid g_{v-1}.$$

Lemma 4

Let f_i denote the minimal polynomial of α^i. Let

$$g_k = \frac{x^{2^n-1} + 1}{\text{lcm } \{f_1, f_2, \cdots f_k\}}.$$

Then $a, b \in V(g_k)$ implies $|\theta(a, b)| < 2^n - 1 - 2k$.

Proof: $a, b \in V(g_k)$ implies $a + b \in V(g_k)$ implies $||a + b|| > k$ by Theorem 1. Since 1 is not a primitive root of unity, $1 + x$ is clearly a factor of g, and hence $V(1 + x) \subset V(g_k)$. Thus the constant sequence of ones is a member of $V(g_k)$, and hence $V(g_k)$ is closed with respect to the operation of complementation, i.e., $h \in V(g_k)$ implies $\tilde{h} \in V(h_k)$ where $\tilde{h}(i) = 1 + h(i)$.

Thus $a, b \in V(g_k)$ implies $a + b \in V(g_k)$ implies $\widetilde{a + b} \in V(g_k)$ implies $||\widetilde{a + b}|| = 2^n - 1 - ||a + b|| > k$ implies $k < ||a + b|| < 2^n - 1 - k$ implies $|\theta(a, b)| < (2^n - 1) - 2k$.

Proof of Theorem 2: Let $\beta = \alpha^{-2}$. Then β is clearly a primitive $2^n - 1$ root of unity and

$$\alpha = \alpha^{-2}(2^{n-1} - 1) = \beta^{2^{n-1}} - 1 = \beta^u$$

$$\alpha^t = \begin{cases} \alpha^{(2^{n+1})/2} + 1 & (\text{for } n \text{ odd}) = \\ \alpha^{(2^{n+2})/2} + 1 & \text{for } n \text{ even;} \end{cases}$$

$$\left\{\begin{matrix} \alpha^{-2}[2^{n-1} - 1 - 2^{(n-1)/2}] = \beta^{2^{n-1}} - 1 - 2^{n-1/2} \\ \alpha^{-2}[2^{n-1} - 1 - 2^{n/2}] \quad = \beta^{2^{n-1}} - 1 - 2^{n/2} \end{matrix}\right\} = \beta^v.$$

Now f_1 is the minimal polynomial of $\alpha = \beta_u$ and f_t is the minimal polynomial of $\alpha^t = \beta_v$. By Lemma 2 $m_{f_1} = u > v - 1$ and $m_{f_t} = v > v - 1$. Thus by Lemma 1 f_1 and f_t are factors of g_{v-1}. Hence, $V(f_1) \subset V(g_{v-1})$ and $v(f_t) \subset V(g_{v-1})$. Thus $a \in V(f_1)$ and $b \in V(f_t)$ implies a and $b \in (g_{v-1})$. Thus by Lemma 4

$$|\theta(a, b)| < 2^n - 1 - 2(v - 1) =$$

$$\begin{cases} 2^n - 1 - 2[2^{n-1} - 2 - 2^{n-1/2}] = 2^{(n+1)/2} + 3 \\ 2^n - 1 - 2[2^{n-1} - 2 - 2^{n/2}] \quad = 2^{(n+2)/2} + 3. \end{cases}$$

Since the value of the cross-correlation function is always odd we have

$$|\theta(a, b)| \leq 2^{n+1/2} + 1 \quad \text{for} \quad n \text{ odd}$$

$$|\theta(a, b)| \leq 2^{n+2/2} + 1 \quad \text{for} \quad n \text{ even}.$$

For 13-stage shift registers there are pairs of maximal sequences with cross-correlation peaks as high as $\theta(\tau) = 703$ while proper selection of shift registers in accordance with the above theorem guarantees sequences whose cross correlation satisfies the inequality

$$|\theta(\tau)| \leq 2^{(13+1)/2} + 1 = 129.$$

We note further that for purely random sequences of length $2^{13} - 1 = 8191$ we would expect the cross-correlation function to exceed $2\sigma = 2\sqrt{8192} \sim 180$ for 5 percent of the correlation values and hence linear sequences chosen in accordance with our technique perform better with respect to their cross-correlation properties than purely random sequences.

IV. Construction of Encoding Families

In this section we show how to provide large families of encoding sequences each of period $2^n - 1$ and such that the cross-correlation function of any pair of sequences of the family has a cross-correlation function θ which satisfies the inequality

$$|\theta(\tau)| \leq 2^{(n+2)/2} + 1.$$

In a spread spectrum multiplexing application such families form ideal codes which minimizes interlink interference. Instead of having each communication link employ a different maximal sequence we assign to each link a member of the encoding family to be constructed below. These are nonmaximal linear sequences, and hence their autocorrelation function will not be two-valued; however, the out-of-phase value of the autocorrelation function will satisfy the above inequality. Thus by slightly relaxing the conditions on the autocorrelation function we obtain a family of encoding sequences with the high cross-correlation peaks eliminated.

