

From \mathbb{Z}_4 sequences to QAM sequences

Serdar Boztaş

RMIT University, Melbourne, Australia

**CIMPA WORKSHOP ON SEQUENCES
METU, ANKARA, TURKEY**

August 2008

Outline of Talk

- Introduction to Modulations and Sequences
- The QAM Alphabet and Bounds on QAM signals
- Constructions of Sequences for QAM
- Conclusions

Definitions

Let E_m^n be the set of vectors of length n over the alphabet

$$E_m = \{1, \xi, \xi^2, \dots, \xi^{m-1} \mid \xi = e^{2\pi i/m}\}.$$

Throughout this paper m is an arbitrary positive integer satisfying $m \geq 2$. For any $x = (x_0, x_1, \dots, x_{n-1}) \in E_m^n$ and $y = (y_0, y_1, \dots, y_{n-1}) \in E_m^n$ the **periodic** crosscorrelation function $\theta(x, y; l)$ is defined as follows:

$$\theta(x, y; l) = \sum_{j=0}^{n-1} x_j \overline{y_{j+l}}, \quad l = 0, 1, \dots, n-1 \quad (1)$$

where \bar{z} denotes the complex conjugate of z , and the addition in the subscript of y_{j+l} is modulo n .

Correlations

The performance of a code $C \subseteq E_m^n$ is characterized by

- (a) the maximum periodic crosscorrelation,
- (b) maximum periodic nontrivial autocorrelation, and
- (c) maximum periodic correlation magnitudes given below:

$$\theta_c(C) = \max\{|\theta(x, y; l)| : x, y \in C, x \neq y, l = 0, 1, \dots, n - 1\},$$

$$\theta_a(C) = \max\{|\theta(x, x; l)| : x \in C, l = 1, \dots, n - 1\},$$

$$\theta(C) = \max\{\theta_a(C), \theta_c(C)\}.$$

In general we want these to be **as small as possible** for given code parameters, namely $|C|$ and n and m .

Lower Bounds

The first lower bound on $\theta(C)$ is due to Welch and applies to arbitrary complex sequences with constant norm, and hence to $C \subseteq E_m^n$. A lower bound on $\theta_a(C)$ for such sequences was also derived by Welch. Another important lower bound on $\theta(C)$ for $C \subseteq E_m^n$ is that of Sidelnikov, which is usually slightly better than Welch's but much more complicated.

The class of sequence families which are subsets of E_m^n , for some m are by far the best understood from the point of view of sequence design.

Remark: A sequence family is a **cyclically distinct** subset of E_m^n while the corresponding code C includes all cyclic shifts of each member of the sequence family.

Correlation Example

To clarify correlations, if we have the sequence $s = (0, 1, 1, 0, 1)$ over $GF(2)$ the actual transmitted sequence is $\mathbf{x} = (1, -1, -1, 1, -1)$ and it is this second sequence that is used to compute correlations—here we show the autocorrelation of \mathbf{x} :

\mathbf{x}	1	-1	-1	1	-1	1	-1	-1	1	-1	l	$\theta(x, x; l)$
$T^0(\mathbf{x})$	<u>1</u>	<u>-1</u>	<u>-1</u>	<u>1</u>	<u>-1</u>						0	$5 - 0 = +5$
$T^1(\mathbf{x})$		1	<u>-1</u>	-1	1	-1					1	$1 - 4 = -3$
$T^2(\mathbf{x})$			1	-1	<u>-1</u>	<u>1</u>	<u>-1</u>				2	$3 - 2 = +1$
$T^3(\mathbf{x})$				<u>1</u>	<u>-1</u>	-1	1	<u>-1</u>			3	$3 - 2 = +1$
$T^4(\mathbf{x})$					1	-1	<u>-1</u>	1	-1		4	$1 - 4 = -3$
$T^5(\mathbf{x})$						<u>1</u>	<u>-1</u>	<u>-1</u>	<u>1</u>	<u>-1</u>	0	$5 - 0 = +5$

Homework: $\theta(x, x; l) = \text{_____} - \text{_____} d_H(\mathbf{x}, \text{_____})$

Why is this a Hard problem?

Consider a code $C \subseteq E_2^n$ which is a collection of n -dimensional real vectors with entries ± 1 . Since they all have norm \sqrt{n} they lie on the surface of a sphere in \mathbf{R}^n . The code design problem is to maximize the number of points on this surface subject to an upper bound on the maximum pairwise (Euclidean) inner product (which is the same as the correlation between two codewords).

Sequence design is even harder, since whenever you place a point \mathbf{x} on the surface of the sphere you also have to include the points corresponding to all its cyclic shifts $(T^l(\mathbf{x}), l = 1, \dots, n - 1)$ so geometric problem is even harder to control.

Introducing m -Sequences

Consider the sequence $\mathbf{x} = ((-1)^{\text{tr}(\alpha^t)})_{t=0}^{2^k-2}$ where $\text{tr} : GF(2^k) \rightarrow GF(2)$ and α is a primitive element in $GF(2^k)$. Together with all its cyclic shifts $T^l \mathbf{x} = ((-1)^{\text{tr}(\alpha^{t+l})})_{t=0}^{2^k-2}$ it forms a family of $2^k - 1$ sequences where $\theta(x, x; l) = -1$ for all l not divisible by the period $2^k - 1$.

This is because the sum

$\theta(x, x; l) = \sum_{t=0}^{2^k-2} (-1)^{\text{tr}(\alpha^{t+l})} (-1)^{\text{tr}(\alpha^t)}$ is equal to

$\theta(x, x; l) = \sum_{t=0}^{2^k-2} (-1)^{\text{tr}((1+\alpha^l)\alpha^t)}$ which is the same as $\sum_{u \in GF(2^k)^*} (-1)^{\text{tr}(u)}$ but this sum is simply a sum of a nontrivial character over all nonzero elements of $GF(2^k)$.

Gold Sequences

For $m = 2$ and $n = 2^k - 1$, $k \geq 3$, and k odd, the sequence family due to Gold with $(n+2)$ sequences is optimal with $\theta(C) = 1 + \sqrt{2(n+1)}$. It uses m -sequences and their decimations.

The binary Gold family over E_2^n is given by the sequences below and all their cyclic shifts, i.e.,
 $\mathcal{G} = \{(s_0(t))_{t=0}^{n-1}, (s_1(t))_{t=0}^{n-1}, \dots, (s_{n+1}(t))_{t=0}^{n-1}\}$, where

$$\begin{aligned} s_\infty(t) &= (-1)^{\text{tr}(\alpha^t)} \\ s_i(t) &= (-1)^{\text{tr}(\alpha^{t+i}) + \text{tr}(\alpha^{3t})}, \quad i = 0, \dots, n \end{aligned}$$

For this case, the Welch and Sidelnikov bounds give $\theta(C) \geq \sqrt{2n}$ so the Gold family is nearly optimal and asymptotically optimal.

Gold Sequences

Instead of $s_i(t) = (-1)^{\text{tr}(\alpha^{t+i}) + \text{tr}(\alpha^{3t})}$ as in Gold's original design it is possible to use $\text{tr}(\alpha^{t+i}) + \text{tr}(\alpha^{(2^u+1)t})$ in the exponent, provided $\text{gcd}(k, u) = 1$. For the relationship to a certain binary quadratic form if the formulation is shifted to Boolean functions and the determination of the rank of a related symplectic form to compute $\theta(C)$, see McWilliams and Sloane.

The question of what other exponents d yield good correlation distributions for function $\text{tr}(\alpha^{t+i}) + \text{tr}(\alpha^{dt})$ has long been investigated by a large number of authors and there is still more work to do here. Niho, Charpin, Zinoviev, Carlet are some of the names that provided highlights.

Better than Gold

Boztaş-Kumar have designed an E_2^n sequence family ($n = 2^k - 1$, k odd) which has exactly the same parameters (including correlation distribution and thus $\theta(C)$) as the Gold family but is not linear (which is an advantage in some security-related applications). The definition is given below

$$s_\infty(t) = (-1)^{\text{tr}(\alpha^t)}$$
$$s_i(t) = (-1)^{\text{tr}(\alpha^{t+i}) + \sum_{j=1}^{(k-1)/2} \text{tr}(\alpha^{(2^j+1)t})}, \quad i = 0, \dots, n$$

Note that including all the quadratic exponents preserves the correlation and improves the nonlinearity of the sequences.

Better than Gold

As discussed by other speakers' the Z_4 -linearity of Kerdock and Preparata codes was proved in 1994. Prior to that work, Solé, Boztas-Hammons-Kumar, and Udaya independently discovered Family A, which is an optimal set of sequences in E_4^n and gives rise to a code if all the cyclic shifts of its cyclically distinct members are included.

Family A delivers the promise of the lower bounds by reducing $\theta(C)$ by a factor of $\sqrt{2}$. This is equivalent to having the same signal-to-interference ratio (and thus the same performance) in a CDMA mobile phone system when the received signal strength from the desired user is reduced by 3 dB, i.e., reduced power/original power = $(1/\sqrt{2}) \approx 0.707$, about a 30 % reduction.

Family A

For $m = 4$ and $n = 2^k - 2$, $k \geq 3$, if k is odd, the so-called *Family A* is optimal with $\theta(C) = 1 + \sqrt{n+1}$. The definition of Family A using Galois rings will be given below:

We denote the Galois ring as $R = GR(4, k)$ and note that it is a Galois extension of Z_4 , defined by $R = Z_4[\beta]$ where β has multiplicative order $2^k - 1$ and is a root of a primitive basic irreducible polynomial (i.e., a basic irreducible polynomial whose modulo 2 reduction is a primitive polynomial over Z_2). It is always possible to construct such a polynomial. Note that the ring R contains 4^k elements, and $R = \langle 1, \beta, \dots, \beta^{k-1} \rangle$ as a Z_4 -module.

