Applications of Exponential Sums in Communications Theory

Kenneth G. Paterson
Extended Enterprise Laboratory
HP Laboratories Bristol

HPL-1999-101
13th September, 1999*

exponential sums, curves, finite fields, codes, communications, sequences, correlation, CDMA, OFDM

We provide an introductory overview of how exponential sums, and bounds for them, have been exploited by coding theorists and communications engineers.

* Internal Accession Date Only

Applications of Exponential Sums in Communications Theory

Kenneth G. Paterson

Mathematics, Cryptography and Security Group,
Hewlett-Packard Laboratories,
Filton Road, Stoke-Gifford,
Bristol BS34 8QZ, U.K.
kp@hplb.hpl.hp.com

Abstract. We provide an introductory overview of how exponential sums, and bounds for them, have been exploited by coding theorists and communications engineers.

1 Introduction

An exponential sum is a sum of complex numbers of absolute value one in which each term is obtained by evaluating a function of additive and/or multiplicative characters of a finite field $\mathbb{F}_q$, and where the sum is taken over the whole of $\mathbb{F}_q$. Exponential sums date back to early work of Lagrange and Gauss, the latter explicitly evaluating certain basic exponential sums now called Gauss sums in his honour. Since then, much more general exponential sums have been considered, but generally, it is impossible to find explicit expressions evaluating these more complicated sums. However their evaluation is intimately connected to the problem of counting the numbers of points on related curves (more generally, algebraic varieties) defined over finite extensions of $\mathbb{F}_q$ and deep methods in algebraic geometry have been developed to find good bounds on such numbers. Two major achievements of these methods are Weil's 1940 announcement of the proof of the Riemann hypothesis for curves over finite fields [66] and Deligne's Fields medal winning proof of the Weil conjectures for algebraic varieties [8]. These results are justly regarded as being high-points of twentieth century mathematics, and from them, good bounds for many classes of exponential sums can easily be deduced.

In contrast to the depth and sophistication of the techniques used by Weil and Deligne, the bounds they proved are rather easy to state and to use. Coding theorists and communications engineers have been extraordinarily fecund in exploiting this ease of use. In this paper, we quote some bounds for exponential sums, briefly sketch the connection to curves over finite fields and examine some applications of exponential sums in communications theory. We make no attempt to be exhaustive in our coverage. Rather our aim is to provide an introductory tour, focusing on salient points, basic techniques and a few applications. For this reason, all of our applications will involve, in various guises, a class of codes called dual BCH codes. We provide pointers to the vast literature for more advanced topics, and immediately recommend the survey [21] for a snapshot of the whole area.

We show how the minimum distances of dual BCH codes and other cyclic codes can be evaluated in terms of exponential sums. We then consider the problem, important in multiple-access spread-spectrum communications, of designing sequence sets whose periodic cross-correlations and auto-correlations are all small. Then we look at how exponential sums can be used to study binary sequences with small partial and aperiodic correlations. These are also important in spread-spectrum applications. We also consider the application of exponential sums in a relatively new communications application, the power control problem in Orthogonal Frequency Division Multiplexing (OFDM). Finally, we briefly consider some more advanced applications of exponential sums.

2 Finite Fields, Their Characters and the Dual BCH Codes

We set out some facts concerning the trace map on a finite field, assuming the reader to be familiar with the basic properties of finite fields (existence, uniqueness, primitive elements and so on). Basic references for finite fields are [23, 31, 32]. We will almost exclusively be concerned with fields of characteristic two in this paper, though almost everything we say can be generalised to characteristic p with appropriate modifications.

Throughout, m, n will denote positive integers with $m|n$. Also, $\mathbb{F}_{2^n}$ denotes the finite field with 2^n elements and $\mathbb{F}^*_{2^n}$ the set of non-zero elements of $\mathbb{F}_{2^n}$. The relative trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ is defined by

$$\mathrm{tr}^n_m(x) = \sum_{i=0}^{n/m-1} x^{2^{mi}}.$$

The trace map $\mathrm{tr}^n_m(x)$ has the following properties:

- It is an $\mathbb{F}_{2^m}$-linear mapping onto $\mathbb{F}_{2^m}$.

- For each $b \in \mathbb{F}_{2^m}$, the equation
$$\mathrm{tr}_m^n(x) = b$$
has exactly 2^{n-m} solutions $x \in \mathbb{F}_{2^n}$. In other words, the trace map is 'equi-distributed' on sub-fields.
- $\mathrm{tr}_1^m(\mathrm{tr}_m^n(x)) = \mathrm{tr}_1^n(x)$ for $x \in \mathbb{F}_{2^n}$.

Next we introduce the characters of $\mathbb{F}_{2^n}$. Of course these can be defined more generally for any finite field $\mathbb{F}_q$. Even more generally, the characters of an abelian group are just the homomorphisms from that group onto the set U of complex numbers of absolute value 1. The field $\mathbb{F}_{2^n}$ contains two abelian subgroups of particular interest, namely the additive and multiplicative groups of the finite field, and so we have two corresponding sets of characters.

For each $b \in \mathbb{F}_{2^n}$, define a map χ_b from $\mathbb{F}_{2^n}$ to the set $\{1, -1\}$ by writing
$$\chi_b(x) = (-1)^{\mathrm{tr}_1^n(bx)}, \quad x \in \mathbb{F}_{2^n}.$$
The maps χ_b are called the *additive characters* of $\mathbb{F}_{2^n}$: by linearity of trace, it can be seen that these maps are homomorphisms from the group $(\mathbb{F}_{2^n}, +)$ to U. The map χ_0 is called the *trivial* additive character because $\chi_0(x) = 0$ for all $x \in \mathbb{F}_{2^n}$. Notice that if $b \neq 0$, then
$$\sum_{x \in \mathbb{F}_{2^n}} \chi_b(x) = 0 \tag{1}$$
because of the equi-distribution properties of the trace map.

Now let $N = 2^n - 1$ and let $\omega = \exp(2\pi i/N)$ be a complex N-th root of unity. Let α be a primitive element in $\mathbb{F}_{2^n}$. For each integer j with $0 \le j < 2^n - 1$, we define a map ψ_j from $\mathbb{F}_{2^n}^*$ to the set U of powers of ω by writing
$$\psi_j(\alpha^i) = \omega^{ji}, \quad 0 \le i < 2^n - 1.$$
The maps ψ_j are called the *multiplicative characters* of $\mathbb{F}_{2^n}$: they are homomorphisms from $(\mathbb{F}_{2^n}^*, \cdot)$ to U. The map ψ_0 is called the *trivial* multiplicative character.

For much more information about characters of finite fields, see [22, 23, 32]

Next we define the main class of codes that we'll work with in this paper, the dual BCH codes. In fact, we work with a sub-class of these codes, more properly called binary, primitive, dual BCH codes.

Let α be primitive in $\mathbb{F}_{2^n}$ and let t be a positive integer with $1 \leq 2t-1 \leq 2^{\lceil n/2 \rceil}+1$. Let $\mathcal{G}_t$ denote the set of polynomials

$$\mathcal{G}_t = \{g_1 x + g_3 x^3 + \cdots + g_{2t-1} x^{2t-1} : g_i \in \mathbb{F}_{2^n}\}.$$

For each $g \in \mathcal{G}$, define a length 2^n-1, binary word

$$c_g = (\mathrm{tr}_1^n(g(1)), \mathrm{tr}_1^n(g(\alpha)), \ldots, \mathrm{tr}_1^n(g(\alpha^{2^n-2}))).$$

and define a code $\mathcal{C}_t$ by:

$$\mathcal{C}_t = \{c_g : g \in \mathcal{G}_t\}.$$

So the words of $\mathcal{C}_t$ are obtained by evaluating certain degree $2t-1$ polynomials on the non-zero elements $1, \alpha, \ldots, \alpha^{2^n-2}$ of $\mathbb{F}_{2^n}$, and then applying the trace map.

It follows from the linearity of the trace map that the code $\mathcal{C}_t$ is linear. It can be shown that the dimension of the code is equal to nt over $\mathbb{F}_2$, the set of polynomials $\{cx^{2i-1} : 1 \leq i \leq t, c \in \mathbb{F}_{2^n}\}$ leading to a basis for the code. By examining these 'basis polynomials', it's now easy to show that the code is cyclic. It is a consequence of a theorem of Delsarte that the code $\mathcal{C}_t$ is the dual of the primitive, binary BCH code with designed distance $2t+1$ whose zeros include $\alpha, \alpha^3, \ldots, \alpha^{2t-1}$. See [34, Chapters 8 and 9] for more background on BCH codes and their duals.