The procedure for generating these encoding families is embodied in the following theorem.

Theorem

Let f_1 and f_t be a preferred pair of primitive polynomials of degree n whose corresponding shift registers generate maximal linear sequences of period $2^n - 1$ and whose cross-correlation function θ satisfies the inequality.

$$|\theta| \leq t = \begin{cases} 2^{(n+1)/2} + 1 & \text{for} \quad n \text{ odd} \\ 2^{(n+2)/2} + 1 & \text{for} \quad n \text{ even} \quad n \not\equiv \bmod 4. \end{cases}$$

Then the shift register corresponding to the product polynomial $f_1 \cdot f_t$ will generate $2^n + 1$ different sequences each period $2^n - 1$ and such that the cross-correlation function θ of any pair of such sequences satisfies the above inequality.

Proof: $a \in V(f_1 \cdot f_t) = V(f_1) + V(f_t)$ implies $a = b + c$ where $b \in V(f_1)$ and $c \in V(f_t)$. Period $(b + c) = \text{lcm}\{\text{period } b, \text{period } c\} = 2^n - 1$. Since degree $f_1 \cdot f_t = 2n$, there are $(2^{2n} - 1)/(2^n - 1) = 2^n + 1$ essentially different sequences in $V(f_1 \cdot f_t)$. Finally $a, b \in V(f_1 \cdot f_t)$ implies

$$\begin{cases} a = a_1 + a_t \\ b = b_1 + b_t \end{cases}$$

where $a_1, b_1 \in V(f_1)$, and $a_t, b_t \in V(f_t)$. $|\theta(a, b)| = |\theta(a_1 + b_1, a_t + b_t)| \leq t$ by Theorem 2 since $a_1 + b_1 \in V(f_1)$ and $a_1 + b_1 \in V(f_t)$.

Thus, by way of illustration, if we consider the pair of polynomials, $f_1(x) = 1 + x + x^2 + x^3 + x^7$ and $f_t(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^7$ then the product polynomial is $f_1(x)\, f_2(x) = 1 + x^2 + x^6 + x^8 + x^{11} + x^{12} + x^{14}$ and the corresponding 14-stage shift register will generate 129 different linear sequences of period 127. The cross-correlation function θ of any pair of such sequences will satisfy the inequality $|\theta(\tau)| \leq 17$.

Robert Gold
Magnavox Research Laboratories
Torrance, Calif. 90503

References

[1] N. Zierler, "Linear recurring sequences," *J. SIAM*, vol. 7, March 1959.
[2] R. Gold, "Characteristic linear sequences and their coset functions," (accepted for publication *J. Soc. Ind. Appl. Math.*, May 1965).
[3] W. W. Peterson, *Error Correcting Codes*. New York: Wiley, 1961.
[4] T. Kasami, "Weight distribution formula for some class of cyclic codes," University of Illinois, Urbana, Rept. R-265, April 1966.
[5] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions" (submitted for publication, January 1967).

Average Digit-Error Probability After Decoding Random Codes

Introduction

When a transmitted code word is decoded incorrectly due to channel errors, it does not follow that all of the digits in the decoded word are incorrect. One way of getting an estimate of the actual number of digit errors to be expected is to determine the average over a whole class of codes of the digit-error probability and to compare this with the word-error probability averaged over the same class. In this correspondence the ratio of these two averages is determined for random block codes and it is shown that, at fixed code rate and channel-error probability, the ratio approaches a nonzero limit with increasing code length; the value of this limit is given as a function of code rate and channel-error probability. It is pointed out that the result can be extended to random linear codes and to the information digits of random parity check codes is also given. A more detailed derivation for these two linear cases is given elsewhere.[1]

It should be stressed at the outset that both the average word-error probability and the average digit-error probability can be strongly influenced (particularly at small channel probabilities) by a very few codes with unusually large word- and digit-error probabilities. Hence, it is unlikely that there is any easy extension of these results to statements about the distribution of the ratio of the two probabilities over the classes of codes considered.

Notation and Assumptions

Let n = code length
R = code rate
$K = 2^{nR}$
p = channel-error probability
$H(t) = -t \log_2 t - (1 - t) \log_2 (1 - t)$
p_R = smaller solution of $R + H(p_R) = 1$
$p_C = p_R^2/(1 - 2\, p_R + 2p_R^2)$
p_W = average word-error probability
p_D = average digit-error probability
$\mathbf{E}$ = expected value of.

The symbol $\sim$ used in equations of the form $f(t) \sim g(t)$ as $t \to \infty$ means that the ratio of the two functions approaches unity: $f(t)/g(t) \to 1$.

The expression $o(n)$ used in equations of the form $f(n) = o(n)$ as $n \to \infty$ means $f(n)/n \to 0$ as $n \to \infty$.

Manuscript received December 12, 1966; revised May 22, 1967.
[1] J. N. Pierce, "Average digit error probability after decoding random linear codes," Air Force Cambridge Research Labs., Bedford, Mass., Rept. 66-695, October 1966.