Optimum Code-Division Multiple-Access Codes Using Spread Spectrum Techniques

Kyung-sik Kim

Spread Spectrum 技術을 利用한 最適 Code-Division Multiple-Access Codes

金 敬 植

—Summary—

The purpose of this paper is to review several of the code-division multiple-access sequence desings which are known to nearly achieve the Welch bound. Specially, with the variety of desings available, it appears that convenience of mechanization may very well be the deciding factor in a design.

Introduction

Judge (1962) has considered code-division multiplexing by using quasiorthogonal binary function (linear maximal sequences) and states that for two equal power signals multiplexed together signal to noise is

$$\frac{S}{N(2)}=\frac{S}{(K_1^2+T_o/T)^{1/2}} \tag{1}$$

in each receiver. For b signals

$$\frac{S}{N(b)}=\frac{S}{[b(K_1^2+T_o/T)]^{1/2}} \tag{2}$$

where T =the crosscorrelation integration period,

T_0=the code bit period,

K_1=value of DC correlation.

Judge's result shows that some Mersenne prime sequences exhibit crosscorrelation values superior to other, sometime even for nonprime sequences longer than prime sequences. The composite code sequences are of great utility when crosscorrelation is a prime consideration. Their real advantage lies in that for every code in a set of 2^n-1, crosscorrelation values are well defined , and a system can be designed to operate within this definition.

Welch (1974) published a bound on inner products which could be specialized to the case of periodic correlation of spread-spectrum code-division multiple-access(CDMA) signal sets. Specifically, consider a set of M sequences a_t^i, $i=1,\cdots,M$, of period L,

$$a_t^i = a_{t+L}^i \tag{3}$$

The periodic crosscorrelation between sequence i and soquence j at shift τ is defined as

$$C_{ij}(\tau)\triangle\sum_{t=0}^{L-1} a_{t+\tau}^i(a_t^j)^* \tag{4}$$

(()* denotes conjugation), the maximum auto-correlation of the set is

$$C_1 \triangleq \max_{i} \max_{o<\tau<L} |C_{ij}(\tau)| \qquad (5)$$

and the maximum crosscorrelation of the set is

$$C_2 \triangleq \max_{i\neq j} \max_{o\leq\tau\leq L} |C_{ij}(\tau)| \qquad (6)$$

Under the assumption that the sequences all have the same energy per period, i.e.,

$$C_{ij}(O)=C_{jj}(O) \qquad (7)$$

Welch demonstrates the .nomalized correlation bound

$$C_{max} \triangleq \frac{\max(C_1,C_2)}{C_{11}(O)} \leq \sqrt{\frac{M-1}{ML-1}} \qquad (8)$$

This bound has become the standard against which a possible CDMA signal set design is compared, despite the fact that Cmax often is not specifically a parameter in the communication system design(Pursley and Darwate, 1977).

All of the designs basically achieve Welch's lower bound on the maxmum value of periodic crosscorrelation between signals and are optimum in this sense.

Optimum CDMA Code Designs

The Gold codes (Gold, 1966, 1967) are attractive for application in which a number of code-division multiplexed signals are to be used. The same guarantee of bounded crosscorrelation is impossible for maximal sequnces of the same length. Gold has presented a methode for choosing the codes used as components to generate Gold sequences that gives a set of sequences, each of whose members has crosscorrelation bounded by $|\theta(\tau)|\leqq 2^{(n+1)/2}+1^{(bits)}$when compared with any other member of the set. An equivalent result is given by Anderson (1969) for the Gold codes ; that is, Anderson's expression for the crosscorrelation bound is

$$|\theta(\tau)|_G \leq \left(\frac{\sqrt{2}\sqrt{1+1/L}+1/\sqrt{2}}{L}\right)^{1/2} \qquad (9)$$

It is apparent from this expression that as L→∞, $|\theta(\tau)| \rightarrow \sqrt{2}/\sqrt{L}$. Convergence is sufficiently rapid that for any code sequence length of interest $|\theta(\tau)|=\sqrt{2}/\sqrt{L}$ percent. Notice that one expressiong ives crosscorrelation. in bits, whereas the other gives a percentage of maximum correlation. Bynormalizing maximum correlation to one $2^{(n+1/2}+1 \approx \sqrt{2}L/\sqrt{L}$ for large L. Anderson also states that the crosscorrelation function for maximal sequences is bounded by

$$|\theta(\tau)| \leq \left(\frac{1+1/L-1/L^2}{L}\right)^{1/2} \qquad (10)$$

Now, as L→∞, $|\theta(\tau)| \rightarrow 1/\sqrt{L}$. For a given value of L the Gɔld codes exhibit crosscorrelation that $(\sqrt{2}/\sqrt{L})\,/\,(1/\sqrt{L}) = \sqrt{2}$ greater than maximal length sequences of the same length.