In Section 4 we will obtain bounds on the minimum Hamming distances of the codes $\mathcal{C}_t$ by using Weil's bound on the size of exponential sums with polynomial argument.

3 Exponential Sums

As we stated in the introduction, exponential sums are sums in which each term is obtained by evaluating a function of additive and/or multiplicative characters of a finite field $\mathbb{F}_q$, and where the sum is taken over the whole of $\mathbb{F}_q$. Here we consider some classes of sums over finite fields of characteristic 2, stating bounds for such sums. We also sketch the connection between exponential sums and the problem of counting the numbers of points on certain curves over finite fields. For a much more detailed exposition of the theory of exponential sums, we recommend [32, Chapter 5].

Let χ be a non-trivial additive character of $\mathbb{F}_{2^n}$ and let g be a polynomial of odd degree $r < 2^n$ over $\mathbb{F}_{2^n}$. We are interested in sums of the form

$$\sum_{x \in \mathbb{F}_{2^n}} \chi(g(x))$$

which are called *exponential sums with polynomial argument* or *Weil sums*. For special choices of g, the sums can be evaluated explicitly (for example, when $g(x) = x$ we know from (1) that the sum is identically zero). Usually though, we have to settle for bounds on the size of the sums. The following result, known as Weil's theorem or the Carlitz-Uchiyama/Weil bound, is the fundamental estimate on the size of Weil sums:

Result 1 *[66, 4] With notation as above,*

$$\left| \sum_{x \in \mathbb{F}_{2^n}} \chi(g(x)) \right| \leq (r-1)2^{n/2}.$$

Notice the Weil sums, being sums of 2^n complex numbers of absolute magnitude 1, are potentially of size $O(2^n)$. The above bound shows that (at least when r is not too large), the Weil sums are much smaller than this. Notice also that the case $r = 1$ of Weil's bound recovers (1). The condition that g have odd degree r can be replaced by much weaker criteria, for example that the polynomial $y^2 + y + g(x)$ in two variables be absolutely irreducible, or that the polynomial g *not* be of the form $h(x)^2 + h(x) + d$ for any polynomial h over $\mathbb{F}_{2^n}$ and any $d \in \mathbb{F}_{2^n}$.

3.1 Exponential Sums and Curves over Finite Fields

We sketch the connection between Weil exponential sums and the problem of counting points on curves over finite fields and outline how Weil's theorem is proved using algebraic-geometric methods. For modern and accessible approaches to the proof of Weil's theorem and related results, see the books [36, 61]. For an elementary approach avoiding algebraic geometry, see [54]. For introductory explanations, see [22, Chapters 10 and 11] and [32, Notes to Chapter 6].

To make the connection, we need the following simple result:

Lemma 1. *[32, Theorem 2.25] For $b \in \mathbb{F}_{2^n}$, we have $tr_1^n(b) = 0$ if and only if $y^2 + y = b$ for some $y \in \mathbb{F}_{2^n}$.*

Now consider the exponential sum

$$\sum_{xin\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^n(g(x))} = |\{x \in \mathbb{F}_{2^n} : \mathrm{tr}_1^n(g(x)) = 0\}| - |\{x \in \mathbb{F}_{2^n} : \mathrm{tr}_1^n(g(x)) = 1\}|$$

$$= 2|\{x \in \mathbb{F}_{2^n} : \mathrm{tr}_1^n(g(x)) = 0\}| - 2^n.$$

But we know that $\mathrm{tr}_1^n(g(x)) = 0$ if and only if there exists a solution $y \in \mathbb{F}_{2^n}$ to the equation $y^2 + y = g(x)$, in other words, if and only if there is a y such that (x, y) is a point on the *affine curve* C whose equation is $h(x, y) = 0$ where $h(x, y) = y^2 + y + g(x)$. Notice though that if y is a solution to $h(x, y) = 0$, then so too is $y + 1$. So the points on C come in pairs and are in 2-1 correspondence with the x satisfying $\mathrm{tr}_1^n(g(x)) = 0$. We deduce that

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^n(g(x))} = |C| - 2^n$$

where $|C|$ denotes the number of points on the affine curve C.

Next we introduce a projective version of C. We consider a homogeneous version of the equation defining C:

$$H(x, y, z) = y^2 z^{r-2} + y z^{r-1} + z^r g(x/z)$$

(where r is the degree of g) and count the projective points $[x, y, z]$ satisfying $H(x, y, z) = 0$. Notice that $H(x, y, 1) = h(x, y)$ for all x, y, so the set of projective points $[x, y, z]$ satisfying $H(x, y, z) = 0$ accounts for all the points on the affine curve, once each. But the projective curve has one additional point $[0, 1, 0]$, called a point at infinity. So if N denotes the number of projective points on C, then we have $N = |C| + 1$ and

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^n(g(x))} = N - 1 - 2^n. \tag{2}$$

In his paper [66], Weil considered the numbers of points on general absolutely irreducible projective curves. Let C be such a curve defined over a finite field $\mathbb{F}_q$. For $s \geq 1$, let N_s denote the number of projective points on C whose coordinates all lie in the extension $\mathbb{F}_{q^s}$, called $\mathbb{F}_{q^s}$-rational points. Then the function

$$Z(u) = \exp\left(\sum_{s=1}^{\infty} \frac{N_s u^s}{s}\right)$$

is called the zeta function of C. This function contains all the information about the numbers of projective points on C over extensions of $\mathbb{F}_q$. Weil was able to show that $Z(u)$ is actually a rational function of u, in fact, he showed:

$$Z(u) = \frac{P(u)}{(1-u)(1-qu)}$$

where $P(u)$ is a degree $2g$ polynomial with integer coefficients and constant term 1. Here g, the genus of C, is a topological number associated with the curve. Writing

$$P(u) = \prod_{i=1}^{2g} (1 - \omega_i u)$$

Weil also showed that the $2g$ complex numbers $\omega_1, \ldots, \omega_{2g}$ all satisfy $|\omega_i| = q^{1/2}$. This last fact, conjectured by Artin and proved by Weil, is *the Riemann hypothesis for curves over finite fields*, so-called by analogy with the Riemann hypothesis for the classical zeta function.

Now a straightforward calculation shows that

$$u \frac{d \log Z(u)}{du} = \sum_{s=1}^{\infty} N_s u^s.$$

On the other hand,

$$\begin{aligned} u \frac{d \log Z(u)}{du} = u \frac{Z'(u)}{Z(u)} &= u \left(\sum_{j=1}^{2g} \frac{-\omega_i}{1 - \omega_i u} + \frac{1}{1-u} + \frac{q}{1-qu} \right) \\ &= \sum_{s=1}^{\infty} \left(\sum_{i=1}^{2g} (\omega_i)^s + 1 + q^s \right) u^s. \end{aligned}$$

By comparing the two power series, we get

$$N_s = q^s + 1 - \sum_{i=1}^{2g} (\omega_i)^s$$

and so

$$|N_s - q^s - 1| \leq 2gq^{1/2}. \tag{3}$$

We can now specialise to the projective curve C arising from our exponential sum. It turns out that the curve is always absolutely irreducible when r is odd and has genus $g = (r-1)/2$. Taking $q = 2^n$ and $s = 1$, the bound (3) tells us that $N = N_1$, the number of projective points on our curve, satisfies $|N - 2^n - 1| \leq (r-1)q^{1/2}$. Comparing with the identity (2), we now obtain the bound of Result 1.

These results have been generalised considerably to the situation where C is replaced by any non-singular algebraic variety V. Dwork [12] showed that the analogous zeta function is rational while Deligne [8] finally proved Weil's conjectures concerning the analogue of the Riemann hypothesis for such varieties. These deep results have also been exploited by coding theorists. We will summarise this work briefly in the final section.

3.2 Hybrid Exponential Sums

We loosely define hybrid exponential sums to be exponential sums in which the summand is a product of a multiplicative and an additive character. Perhaps the simplest hybrid sums are the Gaussian sums:

Definition 1. *Let χ be an additive character and ψ a multiplicative character of $\mathbb{F}_{2^n}$. Then the Gaussian sum $G(\chi, \psi)$ is defined by*

$$G(\chi, \psi) = \sum_{x \in \mathbb{F}_{2^n}^*} \chi(x)\psi(x).$$

The following result about Gaussian sums is basic; elementary proofs can be found in [32, Theorem 5.11] and [22, Proposition 8.2.2].