Family A

Every element $c \in R$ has a unique 2-adic representation $c = a + 2b$, where a, b belong to the Teichmuller set

$$\mathcal{T} = \{0, 1, \beta, \dots, \beta^{2^k-2}\}.$$

Denote the modulo 2 reduction function by μ and extend it to polynomials, then $\mu(\mathcal{T}) = \{0, 1, \alpha, \dots, \alpha^{2^k-2}\} = GF(2^k)$. The set of invertible elements of R are denoted $R^* = R \setminus 2R$ where $2R$ is the set of zero divisors and is the unique maximal ideal in R . Every element in R^* has a unique representation of the form $\beta^r(1 + 2z)$, $0 \leq r \leq 2^k - 2, z \in \mathcal{T}$.

Family A

Also, R^* is a multiplicative group of order $2^k(2^k - 1)$ which is a direct product $G_1 \times \mathcal{E}$ where G_1 is a cyclic group of order $2^k - 1$ (made up of the nonzero elements in the Teichmüller set) generated by β and \mathcal{E} is made up of elements of the form $1 + 2t$ where $t \in T$.

The *Frobenius map* from R to R is the ring automorphism that takes any element $c = a + 2b$ in the 2-adic representation to the element $c^f = a^2 + 2b^2$ and it generates the Galois group of R over Z_4 with f^k the identity map. The *Trace map* from R to Z_4 is defined by

$$T(c) = c + c^f + c^{f^2} + \cdots + c^{f^{k-1}}, \quad c \in R.$$

Family A

The trace is onto and has nice equidistribution properties. If we let $f_2(c) = c^2$ be the squaring map defined on the finite field $GF(2^k)$ then the finite field trace is given by

$$tr(c) = c + c^2 + c^{2^2} + \cdots + c^{2^{k-1}}, \quad c \in GF(2^k),$$

and the following commutativity relationships hold:

$$\mu \circ f = f_2 \circ \mu, \quad \mu \circ T = tr \circ \mu.$$

Family A

A q -ary sequence family made up of M cyclically distinct sequences of length n can be defined to be the collection of vectors

$$\{\mathbf{s}_1, \dots, \mathbf{s}_M\}, \quad \mathbf{s}_i \in Z_q^n, \quad 1 \leq i \leq M$$

with $\mathbf{s}_1 = (s_1(0), \dots, s_1(n-1))$, where Z_q is the ring of integers modulo q . Here we restrict ourselves to quaternary sequences, i.e., $q = 4$. The (periodic) correlation function between sequences i and j at relative shift l is defined as

$$C_{i,j}(l) = \sum_{t=0}^{n-1} \omega^{s_i(t \oplus l) - s_j(t)}$$

Family A

Here $\omega = \exp(2\pi i/4) = \sqrt{-1}$ is a primitive fourth root of unity and \oplus denotes addition modulo n . Clearly

$$C_{i,j}(l) = \sum_{t=0}^{n-1} \omega^{s_i(t \oplus l) - s_j(t)} = \theta(\mathbf{x}_i, \mathbf{x}_j; l)$$

where

$$\mathbf{x}_i = (\omega^{s_i(0)}, \omega^{s_i(1)}, \dots, \omega^{s_i(n-1)}),$$

etc. Hence we are working in E_4^n .

We shall denote the set of cyclically distinct sequences over Z_4 which obey a common linear recurrence whose characteristic polynomial is $f \in Z_4[x]$ as $S(f)$.

Family A

Let f be a primitive basic irreducible polynomial of degree k , k odd, over the ring $Z_4[x]$. Then Family A is $S(f)$ and comprises a set of $M = 2^k + 1$ cyclically distinct sequences over Z_4 with length $n = 2^k - 1$.

Each element s_i of *Family A* can be expressed as $s_i(t) = T(\gamma\beta^t)$ where β is a generator of the Teichmuller set, and $\gamma \neq 0$. In fact the enumeration of representatives

$$\Gamma_\nu = \{2\nu\} \cup \{(1 - \beta^j)\nu : j = \infty, 0, 1, \dots, 2^k - 2\}$$

can be used to enumerate the cyclically distinct elements in *Family A*, since each member γ_i , $1 \leq i \leq 2^k + 1$ of Γ_ν gives a distinct sequence $s_i(t) = T(\gamma_i\beta^t)$.

Family A Since

$$\theta(\mathbf{x}_i, \mathbf{x}_j; l) = \sum_{t=0}^{n-1} \omega^{s_i(t \oplus l) - s_j(t)} = \sum_{t=0}^{n-1} \omega^{T([\gamma_i \beta^l - \gamma_j] \beta^t)}$$

The complete full period correlation distribution for Family A is obtained by considering the distribution of values taken by sums of the form

$$\Gamma(\gamma) = \sum_{x \in G_1} \omega^{T(\gamma x)} = \sum_{t=0}^{2^n - 2} \omega^{T(\gamma \beta^t)},$$

as γ ranges over the ring R , where we count the solutions of $\gamma = \gamma_i \beta^l - \gamma_j$.

Theorem (Boztaş-Hammons-Kumar): For *Family A* we have:

Family A

1. If $k = 2s + 1$, then

$$\theta(i, j; l) = \left\{ \begin{array}{ll} 2^k - 1, & 2^k + 1 \text{ times,} \\ -1, & 2^{2k} - 2 \text{ times,} \\ -1 + 2^s + \omega 2^s, & (2^{k-2} + 2^{s-1}) \\ & \cdot (2^{2k} - 2) \text{ times,} \\ -1 + 2^s - \omega 2^s, & (2^{k-2} + 2^{s-1}) \\ & \cdot (2^{2k} - 2) \text{ times,} \\ -1 - 2^s + \omega 2^s, & (2^{k-2} - 2^{s-1}) \\ & \cdot (2^{2k} - 2) \text{ times,} \\ -1 - 2^s - \omega 2^s, & (2^{k-2} - 2^{s-1}) \\ & \cdot (2^{2k} - 2) \text{ times.} \end{array} \right.$$

2. If $k = 2s$, then

$$\theta(i, j; l) = \begin{cases} 2^k - 1, & 2^k + 1 \text{ times,} \\ -1, & 2^{2k} - 2 \text{ times,} \\ -1 + 2^s, & (2^{k-2} + 2^{s-1}) \\ & \cdot (2^{2k} - 2) \text{ times,} \\ -1 - 2^s, & (2^{k-2} + 2^{s-1}) \\ & \cdot (2^{2k} - 2) \text{ times,} \\ -1 + \omega 2^s, & 2^{k-2}(2^{2k} - 2) \text{ times,} \\ -1 - \omega 2^s, & 2^{k-2}(2^{2k} - 2) \text{ times.} \end{cases}$$

Family A: Correlation Proof

Let each $x \in R$ be associated with the vector $\mathbf{V}_x = (T(x), T(x\beta), T(x\beta^2), \dots, T(x\beta^{k-1}))$. Since $R = \langle 1, \beta, \dots, \beta^{k-1} \rangle$ as a \mathbb{Z}_4 -module and T is nontrivial this sets up a 1-to-1 correspondence between R and k -tuples over \mathbb{Z}_4 . The Galois Ring trace T is equidistributed and thus each component of \mathbf{V}_x takes on each value in \mathbb{Z}_4 equally often as x ranges over the Galois Ring R . Also each r -tuple having exclusively 0 and 2 entries only appears when $x \in R \setminus R^*$, i.e., when x is a zero divisor, and in particular each entry takes on the value 0 and 2 equally often in this case. Thus we have

$$\sum_{x \in R} \omega^{T(x)} = \sum_{x \in R \setminus R^*} \omega^{T(x)} = \sum_{x \in R^*} \omega^{T(x)} = 0$$

Family A: Correlation Proof

We also can obtain easily

$$\sum_{x \in R} (-1)^{T(x)} = 0,$$

and

$$\sum_{x \in R \setminus R^*} (-1)^{T(x)} = - \sum_{x \in R^*} (-1)^{T(x)} = 2^k.$$

Hint: $x \in R \setminus R^* \Rightarrow T(x) = 0$ or 2 . Since $\mu f(x) = \prod_{i=0}^{k-1} (x - \alpha^{2^i})$, is primitive over $GF(2^k)$ and its Hensel lift $f(x) = \prod_{i=0}^{k-1} (x - \beta^{2^i})$ determines the recurrence satisfied by Family A sequences, we conclude that every sequence in Family A can be written as $s(t) = T(\gamma\beta^t)$, for some $\gamma \in R \setminus \{0\}$.

Family A: Correlation Proof

The family A sequences $s(t) = T(\gamma\beta^t)$, for which γ is a zero divisor turn out to be equal to $s(t) = 2\text{tr}(\nu\alpha^t)$ (where $2\nu = \gamma$) which yields a phase of the maximum length sequence $\text{tr}(\alpha^t)$ defined on the finite field $GF(2^k)$ and $\omega^{T(\gamma\beta^t)} = (-1)^{\text{tr}(\nu\alpha^t)}$.

The set of cyclically distinct sequences in Family A can be determined to be $s_i(t) = T(\gamma\beta^t)$ where γ ranges over

$$\Gamma_\nu = \{2\nu\} \cup \{(1 - \beta^j)\nu : j = \infty, 0, 1, \dots, 2^k - 2\}.$$

Family A: Correlation Proof

The exponential sum $\Gamma(\gamma) = \sum_{u \in G_1} \omega^{T(\gamma u)} = \sum_{t=0}^{2^n-2} \omega^{T(\gamma \beta^t)}$ satisfies:

- ◇ If $\gamma \in R^*$ then $|1 + \Gamma(\gamma)|^2 = 2^k$
- ◇ If $\gamma \in R \setminus R^*$ and $\gamma \neq 0$ then $\Gamma(\gamma) = -1$.