Kasami sequences (Kasami, 1966, Roefs, 1977) were designed originally as linear cyclic error-correcting codes. The underlying arithmetic in Kasami's design is performed in the finite field GF(2^n), n even, with $M_1(z)$ representing the minimum polynomial over GF(2) of a primitive element of .GF(2^n), and $M_s(z)$ representing the minimum polynomial over GF(2) of α^s, where $s=2^n/^2+1$. Thus α^s has order $2^n/^2-1$ and is a primitive element of GF($2^n/^2$). Hence $M_1(z)$ and $M_s(z)$ can be viewed as the characteristic polynomials of binary (0,1) linear feedback shift registers which generate M-sequences, b^1_t and b^s_t of lengths 2^n-1 and $2^n/^2-1$ respectively. The Kasami sequence set consists of linear combinations of the two sequences which, after converting to ±1 sequences, are

$$a^t_t=(-1)b^1_t+b^s_{t+t}, \text{ and } a^{2^{n/2}}_t=(-)^{b^1_t} \qquad (11)$$

This yields a set of

$$M=2^{n}/^{2} \qquad (12)$$

sequences, all with period

$$L=2^{n}-1 \qquad (13)$$

and

$$\max(C_1,C_2)=2^{n}/^{2}+1 \qquad (14)$$

Bent sequences (Olsen, 1977) possess an underlying arithmetic structure in GF(2^n), n divisible by 4, which is linked to the space Vn of binary n-tuples over GF(2) by a basis $\beta_1, \beta_2, \cdots, \beta_n$ for GF(2^n) which has the property that

$$tr(\beta_i\beta j)=\begin{cases}1, & i=j\\ 0, & \text{otherwise}\end{cases} \qquad (15)$$

Here $t_r(\cdot)$ represents the trace function mapping GF(2^n) onto GF(2) (Berlekamp, 1968). This generates a correspondence between discrete Fourier transforms of functions defined on Vn and trace transforms of the same functions defined on GF(2^n). This property is exploited along with the fact that bent functions (Rothaus, 1976) on Vn hase a flat Fourier transform to eventually give the following set of sequences :

$$a_t^i=(-1)^{G(Y_1)+{}_{Y1}T_{Y2}+{}_{C}T_{X}+{}_{I}T_{Y}} \qquad (16)$$

where X is the (vector) contents at time t of a Galois-configured linear-feedback shiftregister with a primitive characteristic polynomial of degree n,

$$Y \triangleq \begin{bmatrix}Y_1\\ Y_2\end{bmatrix} = LX \qquad (17)$$

where L is a specially designed n/2×n matrix, the dimensions of Y_1 and Y_2 being n/4, I is the representation of i as a binary n/2-tuple, C is a fixed non-zero constant and $G(Y_1)$ is a fixed arbitrary Boolean Function of Y_1. This design results in a set of sequences with the same M, L, and $\max(C_1,C_2)$parameters as the Kasami Sequences.

Group charaoter sequences (Lerner, 1961, Scholtz and Welch, 1978) are based on properties of the group M(L) of integers relatively prime to L under multiplication modulo L. In the special case when L is a prime, then

$$a_t^i = \begin{cases} 0 & , t=0\\ \rho^{i\ell(t)} & , 0<t<L\end{cases} \qquad (18)$$

where ρ is a primitive L-1st root of unity and $\ell(t)$ is the moduol L logarithm of t in the sense that

$$g^{\ell(t)}=t \text{ modulo } L \qquad (19)$$

g being a primitive element of M(L). The index i is restricted to $1 \leqq i < L-1$. Of course for large values of L the use of $a_0^1=1$ will make little difference in the final results. Group character sequences have the following properties :

$$\begin{cases} M=L-2\\ L=\text{prime number}\\ C_1=1\\ C_2=\sqrt{L}\\ C_{11}(0)=L-1\end{cases} \qquad (20)$$

Generally the ith sequence is composed of (L−1)/gcd(i, L−1) order roots of unity, e. g., i=(L−1)/2 is a sequence of ±1's and is usually called a quadratic residue sequence.