Result 2 *Let χ be a non-trivial additive character and ψ a non-trivial multiplicative character of $\mathbb{F}_{2^n}$. Then*

$$|G(\chi, \psi)| = 2^{n/2}.$$

Why should this result be surprising? The sum is of size $2^{n/2}$, only slightly bigger than the square root of the size of the domain over which the sum is taken. Moreover, the sum has exactly this absolute value for *every* pair of non-trivial characters.

Hybrid exponential sums with polynomial arguments have also been considered; the following is a useful general purpose bound on such sums, again due to Weil [66].

Result 3 *Let ψ be a non-trivial multiplicative character of $\mathbb{F}_{2^n}$ of order d with $d|(2^n - 1)$. Let χ be a non-trivial additive character of $\mathbb{F}_{2^n}$. Let $f(x) \in \mathbb{F}_{2^n}[x]$ have m distinct roots and $g(x) \in \mathbb{F}_{2^n}[x]$ have degree r. Suppose that* $\gcd(d, \deg f) = 1$ *and that r is odd. Then*

$$\left| \sum_{x \in \mathbb{F}_{2^n}^*} \chi(g(x))\psi(f(x)) \right| \leq (m + r - 1)2^{n/2}.$$

Here, the technical conditions on the polynomials f and g are needed to rule out various degenerate cases. They can be replaced by weaker conditions — see [54, Theorem 2G, p.45]. We emphasise again that the bound shows that the hybrid sums are much smaller than the size of the field over which the sum is taken.

4 Application: Minimum Distance of Dual BCH Codes

When $t = 1$, the code $\mathcal{C}_t$ is called the simplex code. The minimum Hamming distance of this code is exceedingly simple to calculate. Recall that the code is linear, so we need to find the minimum Hamming weight of a non-zero codeword of $\mathcal{C}_1$. Now a non-zero codeword c has components of the form $\mathrm{tr}_1^n(b\alpha^i)$ where $b \in \mathbb{F}_{2^n}^*$ and $0 \leq i < 2^n - 1$. As i runs through the range $0, 1, \ldots, 2^n - 2$, so α^i runs over the whole of $\mathbb{F}_{2^n}^*$, the non-zero elements of $\mathbb{F}_{2^n}$.

Consider the exponential sum (1):

$$\begin{aligned}
0 &= \sum_{x \in \mathbb{F}_{2^n}} \chi_b(x) \\
&= 1 + \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{tr}_1^n(bx)} \\
&= 1 + |\{x \in \mathbb{F}_{2^n}^* : \mathrm{tr}_1^n(bx) = 0\}| - |\{x \in \mathbb{F}_{2^n}^* : \mathrm{tr}_1^n(bx) = 1\}| \\
&= 1 + (2^n - 1 - \mathrm{wt}_H(c)) - \mathrm{wt}_H(c) \\
&= 2^n - 2\mathrm{wt}_H(c)
\end{aligned}$$

Here we have used the fact that the number of components in which c equals 0 is just the code length less the Hamming weight of c. It follows from our last equality that $\mathrm{wt}_H(c) = 2^{m-1}$. So every non-zero codeword of $\mathcal{C}_1$ has Hamming weight equal to 2^{m-1}, and the minimum distance of the code is also 2^{m-1}.

We can apply the same technique, and the Weil bound, to bound the minimum distance of the code $\mathcal{C}_t$. Recall that a non-zero codeword c_g of $\mathcal{C}_t$ comes from a non-zero polynomial $g(x)$ with zero constant term and of odd degree at most $2t-1$. Reversing the steps in the previous calculation, we get:

$$2^n - 2\mathrm{wt}_H(c_g) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^n(g(x))} = \sum_{x \in \mathbb{F}_{2^n}} \chi_1(g(x)) \qquad (4)$$

But this last sum is bounded in absolute value by $(2t-2)2^{n/2}$ according to Result 1. We deduce that

$$2^{n-1} - (t-1)2^{n/2} \leq \mathrm{wt}_H(c_g) \leq 2^{n-1} + (t-1)2^{n/2},$$

and the following theorem is now obvious:

Theorem 4. *Suppose $1 \leq 2t - 1 \leq 2^{\lceil n/2 \rceil} + 1$. Then the minimum Hamming distance of $\mathcal{C}_t$ is at least $2^{n-1} - (t-1)2^{n/2}$.*

This bound can be improved in certain cases [38].

5 Application: Sequence Sets with Low Periodic Correlations

The correlation properties of sets of binary sequences are important in Code-Division Multiple-Access (CDMA) spread-spectrum communications as well as in ranging and synchronisation applications.

We begin in this section by defining the periodic correlation functions for sequences and then stating a basic sequence design problem. This is motivated by a simplified description of how sequences with favourable correlation properties are used in CDMA communications. Then we define a class of sequences, the m-sequences, and look at their correlation properties. Finally, we show how exponential sums can be used to bound the correlations of some sets of sequences obtained from m-sequences and the dual BCH codes.

5.1 Periodic Correlation Functions

Let $u = u_0, u_1, u_2, \ldots$ and $v = v_0, v_1, v_2, \ldots$ be two complex-valued sequences of period N (by which we mean $u_{i+N} = u_i$ and $v_{i+N} = v_i$ for all $i \geq 0$). We define the *periodic cross-correlation* of u and v at a relative shift τ, $0 \leq \tau < N$, to be:

$$\mathrm{CC}(u,v)(\tau) = \sum_{i=0}^{N-1} x_i \cdot \overline{y_{i+\tau}}.$$

and call $CC(u,v)(\cdot)$ the *periodic cross-correlation function* of u and v. This function is a measure of the similarity of the sequences u and v at various shifts. We also define the *periodic auto-correlation* of u at a shift τ, $0 \leq \tau < N$, to be:

$$\mathrm{AC}(u)(\tau) = \mathrm{CC}(u,u)(\tau).$$

The periodic auto-correlation is a measure of the self-similarity of the sequence u when compared to shifts of itself. The auto-correlation of u at shift 0, $\mathrm{AC}(u)(0) = \sum_{i=0}^{N-1} |u_i|^2$, is in many applications a measure of the energy in the transmitted signal corresponding to sequence u. The auto-correlations of u at non-zero shifts are usually called *non-trivial auto-correlations.*

5.2 A Simplified Model for CDMA Communications

We next discuss a simplified model for CDMA communications. In our model, we have K users, all transmitting data simultaneously and without coordination or synchronisation on the same channel. The transmitted signal is the sum of users' individual signals, and is corrupted by noise. The users are transmitting to a single receiver, whose job it is to take the received signal and process it to obtain individual user's data.

Each user is assigned a *spreading code*, which in our model is just a complex-valued sequence of period N. User j is assigned the sequence

$$u^j = u^j_0, u^j_1, u^j_2, \ldots$$

To send a data bit $a_j \in \{0,1\}$, user j actually transmits the sequence $(-1)^{a_j} u^j$, i.e. the sequence of bits:

$$(-1)^{a_j} u^j_0, (-1)^{a_j} u^j_1, (-1)^{a_j} u^j_2, \ldots$$

In other words, he transmits a $\{+1,-1\}$-version of his data bit *spread* by his sequence u^j.

The received signal can be modelled by a sequence $s = s_0, s_1, s_2, \ldots$ where

$$s_i = \sum_{j=0}^{K-1} (-1)^{a_j} u^j_{i+\tau_j}.$$

Here τ_j is the *delay* of user j relative to the receiver. Because the users are transmitting in an uncoordinated fashion, these delays are unknown to the receiver. We have also assumed an ideal situation where there the transmission channel is noiseless.