Proof

$$|\Gamma(\gamma)|^2 = \sum_{t=0}^{2^k-2} \sum_{t'=0}^{2^k-2} \omega^{T(\gamma(\beta^t - \beta^{t'}))} = \sum_{t=0}^{2^k-2} \sum_{u \in G_1} \omega^{\gamma(1-\beta^t)u}$$

(G_1 is the group formed by nonzero elements of the Teichmuller set)

$$|\Gamma(\gamma)|^2 = \omega^{T(0)} + \sum_{t=1}^{2^k-2} \sum_{u \in G_1} \omega^{\gamma(1-\beta^t)u}$$

and since cosets of G_1 in R^* of the form $(1 - \beta^t)G_1$ 'miss' $\pm G_1$

$$|\Gamma(\gamma)|^2 = (2^k - 1) + \sum_{u \in R^*} \omega^{T(u)} - \Gamma(\gamma) - \Gamma(\gamma)^*.$$

Family A: Correlation Proof

We thus have

$$\Gamma(\gamma)\Gamma(\gamma)^* + \Gamma(\gamma) + \Gamma(\gamma)^* + 1 = |\Gamma(\gamma) + 1|^2 = 2^r + \underbrace{\sum_{u \in R^*} \omega^{T(u)}}_0.$$

For $\gamma \neq 0$ a nonunit in R we have

$$\Gamma(\gamma) = \sum_{u \in G_1} \omega^{T(\gamma u)} = \sum_{t=0}^{2^k-2} \omega^{T(2\nu\beta^t)} = \sum_{t=0}^{2^k-2} (-1)^{\text{tr}(\mu(\nu)\alpha^t)}$$

where $2\nu = \gamma$ and $\alpha = \mu(\beta)$ is primitive in $GF(2^k)$.

When $\gamma \in R^*$ since $\Gamma(\gamma)$ has integer real and imaginary part we have (proof by induction):

$$\text{If } k = 2s + 1 \text{ then } \Gamma(\gamma) = -1 \pm 2^s \pm \omega 2^s$$

$$\text{If } k = 2s \text{ then } \Gamma(\gamma) = -1 \pm 2^s \text{ or } \Gamma(\gamma) = -1 \pm \omega 2^s$$

Family A: Correlation Proof

To obtain the complete correlation distribution for Family A, since

$$\theta(\mathbf{x}_i, \mathbf{x}_j; l) = \sum_{t=0}^{n-1} \omega^{s_i(t \oplus l) - s_j(t)} = \sum_{t=0}^{n-1} \omega^{T([\gamma_i \beta^l - \gamma_j] \beta^t)}$$

we need to determine the number of solutions (i, j, l) to the equation

$$\gamma_i \beta^l - \gamma_j = \gamma$$

for each value of γ and then use the distribution of $G(\gamma) = \sum_{t=0}^{n-1} \omega^{T(\gamma \beta^t)}$ which can be obtained separately but we have no time for this.

Family A and Others

Family A is optimal with respect to Welch and Levenshtein bounds only for the case k odd.

For $m = p$, an odd prime, the family due to Kumar and Moreno with $M = n(n + 1)$ is optimal with $n = p^k - 1$, and $\theta(C) = 1 + \sqrt{n + 1}$.

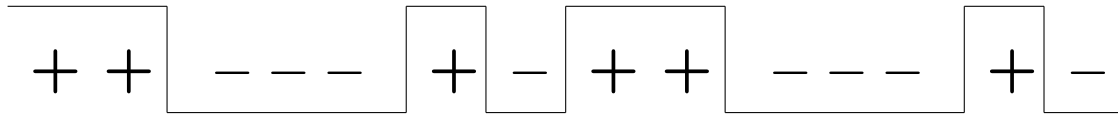
Kumar, Calderbank, Helleseth et. al. have extended Family A to a larger family $S(2)$ (of which Family A is a subset) which has been adopted in wireless telephone standards.

In wireless, some alphabets which are quite different than E_m^n are of interest due to practical constraints such as bandwidth efficiency and noise resistance. Thus we consider QAM based sequences in a later talk.

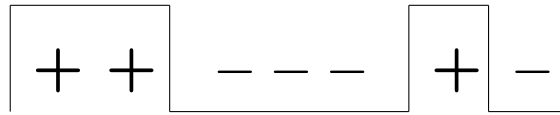
Correlations: Periodic, Aperiodic and Partial

Pseudorandom sequences such as Family A are used in a variety of applications. Depending on the application different correlations, or more than one type of correlation may be of interest. These different correlations are intimately related to each other.

Type of Correlation	Application
Periodic Correlation	Wideband CDMA and other wireless communications
Aperiodic Correlation	Radar and Low Probability of Intercept Communications
Partial Period Correlation	Wideband CDMA and other wireless (acquisition stage)
Hamming Correlation	Frequency Hopping CDMA



spread signal($\times 1$)

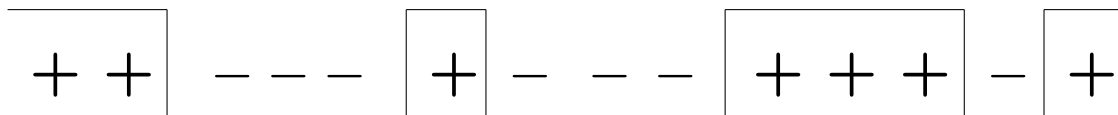


shifted signal

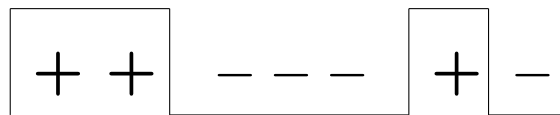
$\theta(x,x;2)=-1$



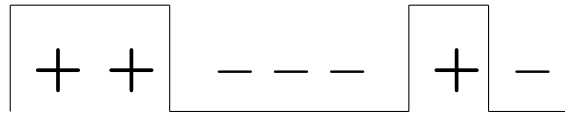
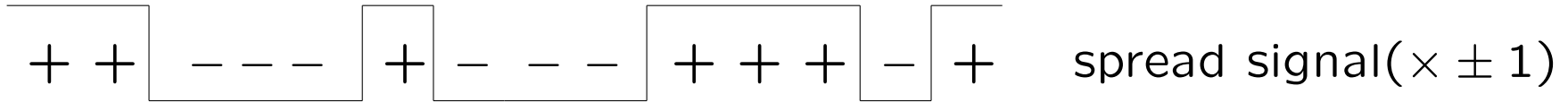
data signal (± 1)



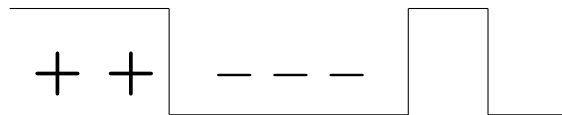
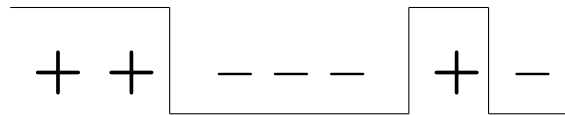
spread signal($\times \pm 1$)



NOT a periodic corr.



NOT periodic but a difference of two APERIODIC correlations



Correlations: Periodic, Aperiodic and Partial

There are a large number of problems in communications and related fields which require the construction of signal sets with the following properties:

The signals should be easily distinguishable from a shifted version of themselves.

The signals should be easily distinguishable from (possibly shifted) versions of other signals in the signal set.

The first property is important in ranging, radar, and Low Probability of Intercept spread spectrum. The second is important in CDMA, and in radar tracking multiple targets simultaneously.

Correlations: Periodic, Aperiodic and Partial

Define the aperiodic crosscorrelation function between two complex sequences of same length n as

$$\theta^{(a)}(\mathbf{x}, \mathbf{y}; l) = \begin{cases} \sum_{j=0}^{n-l} x_j \overline{y_{j+l}} & 0 \leq l \leq n-1 \\ \sum_{j=0}^{n-l} x_{j-l} \overline{y_j} & -n+1 \leq l \leq -1 \\ 0 & \text{else} \end{cases}$$

It turns out that the aperiodic correlation plays a large part in performance not only of radar systems but also communication systems.

Correlations: Periodic, Aperiodic and Partial

Given the sequence $x = (1, 1, 1, -1, 1)$ the aperiodic autocorrelation of x is:

					l	$\theta^{(a)}(x, x; l)$								
				1	1	1	-1	1						
1	1	1	-1	1						-4	1			
	1	1	1	-1	1					-3	0			
		1	1	1	-1	1				-2	1			
			1	1	1	-1	1			-1	0			
				1	1	1	-1	1		0	5			
					1	1	1	-1	1	1	0			
						1	1	1	1	2	1			
							1	1	1	-1	1	3	0	
								1	1	1	-1	1	4	1

Correlations: Periodic, Aperiodic and Partial

Note that we have

$$\theta(x, y; l) = \theta^{(a)}(l) + \theta^{(a)}(n - l), \text{ for } 0 \leq l \leq n - 1,$$

and

$$\theta(x, y; N - l) = \theta^{(a)}(N - l) + \theta^{(a)}(-l), \text{ for } 0 \leq N - l \leq n - 1.$$

It is, unfortunately, much harder to design sequences with good aperiodic correlation, though it plays a very large part in system performance.

Correlations: Periodic, Aperiodic and Partial

Note that $\theta^{(a)}(x, x; l) = \theta^{(a)}(x, x; -l)$ for $l \neq 0$. If $l \neq 0 \Rightarrow |\theta^{(a)}(x, x; l)| \leq 1$ for a binary sequence \mathbf{x} then we say that \mathbf{x} is a Barker sequence. There are only a few Barker sequences known (they are extensively used in Radar). The longest Barker sequence has length 13: $\mathbf{x} = (1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1)$.

Conjecture: There are no more Barker sequences.

There is lots of experimental evidence for this, but no proof.

Correlations: Periodic, Aperiodic and Partial

Since the Barker Conjecture (first informally stated by Turyn) has proved intractable, various authors have considered related problems:

Minimize the maximum absolute value of the sidelobe

$$\min_{\mathbf{x} \in \{\pm 1\}^n} \max_{0 < l < n-1} |\theta^{(a)}(x, x; l)|$$

Minimize the sum of squares of the sidelobes

$$\min_{\mathbf{x} \in \{\pm 1\}^n} \sum_{l=0}^{n-1} |\theta^{(a)}(x, x; l)|^2$$

Aperiodic Correlation of Galois Ring Sequences

Other approaches include:

Use more general alphabets rather than binary.