Welch and Alltop separately has proposed signal designs which incorporate a cyclic difference set structure (Baumert, 1971) to determine the locations of the non-zero elements of a sequence. A(v, k, λ) cyclic difference set is a collection $\{t_i\}$ of integers in the range $0 \leqq d_i < v$ with the property that the equation

$$t_i - t_j = \ell \bmod v$$

has λ solutions for $\ell \neq O$ and k solutions when $\ell = O$. We view the elements are non-zero. The values of the non-zero elements of each sequence are chosen so that any pair of sequences is orthogonal or nearly orthogonal when the shift paramter τ is zero.

For example let {Xt} be an m-sequence over GF(q), i.e., it satisfies an nth order linear recursion over GF(q) and has period q^n-1. Then a cyclic difference set with parameters

$$v = \frac{q^{n-1}}{q-1,}, \; k=\frac{q^{n-1}-1}{q-1}, \; =\frac{q^{n-2}-1}{q-1} \qquad (22)$$

is given by

$$D=\{t:xt=O\} \qquad (23)$$

If we consider a set of sequences based on the above difference set with n=3, then the resulting design parameters are

$$C_{11}(O)=\begin{cases} L=v=q^2+q+1 \\ M=k=q+1 \\ \max(C_1,C_2)=\lambda=1 \end{cases} \qquad (24)$$

Orthogonality of the sequences at $\tau=O$ imposes the result M=k. When g is one less than a multiple of 4, then the rows of a Hadamard matrix (Wallis, Street, and Wallis, 1972) is denoted by b_{ij}, and the elements of the difference set are $t_1, \cdots, t_M$, then

$$a^i_{tj} = \begin{cases} b_{ij} & 1\leqq i\leqq M,\; 1\leqq j\leqq M \\ O & \text{otherwise} \end{cases} \qquad (25)$$

Other similar designs are possible.

Discrete linear FM sequences (Chu, 1972) of various types have been studied. For example,

$$a^i_t = \rho^{it^2}, \; O\leqq t < L, \; O\leqq i < p(L) \qquad (26)$$

where L is an odd number, ρ is a primitive Lth root of unity, and p(L) is the smallest prime divisor of L. When L is prime,

$$L=p(L) \qquad (27)$$

and using Gaussian sums, it can be shown that

$$C\max = L^{-1/2} \qquad (28)$$

Rusults and Discussion

A common point of failure in the design of direct sequence systems lies in using codes that are too short (too few bits between repetitions) for projected interference levels. Worse yet, the shorter codes when multiplied with interference (especially narrowband interference) tend to produce correlations that are not at all noiselike. Therefore a synchro-nization detector or demodulator in such a system is likely to give surrisingly poor performance when it has been assumed (as is the usual case) that correlator output products due to interference are characteristically Gaussian.

It appears that there are many designs which asymptotically achieve the Welch bound on correlation as the sequence period L increases. How does one choose a CDMA signal set design from among the class of optimum designs?

If you are restricted to binary (±1) modulation, the obvious candidates are the Kasami sequences and the bent function sequences. The choice may be dictated by L which is 4^K-1 for Kasami sequences and 16^K-1 for bent sequences, k being an arbitrary integer in each case. The sequences are comparable in terms of implementation complexity for the same L but the bent sequence set has two distinct advantages :

(1) The Kasami sequences have a linear span on the same order of 3n when GF(2^n) is the basic field, while bent sequences apparently have linear spans which can nearly achieve Key's upper bound (Key, 1976),

$$\sum_{i=1}^{d} \binom{n}{i} \qquad (29)$$

where d is the degree of the bent function ($d \leqq n/4$ depending on the function chosen).

(2) All of the Kasami sequence are generated by the same hardware, with choice of sequence made by initializing register contents. Thus it is difficult to initialize a generator to begine producing a copy of a particular Kasami sequence at some arbitrary point within the sequence. On the other hand bent sequence generators have time controlled by a shift register and sequence selection performed by an independent setting. Hence bent sequence generators are easily set to produce a given sequence.

It is worth noting that Gold codes (Gold, 1967) which are now in use in several systems, e.g., Spilker, Jr. (1978) have the same drawbacks as Kasami sequences. In addition, while Gold codes are a larger collection ($M=2^n+1$) of binary sequences for the same period ($L=2^n-1$), they do not come close to achieving the Welch bound.