Now suppose the receiver wishes to estimate the data bit a_ℓ for user ℓ. The receiver calculates, for each τ with $0 \leq \tau < N$, the function $\mathrm{CC}(s, u^\ell)(\tau)$. Notice that:

$$\begin{aligned}
\mathrm{CC}(s, u^\ell)(\tau) &= \sum_{i=0}^{N-1} \left(\sum_{j=0}^{K-1} (-1)^{a_j} u^j_{i+\tau_j} \right) \cdot \overline{u^\ell_{i+\tau}} \\
&= \sum_{j=0}^{K-1} \left(\sum_{i=0}^{N-1} ((-1)^{a_j} u^j_{i+\tau_j} \cdot \overline{u^\ell_{i+\tau}} \right) \\
&= (-1)^{a_\ell} \mathrm{AC}(u^\ell)(\tau - \tau_l) + \sum_{j \neq \ell} (-1)^{a_j} \mathrm{CC}(u^j, u^\ell)(\tau - \tau_j).
\end{aligned}$$

Now suppose that all the non-trivial autocorrelations and all the cross-correlations of the sequences u^j are small. In other words, we assume that for every ℓ and $\tau \neq 0$, $\mathrm{AC}(u^\ell)(\tau)$ is small and that for every j, ℓ and every τ, $\mathrm{CC}(u^j, u^\ell)(\tau)$ is small.

Then when $\tau = \tau_\ell$, the expression above for $\mathrm{CC}(s, u^\ell)(\tau)$ has a first term $(-1)^{a_\ell}\mathrm{AC}(u^\ell)(0)$ whose sign reveals a_ℓ, and whose relatively large magnitude dominates the remaining correlation terms. When $\tau \neq \tau_\ell$ then all the terms are small. Thus the receiver, after calculating $\mathrm{CC}(s, u^\ell)(\tau)$ for each τ should focus on the largest resulting correlation value to estimate the delay τ_ℓ and use the sign of this value to estimate the data bit a^ℓ.

Clearly, the success of this approach to transmitting information crucially depends on the term $(-1)^{a_\ell}\mathrm{AC}(u^\ell)(0)$ not being swamped by the other correlations. In other communications applications, for example, in synchronisation, single sequences with small non-trivial auto-correlations are called for. Thus we are motivated to consider the following basic sequence design problem:

> For a set $\mathcal{U}$ containing K complex-valued sequences of period N, define
>
> $$\mathrm{AC}_{\max}(\mathcal{U}) = \max_{u \in \mathcal{U},\ 1 \leq \tau < N} |\mathrm{AC}(u)(\tau)|,$$
>
> $$\mathrm{CC}_{\max}(\mathcal{U}) = \max_{u \neq v \in \mathcal{U},\ 0 \leq \tau < N} |\mathrm{CC}(u, v)(\tau)|.$$
>
> and
>
> $$\mathrm{C}_{\max}(\mathcal{U}) = \max\{\mathrm{AC}_{\max}, \mathrm{CC}_{\max}\}.$$
>
> Find sequence sets $\mathcal{U}$ which minimise $\mathrm{AC}_{\max}(\mathcal{U})$ (when $K = 1$) or $\mathrm{C}_{\max}(\mathcal{U})$ (when $K > 1$).

There are a number of lower bounds on $\mathrm{C}_{\max}(\mathcal{U})$ for sequence sets consisting of K sequences of period N [30, 51, 59, 67] which can be used to judge how good a particular design is.

For further details of how sequence sets with favourable correlation properties can be exploited in communications applications, see [9, 13, 14, 53, 57, 60].

5.3 The m-sequences and Their Periodic Correlations

We introduce a class of sequences, called the m-sequences, which have good auto-correlation properties.

Let α be a primitive element of $\mathbb{F}_{2^n}$. The sequence $s = s_0, s_1, \ldots$ with

$$s_i = tr_1^n(\beta\alpha^i)$$

is called a *binary m-sequence*. Because α is an element of period $2^n - 1$ in $\mathbb{F}_{2^n}$, the sequence s has period $2^n - 1$. Notice that taking one period of an m-sequence gives us a length $2^n - 1$ vector that is a codeword of the simplex code. From the equi-distribution property of the trace map, we see that s contains 2^{n-1} ones and $2^{n-1} - 1$ zeros in a period. We define a related $\{+1, -1\}$-valued sequence u of period $2^n - 1$ by $u_i = (-1)^{s_i}$.

Lemma 2. *Let s be a binary m-sequence of period $2^n - 1$ and let u be the corresponding complex-valued sequence. Then for $\tau \neq 0 \bmod 2^n - 1$, we have $AC(u)(\tau) = -1$.*

Proof. We have:

$$\begin{aligned}
\mathrm{AC}(u)(\tau) &= \sum_{i=0}^{2^n-2} (-1)^{s_i} \cdot \overline{(-1)^{s_{i+\tau}}} \\
&= \sum_{i=0}^{2^n-2} (-1)^{\mathrm{tr}_1^n(\alpha^i)} \cdot (-1)^{\mathrm{tr}_1^n(\alpha^{i+\tau})} \\
&= \sum_{i=0}^{2^n-2} (-1)^{\mathrm{tr}_1^n[(1+\alpha^\tau)\alpha^i]} \\
&= \sum_{x \in \mathbb{F}_{2^n}^*} \chi_\gamma(x) \quad \text{where } \gamma = 1 + \alpha^\tau \\
&= -1 + \sum_{x \in \mathbb{F}_{2^n}} \chi_\gamma(x) \\
&= -1
\end{aligned}$$

where we have again used (1) and the fact that $\gamma = 1 + \alpha^\tau \neq 0$ provided $\tau \neq 0 \bmod 2^n - 1$. □

Of course, for m-sequences to be useful in applications, we need to have a convenient method for generating them. It turns out that an m-sequence of period $2^n - 1$ satisfies a linear recurrence relation of degree n and can be generated using a simple electronic device called a Linear Feedback Shift Register. For more details, see [31, 32].

5.4 Sequence Sets from m-sequences

Since the auto-correlations of m-sequences are so neatly described, might we not expect the cross-correlations of two different m-sequences to be calculable? In fact, we can always express such cross-correlations as a Weil exponential sum, as we now show.

Let β be a second primitive element of $\mathbb{F}_{2^n}$ and define a second m-sequence $t = t_0, t_1, \ldots$ by $t_i = \mathrm{tr}_1^n(\beta^i)$. Since α and β are both primitive, we can write $\beta = \alpha^d$ for some d with $\gcd(d, 2^n - 1) = 1$. We also define a $\{+1, -1\}$-valued sequence v corresponding to t.

Now consider the cross-correlation:

$$\begin{aligned}
\mathrm{CC}(v,u)(\tau) &= \sum_{i=0}^{2^n-2} (-1)^{\mathrm{tr}_1^n(\alpha^{di})} \cdot (-1)^{\mathrm{tr}_1^n(\alpha^{i+\tau})} \\
&= \sum_{x \in \mathbb{F}_{2^n}^*} (-1)^{\mathrm{tr}_1^n(ax+x^d)} \qquad \text{where } a = \alpha^\tau \\
&= -1 + \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^n(ax+x^d)}.
\end{aligned}$$

More generally, if we consider the sequence set $\mathcal{G}$ consisting of u, v and the term-by-term product of u with all the cyclic shifts of v, then any cross- or auto-correlation of sequences in this set of size $2^n + 1$ can be expressed in a similar way as a Weil exponential sum involving functions of the form $g(x) = ax + x^d$.

In certain special cases, not only can the sums (and therefore $\mathrm{C}_{\max}(\mathcal{G})$) be bounded, but the spectrum of values taken on by the correlations as the pairs of sequences range over $\mathcal{G}$ can be calculated explicitly.

For example, when $d = 2^k + 1$, n is odd and $\gcd(n, k) = 1$, Gold [15, 16] showed that $\mathrm{C}_{\max}(\mathcal{G}) = t(n)$ where $t(n) = 1 + 2^{\lfloor (n+2)/2 \rfloor}$, and that the values taken on by non-trivial correlations of sequences in $\mathcal{G}$, called a Gold code, lie in the set $\{-1, -t(n), t(n) - 2\}$. It can also be shown that the set $\mathcal{G}$ has optimal correlation properties, meeting a lower bound of [59] on the correlations of *binary* sequence sets.

More general results of this type are summarised in [53, Theorem 1]. The analysis used to prove these correlation results is interesting in itself, though not a direct application of exponential sums. One shows that, by choosing a basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, the functions $\mathrm{tr}_1^n(ax + x^d)$ can be described by quadratic forms in n variables over $\mathbb{F}_2$ for these special d. Essentially, this is because the exponent d has a binary expansion of weight 2. According to the theory of Dickson [34, Theorems 4 and 5, Chapter 15], the distribution of values taken on by such a form is determined by an invariant called the *rank* of the form. This rank, and therefore the spectrum of correlation values, depends on the parameters

k and n and can be explicitly calculated. We refer the reader to [35] for a nice treatment of this topic.