Use a pair of sequences for which the **sum** of their autocorrelations add to zero for $l \neq 0$.

Since we want to focus on algebraic problems, we shall consider an algebraic approach to aperiodic correlation for Galois ring sequences.

Aperiodic Correlation of Galois Ring Sequences

We focus on the Galois Ring sequences from Family A which arise from units in the Galois Ring. It is natural to define a Galois ring m -sequence M^ν associated with a unit $\nu \in GR(p^k, r)$ by using the Galois ring trace function $Tr(\cdot)$ defined from $GR(p^k, r)$ to \mathbf{Z}_{p^k} as

$$M^\nu = (M_i^\nu) = (Tr(\nu\alpha^i) : 0 \leq i < N),$$

where $N = p^r - 1$. The cyclically distinct m -sequences are given by the set

$$\{M^p\} \cup \{M^\nu : \nu = 1 + \sum_{j=1}^{k-1} p^j \hat{\nu}_j, \hat{\nu}_j \in \mathcal{T}\},$$

where \mathcal{T} is the *Teichmuller set* of the Galois ring $GR(p^k, r)$.

Aperiodic Correlation of Galois Ring Sequences

\mathcal{T} contains all the powers of the primitive element α and the zero element, i.e.,

$$\mathcal{T} = \{0, 1, \alpha, \dots, \alpha^{N-1}\}.$$

This set shares many properties of finite fields. Its nonzero elements are generated by α and it is closed under multiplication. However, *it is not closed under addition*. Note that the sequence M^p is isomorphic to a $\text{GF}(p)$ m -sequence. Hence there are $(p^{kr} - 1)/(p^r - 1)$ cyclically distinct m -sequences over \mathbf{Z}_p .

Aperiodic Correlation of Galois Ring Sequences

We aim for upper bounds on the aperiodic correlation of the m -sequences M^ν over \mathbf{Z}_{p^k} . We follow the method adopted by Sarwate in 1984 to derive the bound, together with a bound on Gauss like sums or Fourier transform values of these sequences. Let Ω_N be a complex primitive N^{th} root of unity. Then the Gauss sum or Fourier transform $\hat{S} = (\hat{S}_c)$ of an arbitrary q -ary polyphase sequence $S = (S_i) = (\omega^{m_i})$ is defined as

$$\hat{S}_c = \sum_{i=0}^{N-1} \omega^{m_i} \Omega_N^{ic}, \quad 0 \leq c < N.$$

The values \hat{S}_c are Fourier transform values.

Aperiodic Correlation of Galois Ring Sequences

We have

$$S_i = N^{-1} \sum_{c=0}^{N-1} \hat{S}_c \Omega \frac{-ic}{N}, \quad 0 \leq i < N.$$

In this section we will consider only quadriphase sequences derived from m -sequences over \mathbf{Z}_4 . Let $\alpha \in GR(4, r)$, r a positive integer, be a primitive element of the multiplicative order $N = 2^r - 1$. The cyclically distinct quadriphase m -sequences of length N are given by the set

$$\{(\omega^{Tr(2\alpha^i)})\} \cup \{(\omega^{Tr(\nu\alpha^i)}) : \nu = 1 + 2\hat{\nu}, \hat{\nu} \in \mathcal{T}\}.$$

Aperiodic Correlation of Galois Ring Sequences

Note that S^2 is a biphasic m -sequence and it is well known that \hat{S}_c^2 takes the value of $\sqrt{N+1}$ when $c \neq 0$ and takes the value of -1 when $c = 0$. The proof uses the fact that all the phases of binary m -sequences form an Abelian group under pointwise addition. When $\nu \in \mathcal{T}$, this is not true, and hence we cannot easily bound the transform values. When $c = 0$, \hat{S}_0^ν is simply the sum of all quadriphase symbols in S^ν . This value has a magnitude $\approx \sqrt{N+1}$ as shown by Boztaş-Hammons-Kumar and others. To bound the rest of the values we use the Cauchy-Schwartz inequality:

Lemma 1 If V is a real or complex inner product space, then, for all $x, y \in V$, we have $|\langle x, y \rangle| \leq \|x\| \|y\|$,

Aperiodic Correlation of Galois Ring Sequences

Here $\| \cdot \|$ denotes the norm of the space which is obtained from the inner product $\langle \cdot, \cdot \rangle$ defined on V via $\|x\| = \sqrt{\langle x, x \rangle}$. Equality holds if and only if one of the vectors x, y is a scalar multiple of the other. By utilizing the Cauchy-Schwarz inequality we prove the following result.

Theorem 1 The squared magnitudes of the Fourier coefficients of S^ν satisfy the following inequality

$$|\hat{S}_k^\nu|^2 \leq N(1 + \sqrt{N+1}), \quad 1 \leq k < N.$$

Proof

$$|\hat{S}_k^\nu|^2 = \sum_{i=0}^{N-1} \omega^{\text{Tr}(\nu\alpha^i)} \Omega \frac{ik}{N} \sum_{m=0}^{N-1} \omega^{\text{Tr}(-\nu\alpha^m)} \Omega \frac{-mk}{N}$$

Aperiodic Correlation of Galois Ring Sequences

Thus,

$$|\hat{S}_k^\nu|^2 = \sum_{i=0}^{N-1} \sum_{m=0}^{N-1} \omega^{\text{Tr}(\nu(\alpha^i - \alpha^m))} \Omega_N^{k(i-m)}$$

By making the transformation $(i - m) = \tau$,

$$|\hat{S}_k^\nu|^2 = \sum_{\tau=0}^{N-1} \theta_\nu(N - \tau) \Omega_N^{\tau k},$$

where $\theta_\nu(N - \tau)$ is the $(N - \tau)^{\text{th}}$ autocorrelation of S^ν .

Then

$$|\hat{S}_k^\nu|^2 = \theta_\nu(0) - \theta_\nu(1) + \theta_\nu(1) + \sum_{\tau=1}^{N-1} \theta_\nu(N - \tau) \Omega_N^{\tau k}, \quad (2)$$

Aperiodic Correlation of Galois Ring Sequences

It has been shown for Family A that:

$$|\theta_\nu(l)| = \begin{cases} N, & l \equiv 0 \text{ modulo } N \\ \sqrt{N+1}, & \text{otherwise.} \end{cases} \quad (3)$$

Also $|\Omega_N^\tau| = 1$, and after using Lemma 1 to bound the last term in (2), we have

$$\begin{aligned} |\hat{S}_k^\nu|^2 &\leq N - \sqrt{N+1} + \sqrt{N(N+1)}\sqrt{N} \\ &\leq N(1 + \sqrt{N+1}) \end{aligned}$$

which proves the theorem.

Aperiodic Correlation of Galois Ring Sequences

By using the actual values of $\theta(i)$ we can improve the bound slightly. We need some results on the following exponential sums. For any integer c , let $\Gamma(l, c) = \sum_{k=0}^{N-1-l} \Omega \frac{ck}{N}$, $0 \leq l \leq N - 1$. Then define $\Gamma_{l,N}$ as

$$\Gamma_{l,N} = N^{-1} \sum_{c=1}^{N-1} |\Gamma(l, c)|.$$

We have the following lemma proved in Sarwate using a method given by Vinogradov.

Lemma 2 $\Gamma_{l,N} < (2/\pi) \ln(4N/\pi)$, for $0 \leq l \leq N - 1$

Aperiodic Correlation of Galois Ring Sequences

Sarwate also shown that for $N > 6$, the above bound can be improved to

$$\Gamma_{l,N} < (2/\pi) \ln(4e^{\pi/3}N/3\pi) \quad (4)$$

which reduces the constant in the argument of the logarithm from 1.273.. to 1.209...

Let $\Delta(\nu_1, \nu_2, l, c)$ denote the cross ambiguity function of two m -sequences M^{ν_1} and M^{ν_2} , where

$$\Delta(\nu_1, \nu_2, l, c) = \sum_{i=0}^{N-1} \omega^{M_i^{\nu_1} - M_{i+l}^{\nu_2}} \Omega_N^{ic}, 0 \leq c < N. \quad (5)$$

By using Theorem 1 we prove the following:

Aperiodic Correlation of Galois Ring Sequences

Lemma 3 For $c \neq 0$ and either $\nu_1 \neq \nu_2$, any l or $\nu_1 = \nu_2, l \neq 0$ modulo N ,

$$|\Delta(\nu_1, \nu_2, l, c)| = \sqrt{N(1 + \sqrt{N+1})}.$$

Proof We use the fact that m -sequences are closed under pointwise addition or subtraction. Then $\Delta(\nu_1, \nu_2, l, c)$ is equal to the Gauss sum of an appropriate m -sequence. The result then follows from Theorem 1.

We now give the upper bound on the aperiodic cross-correlation function magnitudes by making use of these Lemmas along the lines of the proof given by Sarwate.

Theorem 2

$$|C_{1,2}(l)| < \sqrt{(N+1)} + (2/\pi)\sqrt{N(1+\sqrt{N+1})} \ln(4e^{\pi/3}N/3\pi),$$

for $l \neq 0$

Proof In view of the definition of aperiodic crosscorrelation on slide 33 and

$$\theta_{1,1}^{(a)}(0) = \theta_{2,2}^{(a)}(0) = N \text{ and that } \theta_{1,2}^{(a)}(l) = \theta_{1,2}^{(a)}(-l).$$

it is sufficient to show the result for $1 \leq l \leq N-1$.