The ability to generate and correlate multiphase sequences cosiderably enlarges the variety of periods L for which optimum designs are known. The number of distinct phases which must be handled is a function of the number of sequences actually required as well as the perior length. For example the group character sequences of length $L=257$ are composed in general of 256th roots of unity, but the ith sequence in the set is made up of 256/gcd(256, i)th roots of unity. Hence in this case the 128th sequence is the binary quadratic residue sequence , the 64th and 192th sequences are composed of 4th roots of unity, and in general there are 2^{k-1} sequences using 2^kth roots of unity $k=1, \cdots, 7$, with the remainder using some primitive 256th roots of unity.

In comparing the group character sequences with the discrete linear FM sequences, one must consider the problem of mechanization for large L. The FM sequences have a relatively simple algorithm(26) for determining the phase of each bit. On the other hand group character sequence generation is based on computing the logarithm of t modulo $L-1$. In most cases this is a difficult computation (Pohlig and Hellman, 1978).

The main detractions of the difference set design are : (1) irregularity of the transmitter power, and (2) the requirement of phase coherence, despite the on-off nature of the signal. The orthogonal ±1 modulation of the non-zero pulses is easily achieved, especially when the number k of pulses per period is a power of 2.

Literatures Cited

Anderson, D.R. 1969. Periodic and partial correlation properties of sequences, TRW 7353. 1-01.

Baumert, L.D. 1971. Lecture notes in mathematics cyclic difference sets, Springer-Verlag.

Berlekamp, E.R. 1968. Algebraic code theory, NewYork, McGraw-Hill, Inc.

Chu, D.C. 1972. Polyphase codes with good periodic correlation properties, IEEE Trans. Inform. Theory, Vol. IT-18, pp. 531-532.

Gold, R. 1966. Study of correlation priperties of binary sequences, Magnavox Research Laboratories Report AFAL TR-66-234.

Gold, R. 1967. Optimal binary sequences for spread spectrum multiplexing, IEEE Trans. on Inform. Theory, Vol. IT−13, pp. 619−621.

Judge, W.T. 1962. Multiplexing using quasiorthogonal functions, AIEEE Winter General Mtg.

Kasami, T. 1966. Weight distribution formula for some class of cyclic codes, Coordinated Science Laboratory, Univ. of Illinois, Report R−285.

Key, E.L. 1967. An analysis on the structure and complexity of non-linear binary sequence generators, IEEE Trans. on Inform. Theory, Vol. IT−22, pp. 732−736i.

Lerner, R.M. 1961. Signals havng good correlation functions, IEEE WESCON Convention Record.

Olsen, J.D. 1977. Non-linear binary sequences with asymptotically optimum periodic crosscorrelation, Dissertation, Univ. of Southern Califonia.

Pohlig, S.C., and Hellman, M.E. 1978. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, IEEE Trans. on Inform. Theory, Vol. IT−24, pp. 106−110.

Pursley, M.B., and Darwate, D.V. 1977. Performance evaluation for phase-coded spread spectrum multipul-access communications, Vol. COM−25, pp. 800−803.

Roefs, H.F.A. 1977. Binary sequences for spread spectrum multiple-access communication, Coordinated Science Laboratory, Univ. of Illinois, Report R−785.

Rothaus, O.S. 1976. On bent function, Journal of Combinational Theory, Series A20, pp. 300−305.

Scholtz, R.A., and Welch, L.R. 1978. Group characters, sequences with good correlation properties, IEEE Trans. on Inform. Theory, Vol. IT−24, pp. 537−545.

Spilker, Jr., J.J. 1978. GPS signal structure and performance charateristics, Navigation, Vol. 25, pp. 121−146.

Wallis, W.D., Street, A.D., and Wallis, J.S. 1972. Lecture notes in mathematics combinatorics : Room Squares, Sum-Free Sets, Hadamard matrices, Springer-Varlag.

Welch, L.R. 1974. Lower bounds on the maximum crosscorrelation of signals, IEEE Trans, on Inform. Theory, Vol. IT−20, pp. 397−399.

〈國文抄錄〉

Spread Spectrum 技術을 利用한 最適 Code-Division Multiple-Access Codes

이 硏究는 Welch 境界를 거의 이룰 수 있는 것으로 알려진 여러가지 code-division multiple-access 通信系에서 spread spectrum을 利用하는 sequence들을 調査評價하였다. 특히 設計들의 **利用性이** 多樣하여 決定要素에 따라 適切하고 便利하게 設計할 수 있다.