Also of special note are very recent results [10, 11, 20] which together resolve the long-standing Welch and Niho conjectures concerning the correlation spectra in the cases $d = 2^m + 3$, $n = 2m + 1$ and $d = 2^{2r} + 2^r - 1$, $4r + 1 = 0 \bmod n$, respectively.

Among the many papers considering other families of sequence sets with good correlation properties are [3, 17, 24, 40–43, 50, 56]. See also the survey by Helleseth and Kumar in [47, Vol. II].

5.5 Sequence Sets from Dual BCH Codes

We will examine in more detail the correlations a family of sequences obtained from the dual BCH codes. Let $\mathcal{G}_t^*$ denote the set of polynomials

$$\mathcal{G}_t^* = \{x + g_3x^3 + \cdots + g_{2t-1}x^{2t-1} : g_i \in \mathbb{F}_{2^n}\}.$$

For each $g \in \mathcal{G}$, define a period $2^n - 1$, binary sequence s_g with terms $(s_g)_i$ where

$$(s_g)_i = \mathrm{tr}_1^n(g(\alpha^i)), \quad i \geq 0$$

and let u_g be the $\{+1, -1\}$-valued sequence corresponding to s_g. We define two sequence sets $\mathcal{S}_t$, $\mathcal{U}_t$ by:

$$\mathcal{S}_t = \{s_g : g \in \mathcal{G}_t^*\}, \quad \mathcal{U}_t = \{u_g : g \in \mathcal{G}_t^*\}.$$

We see that the sequences in $\mathcal{U}_t$ are $\{+1, -1\}$ versions of the sequences in $\mathcal{S}_t$ and that $|\mathcal{S}_t| = |\mathcal{U}_t| = 2^{n(t-1)}$. Single periods of the sequences of $\mathcal{S}_t$ are just codewords of the dual BCH code $\mathcal{C}_t$ that are all distinct under cyclic shifting (this explains the restriction to polynomials with coefficient of x equal to 1 in the definition of $\mathcal{G}_t^*$). For example, when $t = 1$, the single sequence in $\mathcal{S}_t$ is just an m-sequence coming from the simplex code.

Consider a pair of sequences u_g and u_h from $\mathcal{U}_t$, where

$$g(x) = x + \sum_{i=0}^{t-1} g_{2i+1}x^{2i+1}, \quad h(x) = x + \sum_{i=0}^{t-1} h_{2i+1}x^{2i+1}.$$

Then a straightforward calculation shows that

$$\mathrm{CC}(u_g, u_h)(\tau) = -1 + \sum_{x \in \mathbb{F}_{2^n}} \chi_1(e(x))$$

where $e(x)$ is the polynomial

$$(1+\alpha^{\tau})x+\sum_{i=0}^{t-1}(g_{2i+1}+\alpha^{(2i+1)\tau}h_{2i+1})x^{2i+1}.$$

So the correlations of sequences in our set can be expressed as Weil exponential sums. Notice that if $\tau \neq 0 \bmod 2^n-1$, or if $g(x) \neq h(x)$ and $\tau = 0 \bmod 2^n-1$, then $e(x)$ is a non-zero polynomial of odd degree and lies in the set $\mathcal{G}_t$. A direct application of Result 1 yields:

Theorem 5. *The sequence set $\mathcal{U}_t$ contains $2^{n(t-1)}$ sequences of period 2^n-1 and satisfies $\mathrm{C}_{\max}(\mathcal{U}_t) \leq 1+(t-1)2^{(n+2)/2}$.*

There is a simple relationship between the correlations $\mathrm{CC}(u_g,u_h)(\tau)$ and the Hamming weights of words of $\mathcal{C}_t$, as we now show. The analysis above shows that c_e is in the code $\mathcal{C}_t$. We already know from (4) that

$$2^n-2\mathrm{wt}_H(c_e)=-1+\sum_{x\in\mathbb{F}_{2^n}}\chi_1(e(x))$$

so we have

$$\mathrm{CC}(u_g,u_h)(\tau)=2^n-2\mathrm{wt}_H(c_e),$$

an identity linking the correlations of pairs of sequences in $\mathcal{U}_t$ with the Hamming weight of a related codeword in $\mathcal{C}_t$.

When $t=1$, Theorem 5 gives us the correct bound on the non-trivial periodic auto-correlations of m-sequences. When $t=2$, the polynomials in $\mathcal{G}_2^*$ are of the form $x+g_3x^3$ and when n is odd, the sequence set $\mathcal{U}_2$ is a subset of the Gold code with $d=3$ (omitting just the sequence v from the Gold code). The theorem gives a bound on $\mathrm{C}_{\max}$ which is slightly weaker than Gold's bound. When n is even, we get a new sequence set satisfying $\mathrm{C}_{\max}(\mathcal{U}_2) \leq t(n)$. This set is a special case of what are called in [53] *Gold-like codes.*

6 Application: Aperiodic and Partial Correlations

Traditionally, it is the periodic auto- and cross-correlations of sequence sets discussed above that have received most attention in the literature. But *aperiodic* and *partial* correlations of sequences emerge as being at least if not more important parameters to study when more realistic models of communications systems are considered.

As usual, u and v will denote complex-valued sequences of period N. Aperiodic correlations are correlations taken over only finite sequences: suppose $0 \leq \tau < N$; Then the *aperiodic cross-correlation* between u and v at a relative shift τ, $0 \leq \tau < N$ is defined to be

$$\mathrm{ACC}(u,v)(\tau) = \sum_{i=0}^{N-\tau-1} u_i \cdot \overline{v_{i+\tau}}.$$

We can also define the *aperiodic auto-correlation function* of sequence u via:

$$\mathrm{AAC}(u)(\tau) = \mathrm{ACC}(u,u)(\tau).$$

Aperiodic correlations are important in, for example, CDMA systems where consecutive periods of a spreading sequence are used to spread different data bits [53, Section V].

Partial correlations are correlations taken over only subsequences of sequences: suppose $0 \leq j, \tau, \ell < N$. Then the *partial cross-correlation* between u and v of period N over the subsequence of length ℓ beginning at position j and with relative shift τ, denoted $\mathrm{PCC}(u,v)(j,k,\ell)$, is defined by

$$\mathrm{PCC}(u,v)(j,\tau,\ell) = \sum_{i=0}^{\ell-1} u_{j+i} \cdot \overline{v_{j+i+\tau}}.$$

Similarly, we define the *partial auto-correlation* by:

$$\mathrm{PAC}(u)(j,\tau,\ell) = \mathrm{PCC}(u,u)(j,\tau,\ell).$$

Notice that when $\ell = N$, the partial correlations revert to the usual periodic correlations. Partial correlations arise as natural parameters of study in CDMA systems where many (possibly several hundred) data bits are spread by each copy of a user's spreading sequence [48, 49, 55] and in systems [9, 14], where a long sequence (typically an m–sequence) is used for synchronisation, but where correlations are computed over only a short subsequence of that sequence for faster acquisition.

So we are motivated to study the problem of constructing sequence sets for which the maximum value of non-trivial aperiodic or partial correlation is as small as possible. But these correlations are much less well understood than periodic correlations. One reason for this is that in the periodic case, we can use the algebraic structure of, for example, a finite field to define sequences and their periodic correlations are then calculated from certain sums taken over the whole finite field. We have seen an example of this in our calculation of the periodic auto-correlations of m-sequences. In contrast, the corresponding aperiodic and partial correlations for such sequences lead to sums over only part of the finite field and the exponential sum results are no longer directly applicable. Nevertheless, as we show next, hybrid exponential sums can be employed to obtain bounds for these new correlations. We concentrate on partial correlations, though very similar methods can be used to handle aperiodic cases too. We make use of a technique called the Pólya-Vinogradov method. For a survey of applications of this technique in number theory and communications see [63] and for related results [29, 33, 52].