Consider the sum

$$\begin{aligned}
& \sum_{c=0}^{N-1} \Delta(\nu_1, \nu_2, l, c) \Gamma_{l,c}^* \\
&= \sum_{c=0}^{N-1} \sum_{i=0}^{N-1} \omega^{M_i^{\nu_1} - M_{i+l}^{\nu_2}} \Omega^{ic} \sum_{k=0}^{N-l-1} \Omega^{-kc} \\
&= \sum_{k=0}^{N-l-1} \sum_{i=0}^{N-1} \omega^{M_i^{\nu_1} - M_{i+l}^{\nu_2}} \sum_{c=0}^{N-1} \Omega^{(i-k)c} \\
&= N \theta_{1,2}^{(a)}(l),
\end{aligned} \tag{6}$$

since the innermost sum has value 0 when $i \neq k$ and a value of N when $i = k$. On the other hand the sum can also be written as

$$\begin{aligned}
& \sum_{c=0}^{N-1} \Delta(\nu_1, \nu_2, l, c) \Gamma_{l,c}^* \\
&= \Delta(\nu_1, \nu_2, l, 0) \Gamma_{l,0}^* + \sum_{c=1}^{N-1} \Delta(\nu_1, \nu_2, l, c) \Gamma_{l,c}^* \\
&= (N-l)\sqrt{(N+1)} + \sum_{c=1}^{N-1} \Delta(\nu_1, \nu_2, l, c) \Gamma_{l,c}^*, \quad l \neq 0 \pmod{N}.
\end{aligned} \tag{7}$$

The function $\Delta(\nu_1, \nu_2, l, 0)$ is the exponential sum of an m -sequence whose value is known to be equal to $\sqrt{(N+1)}$ e.g., Boztaş-Hammons-Kumar. By combining the above equations, we get the result.

This bound can be applied to any set of polyphase sequences provided we have bounds for the Gauss and exponential sums.

Aperiodic Correlation of Galois Ring Sequences

Here we make use of a Gauss sum bound given in Shanbag-Kumar-Hellesteth for a class of Galois ring sequences. The bound depends on a quantity called the *weighted degree* of the polynomial representing the sequences. Let $f(x)$ be a polynomial over $GR(p^k, r)$ with the p -adic expansion

$$f(x) = F_0(x) + pF_1(x) + \cdots + p^{k-1}F_{k-1}(x),$$

where $F_i(x) \in \mathcal{T}[x]$, $0 \leq i \leq k-1$ which can be obtained from the p -adic expansion of the coefficients of $f(\cdot)$. Further, we assume that f is nondegenerate, by this we mean that f satisfies the following conditions:

Aperiodic Correlation of Galois Ring Sequences

1. $f(0) = 0$
2. $f \neq 0 \pmod{p}$ and
3. no monomial in $f(x)$ has degree divisible by p . Let d_j be the degree of $F_j(x)$, $0 \leq j \leq k - 1$. Then the weighted degree of D of $f(x)$ is defined as

$$D = \max\{p^{k-1} d_0, p^{k-2} d_1, \dots, d_{k-1}\}$$

Many polyphase families (re: Talk by Helleseth) have been defined using nondegenerate polynomials.

Aperiodic Correlation of Galois Ring Sequences

Let α be a primitive element of order $N = p^r - 1$ in $GR(p^k, r)$. Then a sequence associated with a unit $\nu \in GR(p^k, r)$ and a nondegenerate polynomial f of weighted degree D is given by

$$M^\nu = (M_i^\nu) = (Tr(f(\nu\alpha^i)) : 0 \leq i < N).$$

Note that when $f(x) = x$, the weighted degree is p^{k-1} and the sequences are m -sequences.

Aperiodic Correlation of Galois Ring Sequences

Theorem 3 [Shanbag-Kumar-Helleseth] Let $f(x)$ be a nondegenerate polynomial with weighted degree D , Then for the Gauss sums of sequences defined above satisfy

$$|\widehat{S}_k^\nu| \leq D \sqrt{N+1}, \quad 1 \leq k < N.$$

Moreover, we have for the exponential sums of the same sequences

$$\theta(S) \leq (D-1) \sqrt{N+1}.$$

Note that when $D=2, p=2, k=2$, the above bound is better than the bound in Lemma 3.

Aperiodic Correlation of Galois Ring Sequences

If we apply the above two bounds to our aperiodic cross-correlation bound in Theorem 2, we get the following improved bound

Theorem 4

$|C_{1,2}(l)| < (D-1)\sqrt{N+1} + (2/\pi)D\sqrt{N+1} \ln(4e^{\pi/3}N/3\pi)$,
for $l \neq 0$ **Proof** The proof is similar to that in Theorem 3 but we use the results in Theorem 3. For quadriphase sequences, $D = 2$, and the improved bound then becomes

$|C_{1,2}(l)| < \sqrt{N+1} + (4/\pi)\sqrt{N+1} \ln(4e^{\pi/3}N/3\pi)$, for $l \neq 0$.

Clearly the above bound depends on the bound in Theorem 1 and any improvement must come from an improvement to Theorem 1 which is left as an open problem.

Aperiodic Correlation of Galois Ring Sequences

N	Bound of <i>Theorem2</i> δ_1	Bound in <i>Shanbaget.al.</i> $\delta_{Shanbhag}$	Improved bound in <i>Theorem5</i> $\delta_{improved}$	<i>Ratio</i> $\frac{\delta_{improved}}{\delta_{Shanbhag}}$
7	9.87	17.42	10.52	0.604
15	19.98	30.18	18.76	0.622
31	38.80	50.52	31.76	0.629
63	73.69	82.54	52.14	0.632
127	138.05	132.42	83.83	0.633
255	256.23	209.45	132.76	0.634
511	472.17	327.57	207.77	0.634
1023	864.89	507.61	322.12	0.635
2047	1576.01	780.61	495.51	0.635
32767	16641.00	4126.23	2621.16	0.635
1048575	294323.00	30439.00	19346.00	0.636

Aperiodic Correlation of Galois Ring Sequences

We compare our results with those in Shanbag et.al. in view of the numerical evidence. Their aperiodic cross-correlation bound is given by (for m -sequences over \mathbf{Z}_4) $|C_{1,2}(l)| < 2\sqrt{N+1}(\ln N + 1)$. We can write

$$\begin{aligned}\delta_{improved} &< \sqrt{N+1} + (4/\pi)\sqrt{N+1} \ln(4e^{\pi/3}N/3\pi) \\ &\approx \sqrt{N+1} + 1.273\sqrt{N+1} (\ln N + 0.19) \\ &< \sqrt{N+1} + 1.273\sqrt{N+1} (\ln N + 1)\end{aligned}$$

which leads to

$$\delta_{Shanbag} - \delta_{improved} > (0.727(\ln N + 1) - 1)\sqrt{N+1}$$

and the right hand side of this expression becomes positive as soon as $N > e$.

Aperiodic Correlation of Galois Ring Sequences

However, our simple bound given in Theorem 1 is asymptotically inferior to the bound in Shanbag et. al.

We have demonstrated that *bravery* as Prof. Helleseth remarked, or *foolhardiness* can sometimes work in the difficult problem of aperiodic correlation.

Finally, we remark that, even though we have discussed bounds only for Galois ring sequences, techniques extend easily for other optimal families of polyphase sequences like the prime phase Kumar-Moreno sequences.

Galois Rings for QAM sequences

QAM signal sets (whereby complex symbols do not necessarily lie on the unit circle but are drawn from a low energy subset of a translate of regular lattice, e.g., $(-1, -1) + 2\mathbb{Z}^2$) are of interest in wireless communication because of bandwidth efficiency and error resilience, as we demonstrate on the blackboard.

Having worked on nonbinary Family A, it was natural for us to look at QAM based sequences. In 1994 we developed a lower bound on complex sequence families with arbitrary energy distribution.

Galois Rings for QAM sequences

Consider a signal set $\mathcal{A} = \{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_M\}$ with the M cyclically distinct signals taking values in the L -dimensional vector space over the field of complex numbers. Hence $\mathbf{a}_m = (a_0^{(m)} a_1^{(m)} \dots a_{L-1}^{(m)})$ with $a_l^{(m)} \in \mathbf{C}$. Define a $2p$ -norm for such vectors $\mathbf{x} = (x_0 x_1 \dots, x_{L-1})$ by

$$\|\mathbf{x}\|_{2p} = \left(|x_0|^{2p} + |x_1|^{2p} + \dots + |x_{L-1}|^{2p} \right)^{1/2p}$$

where $p \geq 1$, is an integer. Then $\|\mathbf{x}\|_2^2$ denotes the energy of the vector \mathbf{x} .

Galois Rings QAM sequences

The classical lower bounds on constant energy complex sequences are due to Welch and Sidelnikov. Sidelnikov's bound actually assumes that the signal alphabet is roots of unity of some fixed order m and gives a tighter lower bound for $m = 2$, as mentioned by other researchers in the context of \mathbf{Z}_4 sequences delivering the promised improvement compared to Gold sequences.

These bounds can be applied to periodic and aperiodic (at a loss of tightness) sequences. We first derive a generalized Welch lower bound for complex valued sequences that need not have constant energy.

Galois Rings QAM sequences

The *correlation*, or *inner product* between two vectors \mathbf{a}_i and \mathbf{a}_j in C^L is given by

$$\theta_{ij} \triangleq \langle \mathbf{a}_i, \mathbf{a}_j \rangle = \sum_{l=1}^L a_l^{(i)} \overline{a_l^{(j)}} \quad 1 \leq i, j \leq M$$

where the autocorrelation θ_{ii} of the i th signal yields its energy $\theta_{ii} = \langle \mathbf{a}_i, \mathbf{a}_i \rangle = \|\mathbf{a}_i\|_2^2$. The *maximum nontrivial correlation* of the set \mathcal{A} is defined to be

$$\theta_{max} = \max_{i \neq j} |\theta_{ij}|.$$

We now state the Generalized Lower Bound on Correlations of Cyclically Distinct Signals

Galois Rings QAM sequences

Theorem Given a family \mathcal{A} , with M cyclically distinct vectors, and a fixed integer $k \geq 1$, the following holds:

$$\theta_{max}^{2k} \geq \frac{1}{(M-1)M} \times \left[\frac{(\sum_{m=1}^M \|\mathbf{a}_m\|_2^{2k})^2}{C_k^{L+k-1}} - \left(\sum_{m=1}^M \|\mathbf{a}_m\|_2^{4k} \right) \right],$$

where C_k^n denotes the binomial coefficient.

Proof: Assume that all the “off peak” correlations are maximal to get

$$M(M-1)\theta_{max}^{2k} + \theta_{11}^{2k} + \theta_{22}^{2k} + \cdots + \theta_{MM}^{2k} \geq \sum_{i,j} |\theta_{ij}|^{2k}$$

or

$$M(M-1)\theta_{max}^{2k} + \|\mathbf{a}_1\|_2^{4k} + \cdots + \|\mathbf{a}_M\|_2^{4k} \geq \sum_{i,j} |\theta_{ij}|^{2k}$$

and define the right hand side of this inequality as B_k .

It can be shown by using Welch's techniques and properties of multinomial coefficients that by expanding B_k as a sum of products and after extensive manipulation one can write

$$B_k \geq \frac{\left[\sum_{m=1}^M (|a_0^{(m)}|^2 + |a_1^{(m)}|^2 + \dots + |a_{L-1}^{(m)}|^2)^k \right]^2}{C_k^{L+k-1}}$$

Rewriting the last equation gives

$$B_k \geq \frac{(\sum_{m=1}^M \|\mathbf{a}_m\|_2^{2k})^2}{C_k^{L+k-1}}.$$

Rearranging gives

$$M(M-1)\theta_{max}^{2k} \geq \frac{(\sum_{m=1}^M \|\mathbf{a}_m\|_2^{2k})^2}{C_k^{L+k-1}} - \left(\sum_{m=1}^M \|\mathbf{a}_m\|_2^{4k} \right).$$

Galois Rings QAM sequences

This theorem about inner products can now be utilized to derive lower bounds on periodic and aperiodic correlations of sequence families, where the asynchronous nature of the communication forces one to consider not only signals but their cyclic shifts as well.

Before proceeding with this, it is convenient to define the following terms: Denote the energy of a member \mathbf{a}_i of the QAM-CDMA sequence family \mathcal{C} by $\mathcal{E}(\mathbf{a}_i)$, i.e., $\mathcal{E}(\mathbf{a}_i) \triangleq \|\mathbf{a}_i\|_2^2$. Then consider the *average energy per signal* of the whole family \mathcal{C} which is given by

$$\overline{\mathcal{E}(\mathcal{C})} = \frac{\sum_{i=1}^M \mathcal{E}(\mathbf{a}_i)}{M},$$

Galois Rings QAM sequences

It is also possible to define higher moments of the energy of a member, namely $\mathcal{E}^k(\mathbf{a}_i)$, and the averages of those quantities over the family \mathcal{C} .

The vector $(x_k \cdots x_{L-1} x_0 \cdots x_{k-1})$ is the k th cyclic shift of $(x_0 \cdots x_{L-1})$. If all the cyclic shifts of the members of our set \mathcal{A} are added to that set to give a set \mathcal{C} , then the periodic auto or cross correlations of pairs from \mathcal{S} are inner products of pairs from \mathcal{C} . There are obviously $M \times L$ members of \mathcal{C} . This yields the following

Galois Rings QAM sequences

Corollary 1 Define

$$C_{ij}(\tau) = \sum_{l=1}^L a_l^{(i)} \overline{a_{l \oplus \tau}^{(j)}}$$

where $u \oplus v$ is defined as $u + v \pmod{L}$. Consider the maximum of both the auto and cross correlations for the family \mathcal{C} given by

$$C_{max} = \max_{i \neq j \text{ or } \tau \neq 0} |C_{ij}(\tau)|.$$

Then

$$C_{max}^{2k} \geq \frac{1}{(ML - 1)ML} \times \left[\frac{L^2 (\sum_{m=1}^M \|\mathbf{a}_m\|_2^{2k})^2}{C_k^{L+k-1}} - L \left(\sum_{m=1}^M \|\mathbf{a}_m\|_2^{4k} \right) \right],$$

which can also be written

$$C_{max}^{2k} \geq \frac{1}{(ML - 1)} \left[\frac{LM (\overline{\mathcal{E}^k})^2 - C_k^{L+k-1} (\overline{\mathcal{E}^{2k}})}{C_k^{L+k-1}} \right]$$

where we've substituted $\overline{\mathcal{E}^m}$ for $\overline{\mathcal{E}^m(\mathcal{C})}$ for simplicity.

If $L = 2N - 1$ and $a_l^{(m)} = 0$ for $N < l \leq L$, the periodic correlations of the L -vectors become the aperiodic correlations of the N -vectors, and hence we have:

Corollary 2 The aperiodic off-peak correlation of the family \mathcal{C} obeys

$$C_{max}^{2k} \geq \frac{1}{[M(2N - 1) - 1]} \left[\frac{(2N - 1)M (\overline{\mathcal{E}^k})^2 - C_k^{2N+k-2} (\overline{\mathcal{E}^{2k}})}{C_k^{2N+k-2}} \right].$$

Galois Rings for QAM sequences

Since the Welch and Sidelnikov bounds are very close to each other, it is sufficient to compare the generalized bound to the Welch bound, from which it has been derived. We give the periodic correlation comparison only, but the aperiodic correlation case is similar.

Theorem Let ρ_{2k} be the ratio between the generalized (see Corollary 2) and the original Welch lower bounds on the $(2k)^{th}$ moments of periodic correlations (with the generalized bound in the numerator). Then

$$\rho_{2k} = \frac{\left[LM \left(\overline{\mathcal{E}^k(\mathcal{C})} \right)^2 - C_k^{L+k-1} \overline{\mathcal{E}^{2k}(\mathcal{C})} \right]}{\left[LM \mathcal{E}^{2k} - C_k^{L+k-1} \mathcal{E}^{2k} \right]}$$

holds (for the uniform energy case \mathcal{E} is simply the energy of any signal in the family) and ρ_{2k} satisfies the two inequalities

$$\frac{[\overline{\mathcal{E}^k(\mathcal{C})}]^2}{\mathcal{E}^{2k}} \leq \rho_{2k} \leq \frac{\overline{\mathcal{E}^{2k}(\mathcal{C})}}{\mathcal{E}^{2k}}$$

Proof: Consider the energy distribution moments of \mathcal{C} as a random variable and hence use the fact that $[\overline{\mathcal{E}^k(\mathcal{C})}]^2 \leq \overline{\mathcal{E}^{2k}(\mathcal{C})}$ must hold. \square

Galois Rings for QAM sequences

When a *uniform energy* CDMA sequence family is used, the upper and lower bounds in (9) are both 1, and hence the generalized Welch bound matches the original bound, as expected. Furthermore, examining the right hand side of (6) shows that as $\overline{\mathcal{E}^{2k}(\mathcal{C})}$ gets larger relative to $\left(\overline{\mathcal{E}^k(\mathcal{C})}\right)^2$, i.e. as the *variance* of the $2k^{\text{th}}$ energy moment of the family \mathcal{C} increases, the generalized lower bound yields a lesser value. Whether this variation in the bound is reflected in the tradeoffs of designing an actual sequence family is not addressed here.

Galois Rings for QAM sequences

In 1998, Levenshtein introduced a new method which improves the *aperiodic* Welch bound from [?] in the case of sequences in E_2^n (n -vectors with ± 1 entries). We have subsequently shown that Levenshtein's method works for sequences in E_m^n , for any $m \geq 2$. To address the aperiodic case, Levenshtein introduced "weights" for shifts of "zero-padded" code words. A suitable choice of weights allowed him to substantially improve Welch's bound for most cases of interest.

In the next few slides, we demonstrate that the original Welch lower bound on *periodic* correlation can be obtained by Levenshtein's method when the weights are uniform.

We then modify Levenshtein's method so that it can be applied to the *periodic* correlation sequences over more general alphabets which can be thought of as the disjoint union of scalings of E_m^n . This gives us the freedom to obtain QAM type of alphabets by modifying the scalings of E_m^n . This will become clearer in the sequel. We make extensive use of the machinery introduced in by Levenshtein.

Let E_m^n be the set of vectors of length n over the alphabet

$$E_m = \{1, \xi, \xi^2, \dots, \xi^{m-1} \mid \xi = e^{2\pi i/m}\}.$$

Here m is an arbitrary positive integer satisfying $m \geq 2$.

We will derive the Welch lower bound by considering a code $C \subseteq E_m^n$ to be made up of all the codewords

and all their *distinct* cyclic shifts. Sometimes, it will be convenient to associate an ‘exponent’ vector $x \in \mathbf{Z}_m^n$ with the corresponding vector $\Phi(x) \in E_m^n$ given by $\Phi(x) = (\Phi(x_1), \dots, \Phi(x_n))$ $\Phi : \mathbf{Z}_m \rightarrow E$, $\Phi(u) \mapsto \xi^u$. For any two subsets A and B of E_m^n define the value

$$F(A, B) := \frac{1}{|A||B|} \sum_{x \in A} \sum_{y \in B} |\langle x, y \rangle|^2, \quad (8)$$

where $\langle u, v \rangle$ denotes the complex inner product of vectors u and v . The desired results for a code $C \subseteq E_m^n$ will be obtained with the help of finding lower and upper bounds on $F(C, C)$.

Lemma For any code $C \subseteq E_m^n$ of size M ,

$$\theta^2(C) \geq \frac{MF(C, C) - n^2}{M - 1}. \quad (9)$$

Proof Considering separately in (8) the cases $x = y$, (in this case $|\langle x, y \rangle| = n$), and $x \neq y$ we get

$$M^2 F(C, C) \leq Mn^2 + M(M - 1) \theta^2(C),$$

which gives the result required.

We now prove a Lemma which is going to be crucial in the rest of this paper.