For $i \geq 0$ we define $\rho(j, \ell)_i$ by:

$$\rho(j,\ell)_i = \begin{cases} 1 \text{ if } j + kN \leq i < j + kN + \ell, \text{ for some } k \in \mathbf{Z}, \\ 0 \text{ otherwise.} \end{cases}$$

Then the sequence $\rho(j, \ell)$ has period N and we can write:

$$\mathrm{PCC}(u,v)(j,\tau,\ell) = \sum_{i=0}^{N-1} \rho(j,\ell)_i \cdot u_i \overline{v_{i+\tau}}. \tag{5}$$

Next we bring the Discrete Fourier Transform (DFT) of the sequence $\rho(j, \ell)$ into play. Generally, if $u = u_0, u_1, \ldots$ is a complex-valued sequence of period N and $\omega = \exp(2\pi i/N)$ then the sequence

$$\hat{u} = \hat{u}_0, \hat{u}_1, \ldots$$

with terms

$$\hat{u}_k = \sum_{i=0}^{N-1} u_i \omega^{ik}, \qquad k \geq 0$$

is called the *Discrete Fourier Transform (DFT) of* u. It is a simple exercise in manipulation of geometric series to show that u can be recovered from $\hat{u}$ via the *Inverse DFT*:

$$u_i = \frac{1}{N} \sum_{k=0}^{N-1} \hat{u}_k \omega^{-ik}, \qquad i \geq 0.$$

The sequence $\rho(j, \ell)$ has a particularly nice DFT:

Lemma 3. *Let $\rho(j,\ell)$ be defined as above. Then*

$$\widehat{\rho(j,\ell)}_k = \begin{cases} \omega^{jk} \cdot \frac{\omega^{\ell k}-1}{\omega^k - 1} & \textit{if } k \neq 0 \bmod N \\ \ell & \textit{if } k = 0 \bmod N \end{cases}$$

Replacing terms of $\rho(j,\ell)$ in (5) by expressions involving the inverse DFT, we get:

$$\mathrm{PCC}(u,v)(j,\tau,\ell) = \frac{1}{N}\sum_{i=0}^{N-1}\sum_{k=0}^{N-1}\widehat{\rho(j,\ell)}_k\omega^{-ik}\cdot u_i\overline{v_{i+\tau}}$$

and then reversing the order of summation:

$$\mathrm{PCC}(u,v)(j,\tau,\ell) = \frac{1}{N}\sum_{k=0}^{N-1}\widehat{\rho(j,\ell)}_k\left(\sum_{i=0}^{N-1}u_i\overline{v_{i+\tau}}\cdot\omega^{-ik}\right).$$

Now consider a non-trivial partial auto-correlation of the $\{+1,-1\}$-valued version of a period $N = 2^n - 1$ m-sequence. We take $u = v$ and $u_i = (-1)^{\mathrm{tr}_1^n(\alpha^i)}$ for some primitive element $\alpha \in \mathbb{F}_{2^n}$ in the above expression. We also take $\tau \neq 0 \bmod 2^n - 1$ and define $\gamma = 1 + \alpha^\tau$ so that $\gamma \neq 0$. Then we have, for $k \neq 0$,

$$\begin{aligned}\sum_{i=0}^{N-1}u_i\overline{u_{i+\tau}}\cdot\omega^{-ik} &= \sum_{i=0}^{N-1}(-1)^{\mathrm{tr}_1^n(\gamma\alpha^i)}\omega^{-ik} \\ &= \sum_{x\in\mathbb{F}_{2^n}^*}\chi_\gamma(x)\psi_{-k}(x) \qquad \text{(substituting } x = \alpha^i\text{)} \\ &= G(\chi_\gamma,\psi_{-k}),\end{aligned}$$

a Gaussian sum. Separating the contributions due to $k = 0$ and $k \neq 0$ and using $\widehat{\rho(j,\ell)}_0 = \ell$ we get:

$$\mathrm{PAC}(u)(j,\tau,\ell) = \frac{\ell}{N}\cdot\mathrm{AC}(u)(\tau) + \frac{1}{N}\sum_{k=1}^{N-1}\widehat{\rho(j,\ell)}_k\cdot G(\chi_\gamma,\psi_{-k})$$

showing that the partial auto-correlation of an m-sequence can be expressed as a sum involving Gaussian sums and a periodic auto-correlation term. To get a bound on $|\mathrm{PAC}(u)(j,\tau,\ell)|$, we use the facts that $\mathrm{AC}(u)(\tau) = -1$ and $|G(\chi_\gamma,\psi_{-k})| = 2^{n/2}$ with the triangle inequality. We obtain:

$$|\mathrm{PAC}(u)(j,\tau,\ell)| \leq \frac{\ell}{N} + \frac{2^{n/2}}{N}\cdot\sum_{k=1}^{N-1}\left|\widehat{\rho(j,\ell)}_k\right| \qquad (6)$$

and we are now left with the problem of estimating a sum involving terms of the DFT of $\rho(j,\ell)$. A bound of $N\log N$ for this sum in the case $j=0$ is reported by Vinogradov [65]; improvements in the constant have been obtained since by Sarwate [52]. Since $|\widehat{\rho(j,\ell)}_k| = |\widehat{\rho(0,\ell)}_k|$, Vinogardov's bound applies to the more general case of $j \neq 0$ too. Combining Vinogradov's bound with inequality (6) we obtain:

Theorem 6. *Let u be the $\{+1,-1\}$-valued version of an m-sequence of period $N=2^n-1$. Then for any j and any $\tau \neq 0$, we have*

$$|PAC(u)(j,\tau,\ell)| \leq 1 + (N+1)^{1/2}\log N.$$

An almost identical method can be used to bound the partial and aperiodic correlations of the sequence set $\mathcal{U}_t$. The only differences are that the Gauss sum is replaced by a hybrid exponential sum with polynomial argument, we use Result 3 rather than Result 2 to bound this sum, and we use Theorem 5 to bound the periodic cross-correlations of sequences from $\mathcal{U}_t$. See also [45] for applications of the Pólya-Vinogradov method to other sequence families and for a survey of other approaches to working with the partial correlations of sequence sets.

In this Section, we started with sequences with favourable periodic correlation properties and then looked at their partial correlations. But computational evidence [45] suggests that the bounds we can obtain using the Pólya-Vinogradov method are rarely tight. Is it possible to design sequence families with better partial correlations from scratch?

7 Application: The Power Control Problem in OFDM

Orthogonal Frequency Division Multiplexing (OFDM) is a communications technique that has recently seen rising popularity in wireless and wire-line communications [1, 2, 5, 6]. OFDM-based solutions have important advantages over more traditional data transmission approaches: OFDM has greater inherent resistance to a certain kind of noise called multi-path interference that plagues wireless communications, while implementations of OFDM systems can be realised using standard digital signal processing techniques and can avoid the use of an expensive channel equalisation process.

In an OFDM system, the transmitted signal is a sum of phase-shifted sinusoidal carriers, the phase shifts carrying the data. The data itself is coded because of channel noise. Given a length N binary code $\mathcal{C}$ and a codeword $c = (c_0, c_1, \dots, c_{N-1}) \in \mathcal{C}$, the transmitted signal at time t for the codeword c can be modelled as the real part of the sum

$$\sum_{j=0}^{N-1} (-1)^{c_j} e^{(2\pi i)jt}.$$

If we define a degree $N-1$ polynomial $c(z)$ by

$$c(z) = (-1)^{c_0} + (-1)^{c_1} z + \cdots + (-1)^{c_{N-1}} z^{N-1},$$

then the OFDM signal at time t is then just the real part of $c(e^{2\pi i t})$ so that the transmitted signal is related to the values of polynomials on $|z| = 1$, the unit circle in the complex plane.

The *envelope power* of the OFDM signal at time t is defined to be $|c(e^{2\pi i t})|^2$. The mean value of this function as t ranges over $[0,1]$ is equal to N (this can be shown simply by computing the integral of $|c(z)|^2 = c(z)\cdot c(1/z)$ around the unit circle). So we define the *peak-to-mean envelope power ratio* or PMEPR of the OFDM signal to be:

$$\mathrm{PMEPR}(c) = \frac{1}{N} \max_{|z|=1} |c(z)|^2$$

and the PMEPR of the code $\mathcal{C}$ to be:

$$\mathrm{PMEPR}(\mathcal{C}) = \frac{1}{N} \max_{c \in \mathcal{C}} \max_{|z|=1} |c(z)|^2.$$

The number $\mathrm{PMEPR}(\mathcal{C})$ is a measure of the dynamic range of the power in the OFDM signals that are obtained from the code $\mathcal{C}$. It is desirable to work with codes $\mathcal{C}$ which have 'small' values of PMEPR, acutely so for low-cost wireless applications. This is because a low value of PMEPR leads to signals that can be amplified by cheap electronic components without too much distortion being introduced, and which make efficient use of regulatory limits that are commonly imposed on the power of wireless signals. Notice that if $c = (0, 0, \dots, 0)$, then $\mathrm{PMEPR}(c) = N$. In fact this is the largest value of PMEPR that can occur, so by 'small' in this context we mean substantially less than N. We can summarise the *OFDM power control problem* as:

> Find binary codes $\mathcal{C}$ which simultaneously are good error correcting codes and have $\mathrm{PMEPR}(\mathcal{C})$ small.

For a summary of previous work on this problem and references to the engineering literature, see [46]. Here we will show how hybrid exponential sums (and a little analysis) can be used to obtain bounds on the PMEPRs of the non-zero words of dual BCH codes. A similar analysis for many other code families can be found in [46]. We also recommend [7, 44] for a completely different approach to the power control problem.

Consider then a general non-zero codeword c_g of the length $N = 2^n - 1$ dual BCH code $\mathcal{C}_t$. We have

$$(c_g)_j = \mathrm{tr}_1^n(g(\alpha^j)), \quad 0 \leq j < N,$$

where g is a polynomial of degree $2t - 1$ over $\mathbb{F}_{2^n}$ and α is primitive in $\mathbb{F}_{2^n}$. So the polynomial $c_g(z)$ corresponding to the codeword c_g is

$$c_g(z) = \sum_{j=0}^{N-1} (-1)^{\mathrm{tr}_1^n(g(\alpha^j))} z^j$$

and we want to obtain a bound for $\max_{|z|=1} |c_g(z)|^2$. Notice that at $z = e^{(2\pi i)\ell/N}$, an N-th root of unity, we have

$$c_g(e^{(2\pi i)\ell/N}) = \sum_{j=0}^{N-1} (-1)^{\mathrm{tr}_1^n(g(\alpha^j))} e^{(2\pi i)j\ell/N} = \sum_{x \in \mathbb{F}_{2^n}} \chi_1(g(x))\psi_\ell(x)$$

— a hybrid exponential sum with polynomial argument. When $\ell \neq 0$, the sum satisfies the conditions of Result 3 with $f(x) = x$ and $m = 1$. So we can immediately say:

$$|c_g(e^{(2\pi i)\ell/N})| \leq (2t-1)2^{n/2} \quad \text{for } \ell \neq 0.$$

On the other hand, for $\ell = 0$, we get:

$$|c_g(1)| = \left| \sum_{j=0}^{N-1} (-1)^{\mathrm{tr}_1^n(g(\alpha^j))} \right| = \left| -1 + \sum_{x \in \mathbb{F}_{2^n}} \chi_1(g(x)) \right| \leq 1 + (2t-2)2^{m/2}$$

according to Result 1. Thus we see that, at the N-th roots of unity, the polynomial $c_g(z)$ has absolute value no greater than $(2t-1)2^{n/2}$.

Now we convert this bound holding at the N-th roots of unity to a bound that is valid on the entire unit circle. We make use of the following lemma, obtained by bounding the coefficients that occur in a Lagrange interpolation of a degree $N - 1$ polynomial from the N-th roots of unity to $|z| = 1$:

Lemma 4. *[46] Let $c(z)$ be a degree $N-1$ polynomial and write $\gamma = e^{(2\pi i)/N}$. Then*

$$\max_{|z|=1} |c(z)| \le \left(\frac{2}{\pi}\log(2N)+2\right)\cdot \max_{0\le j<N} |c(\gamma^j)|.$$

The lemma shows that the interpolation can be achieved at the expense of a factor of $O(\log N)$. Combining the lemma with our exponential sum estimate, we obtain:

Theorem 7. *Let $\mathcal{C}_t^*$ denote the code obtained by removing the all-zero word from the length $N = 2^n - 1$ dual BCH code $\mathcal{C}_t$. Then*

$$\mathit{PMEPR}(\mathcal{C}_t^*) \le \frac{N+1}{N}\cdot(2t-1)^2\cdot\left(\frac{2}{\pi}\log(2N)+2\right)^2.$$

Thus the theorem shows that the PMEPR of the dual BCH codes is $O((\log N)^2)$ for fixed t and large N, clearly much better than the worst case PMEPR value of N. Notice however that for fixed t, we have shown the dual BCH codes to have normalised envelope power at most $(2t-1)^2$ at $t = \ell/N$, $0 \le \ell < N$. The factor of $(\log N)^2$ in the theorem comes from our use of Lagrange interpolation. This indicates that there is room for improvement in our bound on PMEPR($\mathcal{C}_t^*$). Indeed a result of [46] shows that there do exist codes which are asymptotically good (i.e. their normalised minimum distances and rates are both bounded away from zero as $N \to \infty$) and which have PMEPR growing only as $O(\log N)$. Unfortunately, the proof is non-constructive.

For a collection of open problems related to the power control problem, see the closing comments of [46].

8 Further Applications and Literature

In this section, we provide brief notes and pointers to some of the literature on exponential sums and applications that we have not touched upon in earlier sections.

Kloosterman sums [32, Chapter 5] in characteristic 2 are exponential sums of the form

$$\sum_{x\in\mathbb{F}_{2^n}} \chi(ax+\frac{b}{x}), \qquad a,b\in\mathbb{F}_{2^n}.$$

Their evaluation is intimately connected with counting points on *elliptic curves*. If a, b are not both zero, the sum can be bounded by $2\cdot 2^{n/2}$. In much the same way as for the dual BCH codes, we can define a Kloosterman code to be the set of words $c_{a,b}$ where

$$(c_{a,b})_i = \mathrm{tr}_1^n(a\alpha^i + \frac{b}{\alpha^i}), \qquad 0 \leq i < 2^n - 1,\ a, b \in \mathbb{F}_{2^n}\,.$$

It is easy to mimic our previous arguments to show that the Kloosterman code has minimum distance at least $2^{n-1} - 2^{n/2}$. In fact the complete distribution of weights occuring in this code has been calculated [28]. We can also define sequence sets with favourable periodic correlations using the Kloosterman code. The sequences are term-by-term sums of an m-sequence corresponding to a primitive element α and the shifts of its *reciprocal* m-sequence which comes from the element α^{-1}.

Kumar and Moreno [27] have used Deligne's results bounding the numbers of points on algebraic varieties to construct sequence families with good correlations. Their sequences have terms that are powers of a p-th root of unity (rather than the $\{+1, -1\}$-valued sequences we have studied here). They have also used Deligne's results to bound the minimum distances of certain binary codes [37]. These two papers contain a wealth of other references to previous work on codes and sequence designs. The Carlitz-Uchiyama/Weil bound has also been extended using Deligne's theorem and applied to coding theory [39].

Exponential sums have been applied to the study of the covering radii of BCH codes [19, 62] and Goppa codes [21, Section 12 and 13].

Exponential sums over Galois *rings* (rather than Galois fields) have recently received a lot of attention, beginning with the influential paper [18]. There are analogues of the Carlitz-Uchiyama/Weil bound [25] and of Result 3 for hybrid exponential sums [58]. These bounds have been used to construct quaternary codes with large minimum distances and to design quaternary (more generally p^ℓ-ary) sequence families with low periodic and aperiodic correlations. See also [26, 64] and the references therein for related sequence designs. The hybrid sum results of [58] were used in [46] to bound the PMEPR properties of some quaternary codes.

As we have already noted, a complete survey of the whole area of exponential sums and their applications can be found in [21]. We hope this paper serves as a useful introduction to what is a fascinating and thriving area.

References

1. M. Alard and R. Lasalle. Principles of modulation and channel coding for digital broadcasting for mobile receivers. *EBU Review*, 224: 47–69, Aug. 1987.