Let U be the unit circle in the set of complex numbers. For any $x \in U^n$,

$$F(\{x\}, E_m^n) = n$$

Proof Using (8) we have

$$F(\{x\}, E_m^n) = \frac{1}{m^n} \sum_{y \in E_m^n} |\langle x, y \rangle|^2 = \frac{1}{m^n} \Gamma_{n,m} = n$$

provided we can show that

$$\Gamma_{L,m} := \sum_{y \in E_m^n} |\langle x, y \rangle|^2 = m^L L$$

for any $x \in E_m^L$. Note that if we define

$\Phi(v) = (\Phi(v_1), \dots, \Phi(v_{n-l})) = (x_1, \dots, x_{n-l})$, and

$\Phi(z) = (\Phi(z_1), \dots, \Phi(z_{n-l})) = (y_{l+1}, \dots, y_n)$, then we can write

$$\Gamma_{L,m} = \sum_{\Phi(z) \in E_m^L} |\langle \Phi(v), \Phi(z) \rangle|^2, \quad \Phi(v) \in U^L \text{ arbitrary.}$$

Here, $z_k \in \mathbf{Z}_m$ for $k = 1, \dots, L$, while $v_k \in [0, m)$ for $k = 1, \dots, L$. We also define $s_k = v_k/m$, which allows us to write $\xi^{v_k} = e^{2\pi i s_k}$. The sum $\Gamma_{L,m}$ turns out to be independent of $\Phi(v) \in U^L$, and is evaluated below.

$$\Gamma_{L,m} = \sum_{\Phi(z) \in E_m^L} \langle \Phi(v), \Phi(z) \rangle \overline{\langle \Phi(v), \Phi(z) \rangle} =$$

$$\begin{aligned}
&= \sum_{z \in \mathbf{Z}_m^L} \langle \Phi(v), \Phi(z) \rangle \overline{\langle \Phi(v), \Phi(z) \rangle} \\
&= \sum_{0 \leq z_1, \dots, z_L \leq m-1} \left(\sum_{k=1}^L \xi^{v_k - z_k} \right) \left(\sum_{l=1}^L \xi^{z_l - v_l} \right) \\
&= \sum_{0 \leq z_1, \dots, z_L \leq m-1} \left[L + \sum_{1 \leq k \neq l \leq L} e^{2\pi i(s_k - s_l)} \xi^{z_l - z_k} \right]
\end{aligned}$$

separating the two sums and interchanging the order of summation in the second sum now gives

$$= L m^L + \sum_{1 \leq k \neq l \leq L} e^{2\pi i(s_k - s_l)} \sum_{0 \leq z_1, \dots, z_L \leq m-1} \xi^{z_l - z_k}$$

and the inner sum $\sum \xi^{z_l - z_k}$ can easily be seen to be zero, which completes the proof.

Galois Rings for QAM sequences

An immediate result of this Lemma is that

$$F(E_m^n, E_m^n) = F(\{x\}, E_m^n).$$

For any code $C \subseteq E_m^n$,

$$F(C, C) \geq F(E_m^n, E_m^n) = n.$$

Define functions $f_{i,j}(X)$, $i, j = 0, 1, \dots, 2n - 2$, on E_m^n as follows. If $X = (x_0, x_1, \dots, x_{n-1})$, then $f_{i,j}(X) = x_i x_j$. Using this notation one can rewrite (8) in the following form:

$$F(A, B) = \frac{1}{|A||B|} \sum_{X \in A} \sum_{Y \in B} f_{i,j}(X) f_{i,j}(Y).$$

Let us verify that for any two subsets A and B of E_m^n ,

$$(F(A, B))^2 \leq F(A, A) \cdot F(B, B). \quad (10)$$

First change the order of summation and use the Cauchy inequality for codes:

$$\begin{aligned}
\left| \sum_{X \in A} \sum_{Y \in B} \sum_{i,j=0}^{2n-2} f_{i,j}(X) f_{i,j}(Y) \right|^2 &= \left| \sum_{i,j=0}^{2n-2} \sum_{X \in A} f_{i,j}(X) \sum_{Y \in B} f_{i,j}(Y) \right|^2 = \\
&\leq \sum_{i,j=0}^{2n-2} \left| \sum_{X \in A} f_{i,j}(X) \right|^2 \cdot \sum_{i,j=0}^{2n-2} \left| \sum_{Y \in B} f_{i,j}(Y) \right|^2 = \\
&= \sum_{i,j=0}^{2n-2} \sum_{X \in A} f_{i,j}(X) \sum_{Y \in A} f_{i,j}(Y) \cdot \sum_{i,j=0}^{2n-2} \sum_{X \in B} f_{i,j}(X) \sum_{Y \in B} f_{i,j}(Y).
\end{aligned}$$

One more change in the order of summation implies (10). Then we note that for any $A \subseteq E_m^n$ we have $F(A, E_m^n) = F(E_m^n, E_m^n)$ by Lemma 2. Therefore the

use of (10) with $A = C$ and $B = E_m^n$ completes the proof.

We remark that using $F(A, B) := \left(\sum_{x \in A} \sum_{y \in B} |\langle x, y \rangle|^4 \right) / |A||B|$ gives a bound on $\theta^4(C)$. This bound is included in the corollary below:

New ‘Welch’ Lower Bounds We have

$$\theta^2(C) \geq \frac{Mn - n^2}{M - 1}, \quad \theta^4(C) \geq 3n^2 - 2n - (n^4/M).$$

Note that $M = nt$ if there are t cyclically distinct sequences in the code. The new ‘Welch’ bound on $\theta^4(C)$ will be tighter than the original Welch bound for $\theta^4(C)$ if $Mn^2 - 2Mn \geq 0$. where the ratio of the two bounds will be $(3/2)^{1/4} \approx 1.107$ as M and n tend to infinity. The corresponding two cases of Welch’s lower bounds are reproduced here for ease of comparison.

(Welch) We have

$$\theta^2(C) \geq \frac{Mn - n^2}{M - 1}, \quad \theta^4(C) \geq \frac{2Mn^2 - n^4}{M - 1}.$$

We restrict ourselves to the case of QAM signals with two “energy shells” for ease of exposition.

In this section, we consider a *signal* alphabet of the form

$$\mathcal{X} = E_{m_0}^n \cup \sqrt{a}E_{m_1}^n \quad (11)$$

where the union is assumed to be disjoint, i.e., a codeword belongs either to $E_{m_1}^n$, or to $E_{m_2}^n$ but not to, say, $E_{m_1} \times E_{m_2} \times \dots \times E_{m_1}$.

As an example, if we take $\mathcal{X} = E_4^3 \cup \sqrt{2}E_4^3$, the codewords $(-1, +i, -i)$, $\sqrt{2}(+1, -i, -1)$ are allowed while the codeword $(-1, \sqrt{2}, \sqrt{2}i)$ is not allowed. To any vector $x \in \mathcal{X}$, we assign a *weight* $w_{c(x)}$, where

$$w_k \geq 0, \quad k = 0, 1, \quad \text{and} \quad w_0 + w_1 = 1, \quad (12)$$

where $c(x)$, is the “class” of the vector x , i.e.,

$$w_{c(x)} = \begin{cases} w_0 & \text{if } x \in E_{m_1}^n, \\ w_1 & \text{if } x \in \sqrt{a}E_{m_2}^n. \end{cases} \quad (13)$$

For any two subsets A and B of \mathcal{X} , we define the value

$$F(A, B) := \frac{1}{|A||B|} \sum_{x \in A} \sum_{y \in B} w_{c(x)} w_{c(y)} |\langle x, y \rangle|^2, \quad (14)$$

where $\langle u, v \rangle$ denotes the complex inner product of vectors u and v . It is also convenient to define an “un-normalized $F(A, B)$ ” via $G(A, B) := |A||B|F(A, B)$. We now proceed to prove the generalized versions of the results in the previous section.

Lemma 3 For any code $C \subseteq \mathcal{X}$ of size M ,

$$\theta^2(C) \geq \frac{M^2 F(C, C) - (w_0^2 M_0 + w_1^2 M_1 a^2) n^2}{(w_0 M_0 + w_1 M_1)^2 - (w_0^2 M_0 + w_1^2 M_1)} \quad (15)$$

where

$$C = C_0 \cup \sqrt{a}C_1, \quad \text{and}$$

$$|C_i| = M_i, C_i \subseteq E_{m_i}^n, \quad i = 0, 1$$

with $M = M_1 + M_2$.

Proof Considering separately the cases $x = y$ (in this case $|\langle x, y \rangle| = n$ for $x \in C_0$, and $|\langle x, y \rangle| = an$ for $x \in C_1$), and $x \neq y$ (if x and y are in the same “class” we get the upper bounds $M_i(M_i - 1)w_i^2\theta^2(C)$, $i = 0, 1$, while if they are in different classes we get the upper bound $2M_0M_1w_0w_1\theta^2(C)$) we obtain

$$\begin{aligned} G(C, C) = M^2F(C, C) &\leq (w_0^2M_0 + w_1^2M_1a^2)n^2 \\ &+ (M_0^2 - M_0)w_0^2\theta^2(C) + (M_1^2 - M_1)w_1^2\theta^2(C) \\ &+ 2M_0M_1w_0w_1\theta^2(C) \end{aligned}$$

which gives the result required.

Lemma 4 We have

$$F(\{x\}, \mathcal{X}) = \begin{cases} n \left[\gamma w_0^2 + (1 - \gamma) w_0 w_1 a \right] & \text{if } x \in E_{m_0}^n, \\ n \left[\gamma w_0 w_1 a + (1 - \gamma) w_1^2 a^2 \right] & \text{if } x \in E_{m_1}^n, \end{cases}$$

where $\gamma = \frac{m_0^n}{m_0^n + m_1^n}$.

Proof Note that

$$\begin{aligned} G(\{x\}, \mathcal{X}) &= G(\{x\}, E_{m_0}^n \cup \sqrt{a} E_{m_1}^n) = \\ &= w_{c(x)} w_0 \sum_{y \in E_{m_0}^n} |\langle x, y \rangle|^2 + w_{c(x)} w_1 a \sum_{y \in E_{m_1}^n} |\langle x, y \rangle|^2 \end{aligned}$$

which gives

$$G(\{x\}, \mathcal{X}) = \begin{cases} w_0^2 \Gamma_{n, m_0} + w_0 w_1 a \Gamma_{n, m_1} & \text{if } x \in E_{m_0}^n, \\ w_0 w_1 a \Gamma_{n, m_0} + w_1^2 a^2 \Gamma_{n, m_1} & \text{if } x \in E_{m_1}^n, \end{cases}$$

and yields the result required after using Lemma 2 (which states that

$$\Gamma_{n,m_i} = nm_i^n, i = 0, 1) \text{ and noting that}$$

$$F(\{x\}, \mathcal{X}) = G(\{x\}, \mathcal{X}) / (m_0^n + m_1^n) .$$

Now, we can investigate the conditions under which

$$F(C, C) \geq F(\mathcal{X}, \mathcal{X}) = F(E_{m_0}^n \cup \sqrt{a}E_{m_1}^n, E_{m_0}^n \cup \sqrt{a}E_{m_1}^n)$$

can be made to hold.

$$F(C, \mathcal{X}) = n \left[\delta \left(\gamma w_0^2 + (1 - \gamma) w_0 w_1 a \right) + (1 - \delta) \left(\gamma w_0 w_1 a + (1 - \gamma) w_1^2 a^2 \right) \right]$$

Note that for any code $C = C_0 \cup \sqrt{a}C_1$ which is a subset of $E_{m_0}^n \cup \sqrt{a}E_{m_1}^n$ we have

$$G(C_0 \cup \sqrt{a}C_1, \mathcal{X}) = G(C_0 \cup \sqrt{a}C_1, E_{m_0}^n \cup \sqrt{a}E_{m_1}^n) =$$

$$= n \left[M_0 m_0^n w_0^2 + M_1 m_1^n w_0 w_1 a + M_0 m_0^n w_0 w_1 a + M_1 m_1^n w_1^2 a^2 \right]$$

which gives

$$F(C_0 \cup \sqrt{a}C_1, \mathcal{X}) = \frac{G(C_0 \cup \sqrt{a}C_1, \mathcal{X})}{(M_0 + M_1)(m_0^n + m_1^n)} =$$

$$= n \left[\gamma(\delta w_0^2 + (1 - \delta)w_0 w_1 a) + (1 - \gamma)(\delta w_0 w_1 a + (1 - \delta)w_1^2 a^2) \right]$$

where $\delta = M_0/(M_0 + M_1)$.

We now apply Lemma 4 to $C = \mathcal{X}$ to obtain

$$F(\mathcal{X}, \mathcal{X}) = n [\gamma w_0 + (1 - \gamma) a w_1]^2$$

while

$$F(C, \mathcal{X}) = n \left[\delta \left(\gamma w_0^2 + (1 - \gamma) w_0 w_1 a \right) + (1 - \delta) \left(\gamma w_0 w_1 a + (1 - \gamma) w_1^2 a^2 \right) \right]$$

hence the choice $\delta = \gamma$, is sufficient to ensure

$$F(C, \mathcal{X}) \geq F(\mathcal{X}, \mathcal{X})$$

holds (in fact, $F(C, \mathcal{X}) = F(\mathcal{X}, \mathcal{X})$ holds here). We now appeal to an obvious weighted generalization of Lemma ?? to obtain that for the case $\delta = \gamma$, we still have

$$F(C, \mathcal{X})^2 \leq F(\mathcal{X}, \mathcal{X})F(C, C)$$

which now becomes

$$F(\mathcal{X}, \mathcal{X})^2 \leq F(\mathcal{X}, \mathcal{X})F(C, C)$$

which implies

$$F(\mathcal{X}, \mathcal{X}) \leq F(C, C).$$

Hence, for such codes whose codeword distributions across energy “shells” (i.e., $M_0/(M_0 + M_1)$) are equal

to the word distributions for the total codeword space, (i.e., $m_0^n/(m_0^n + m_1^n)$) we have the following:

When $\delta = \gamma$, we have

$$\begin{aligned} \theta^2(C) &\geq \max_{0 \leq w \leq 1} \frac{M^2 F(\mathcal{X}, \mathcal{X}) - (w_0^2 M_0 + w_1^2 M_1 a^2) n^2}{(w_0 M_0 + w_1 M_1)^2 - (w_0^2 M_0 + w_1^2 M_1)} = \\ \max_{0 \leq w \leq 1} &= \frac{Mn(\gamma w + (1 - \gamma)a(1 - w))^2 - (w^2 \gamma + (1 - w)^2 a^2 (1 - \gamma)) n^2}{M(\gamma w + (1 - \gamma)(1 - w))^2 - (w^2 \gamma + (1 - w)^2 (1 - \gamma))} \end{aligned}$$

Proof. Proof: Let $w_0 = w$, $w_1 = 1 - w$, and use Lemma 3.

QAM sequences from Galois Rings

Here we consider a signal set with an arbitrary number, say v , of energy “shells.” Let the *signal* alphabet be of the form

$$\mathcal{X} = \sqrt{a_0}E_{m_0}^n \cup \dots \cup \sqrt{a_{v-1}}E_{m_v}^n \quad (16)$$

where the union is assumed to be disjoint, i.e., a code-word belongs to a unique $\sqrt{a_i}E_{m_i}^n$, for some $i = 0, \dots, v-1$. To any vector $x \in E_{m_0}^n \cup \sqrt{a}E_{m_1}^n$, we assign a *weight* $w_{c(x)}$, where

$$w_k \geq 0, \quad k = 0, 1, \dots, v-1 \quad \text{and} \quad w_0 + \dots + w_{v-1} = 1, \quad (17)$$

where $c(x)$, is the “class” of the vector x (compare Section 3.1). The definitions of $F(A, B)$ and $G(A, B)$ are as in Section 1. The quantities M_i, γ_i, δ_i ,

for $i = 0, \dots, v - 1$, all have the same meanings as in Section 3.1. The arguments to prove Theorem 4 parallel those in Section 3.1 and are omitted.

By choosing $\delta_i = \gamma_i$, $i = 0, \dots, v - 1$, we have

$$\theta^2(C) \geq \max_{\substack{w_0 + \dots + w_{v-1} = 1 \\ w_i \geq 0, i=0, \dots, v-1}} \frac{Mn(\sum_{i=0}^{v-1} w_i \gamma_i a_i)^2 - n^2(\sum_{i=0}^{v-1} w_i^2 \gamma_i a_i^2)}{M(\sum_{i=0}^{v-1} w_i \gamma_i)^2 - (\sum_{i=0}^{v-1} w_i^2 \gamma_i)}$$

Note that the family of bounds we have obtained are in general non-convex as a function of (w_0, \dots, w_{v-1}) . We now state a special case of a previously proved theorem on CDMA sequences with arbitrary energy distribution.

Theorem For any complex sequence family C with arbitrary energy distribution, length n and M cyclically

distinct sequences x_1, \dots, x_M , we have the lower bound

$$\theta^2 \geq \left[M (\overline{\mathcal{E}})^2 - (\overline{\mathcal{E}^2}) \right] / (Mn - 1) \approx$$

$$n \left[\left(\sum_{i=0}^{v-1} \gamma_i a_i^2 \right)^2 - \frac{1}{M} \left(\sum_{i=0}^{v-1} \gamma_i a_i^4 \right) \right]$$

where $\overline{\mathcal{E}^k}$ is the average of the k^{th} energy moment of the sequence family. We now consider an example which uses the symbol constellation $E_4^n \cup \sqrt{2}E_4^n$ of the figure above.

Example Let $\gamma_i = 1/2, m_i = 4, i = 0, 1, a_0 = 1, a_1 = 2$, and $M = nt$, i.e., t cyclically distinct sequences each of length n . Then the bound in Theorem 3 becomes $\theta^2 \geq n(\frac{9}{4} - \frac{5}{2nt})$. However, the new bound in Theorem 2

becomes

$$\theta^2 \geq \frac{\frac{Mn}{4} (w + 2(1 - w))^2 - \frac{n^2}{2} (w^2 + 2^2(1 - w)^2)}{\frac{M}{4} (w + (1 - w))^2 - \frac{1}{2} (w^2 + (1 - w)^2)}$$

which is a ratio of two quadratics. Simply letting $w \rightarrow 0$ yields

$$\theta^2 \geq [4Mn - 8n^2] / (M - 2) = [4n^2(t - 2)] / (nt - 2) \approx 4n [(t - 2)/t] \text{ which is clearly better for typical values } t \geq n \text{ of practical interest and tends to } 4n \text{ as } t \rightarrow \infty.$$

We have developed a new lower bound for the periodic correlation of sequence families. It must be emphasized that the new bound, while tighter than the previously derived lower bound on QAM sequences, applies to a more restricted type of sequence, i.e., sequences

which are restricted to have symbols in one of the possible “shells” of the constellation. We have a table which compares various performance parameters of different constellations, for the case that $M \approx n^2$, which is of most interest for asynchronous CDMA applications. Note that it is possible to use the constellation $E_4^n \cup \sqrt{2}E_4^n$ and obtain improved minimum Euclidean distance at the cost of degraded Peak-Off-Peak correlation ratio over 8-PSK. The challenge is to apply algebraic design techniques to design families that approach the bounds derived here.

Sequence Type	Data Rate	Minimum Peak to Off-Peak Ratio $\sqrt{\mathcal{E}}/\theta(C)$	Minimum Euclidean Distance d
4-PSK	2 bits	$\frac{n}{\sqrt{n}} = \sqrt{n}^*$	$2 \sin(\pi/4) = \sqrt{2}$
8-PSK	3 bits	$\frac{n}{\sqrt{n}} = \sqrt{n}^*$	$2 \sin(\pi/8) \approx 0.765$
$E_4^n \cup \sqrt{2}E_4^n$	3 bits	$\leq \frac{n}{\sqrt{4n}} = \frac{1}{2}\sqrt{n}$	1

Performance parameters of various constellations for $M \approx n^2$. The symbol * means that a known sequence family achieves the given value.

Recent work by Garg and Kumar has applied interleaving to obtain many more QAM based sequence designs, where they have used our design principles and extended them.