2. J.A.C. Bingham. Multicarrier modulation for data transmission: an idea whose time has come. *IEEE Commun. Magazine*, 28(1): 5–14, May 1990.
3. S. Boztas and P.V. Kumar. Binary sequences with Gold-like correlation but larger linear span. *IEEE Trans. Inform. Theory*, IT-40(2): 532–537, March 1994.
4. L. Carlitz and S. Uchiyama. Bounds for exponential sums. *Duke Math. J.*, 24:37–41, 1957.
5. P.S. Chow, J.M. Cioffi, and J.A.C. Bingham. DMT-based ADSL: concept, architecture, and performance. In *IEE Colloquium on 'High Speed Access Technology and Services, Including Video-on-Demand'*, pages 3/1–6, Oct. 1994.
6. L.J. Cimini, Jr. Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing. *IEEE Trans. Commun.*, 33:665–675, July 1985.
7. J.A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes. *IEEE Trans. Inform. Theory*, to appear Nov. 1999.
8. P. Deligne. La conjecture du W. *Publ. Math. IHES*, 43: 273–307, 1974.
9. R. C. Dixon. *Spread Spectrum Systems with Commercial Applications (3rd edition).* Wiley–Interscience, New York, 1994.
10. H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. *IEEE Trans. Inform. Theory*, IT-45: 1271–1275, 1999.
11. H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case. *Information and Computation*, to appear.
12. B. Dwork. On the rationality of the zeta function. *Amer. J. Math.*, 82:631–648, 1959.
13. P. Fan and M. Darnell. *Sequence design for communications applications.* John Wiley and Sons, New York, 1996.
14. H. Fukumasa, R. Kohno, and H. Imai. Pseudo–noise sequences for tracking and data relay satellite and related systems. *Trans. of IEICE*, E(5): 1137–1144, May 1991.
15. R. Gold. Optimal binary sequences for spread spectrum multiplexing. *IEEE Trans. Inform. Theory*, IT-13: 619–621, 1967.
16. R. Gold. Maximal recursive sequences with 3-valued cross-correlation functions. *IEEE Trans. Inform. Theory*, IT-14: 154–156, 1968.
17. G. Gong. Theory and applications of q–ary interleaved sequences. *IEEE Trans. Inform. Theory*, IT-41(2): 400–411, March 1995.
18. A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. *IEEE Trans. Inform. Theory*, IT-40: 301–319, 1994.
19. T. Helleseth. On the covering radius of cyclic linear codes and arithmetic codes. *Discrete. Appl. Math.*, 11: 157–173, 1985.
20. H. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences. *preprint*, 1999.
21. N.E. Hurt. Exponential sums and coding theory: A review. *Acta Applicandae Mathematicae*, 46: 49–91, 1997.
22. K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory (2nd edition), Graduate Texts in Mathematics Vol. 84.* Springer, Berlin, 1990.
23. D. Jungnickel. *Finite Fields — Structure and Arithmetics.* B.I. Wissenschaftsverlag, Mannheim, 1993.
24. A.M. Klapper. d–form sequences: Families of sequences with low correlation values and large linear spans. *IEEE Trans. Inform. Theory*, IT-41(2): 423–431, March 1995.

25. P.V. Kumar, T. Helleseth, and A.R. Calderbank. An upper bound for Weil exponential sums over Galois rings and applications. *IEEE Trans. Inform. Theory*, IT-41(2): 456–468, March 1995.
26. P.V. Kumar, T. Helleseth, A.R. Calderbank, and A.R. Hammons Jr. Large families of quaternary sequences with low correlation. *IEEE Trans. Inform. Theory*, IT-42(2): 579–592, March 1996.
27. P.V. Kumar and O. Moreno. Prime-phase sequences with periodic correlation properties better than binary sequences. *IEEE Trans. Inform. Theory*, IT-37(3): 603–616, May 1991.
28. G. Lachaud and J. Wolfmann. Sommes de kloosterman, coubes elliptiques et codes cycliques en caracteristique 2. *Comptes Rendu Academie Science Paris*, 305: 881–883, 1987.
29. J. Lahtonen. On the odd and aperiodic correlation properties of the Kasami sequences. *IEEE Trans. Inform. Theory*, IT-41(5): 1506–1508, Sept. 1995.
30. V.I. Levenshtein. Bounds on the maximal cardinality of a code with bounded modulus of the innner product. *Soviet Math. Dokl.*, 25(2): 526–531, 1982.
31. R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications (2nd Edition).* Cambridge University Press, Cambridge, 1994.
32. R. Lidl and H. Niederreiter. *Finite Fields.* Encyclopedia of Mathematics and Its Applications, Vol. 20 (2nd Edition), Cambridge University Press, Cambridge, 1997.
33. S. Litsyn and A. Tietäväinen. Character sum constructions of constrained error-correcting codes. *AAECC*, 5: 45–51, 1994.
34. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* North Holland, Amsterdam, 1977.
35. R.J. McEliece. *Finite fields for computer scientists and engineers.* Kluwer, Boston, 1987.
36. C.J. Moreno. *Algebraic Curves over Finite Fields.* Cambridge University Press, Cambridge, 1991.
37. O. Moreno and P.V. Kumar. Minimum distance bounds for cyclic codes and Deligne's theorem. *IEEE Trans. Inform. Theory*, IT-39(5): 1524–1534, Sept. 1993.
38. O. Moreno and C.J. Moreno. The MacWilliams-Sloane conjecture on the tightness of the Carlitz-Uchiyama bound and the weights of duals of BCH codes. *IEEE Trans. Inform. Theory*, IT-40(6): 1894–1907, Nov. 1994.
39. O. Moreno, V.A. Zinoviev, and P.V. Kumar. An extension of the Weil-Carlitz-Uchiyama bound. *Finite Fields and their Applications*, 1: 360–371, 1995.
40. J.-S. No. Generalization of GMW sequences and No sequences. *IEEE Trans. Inform. Theory*, IT-42(1): 260–262, Jan. 1996.
41. J.-S. No and P.V. Kumar. A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span. *IEEE Trans. Inform. Theory*, IT-35(2):371–379, March 1989.
42. J.D. Olsen, R.A. Scholtz, and L.R. Welch. Bent–function sequences. *IEEE Trans. Inform. Theory*, IT-28(6): 858–864, Nov. 1982.
43. K.G. Paterson. Binary sequence sets with favourable correlation properties from difference sets and MDS codes. *IEEE Transactions on Information Theory*, 44:172–180, 1998.
44. K.G. Paterson. Generalised Reed-Muller codes and power control in OFDM. *IEEE Transactions on Information Theory*, to appear.
45. K.G. Paterson and P.J.G. Lothian. Bounds on partial correlations of sequences. *IEEE Transactions on Information Theory*, 44:1164–1175, 1998.

46. K.G. Paterson and V. Tarokh. On the existence and construction of good codes with low peak-to-average power ratios. *Hewlett-Packard Laboratories Technical Report HPL-1999-51, submitted*, 1999. `http://www.hpl.hp.com/techreports/1999/HPL-1999-51.html`.
47. V.S. Pless and W. Huffman, eds. *Handbook of Coding Theory Vols. I & II.* Elsevier, 1998.
48. M.B. Pursley. On the mean-square partial correlation of periodic sequences. In *Proc. of Conf. on Information Sciences and Systems*, pages 377–379, John Hopkins Univ., Baltimore MD, March 28–30 1979.
49. M.B. Pursley, D.V. Sarwate, and T.U. Basar. Partial correlation effects in direct–sequence spread–spectrum multiple–access communications systems. *IEEE Trans. Commun.*, COM-32(5): 567–573, May 1984.
50. L.C. Quynh and S. Prasad. New class of sequences sets with good auto- and crosscorrelation functions. *IEE Proc. (F)*, 133(3): 281–287, June 1986.
51. D.V. Sarwate. Bounds on crosscorrelation and autocorrelation of sequences. *IEEE Trans. Inform. Theory*, IT-25(6): 720–724, Nov. 1979.
52. D.V. Sarwate. An upper bound on the aperiodic autocorrelation function for a maximal-length sequence. *IEEE Trans. Inform. Theory*, IT-30(4): 685–687, July 1984.
53. D.V. Sarwate and M.B. Pursley. Cross-correlation properties of pseudorandom and related sequences. *Proc. IEEE*, 68: 593–618, May 1980.
54. W. Schmidt. *Equations Over Finite Fields — An Elementary Approach. Lecture Notes in Mathematics, Vol. 536.* Springer, Berlin, 1976.
55. R.A. Scholtz. Criteria for sequence set design in CDMA communications. In G. Cohen, T. Mora, and O. Moreno, editors, *Applied Algebra, Algebraic Algorithms and Error–Correcting Codes (AAECC–10)* , pages 57–65, Puerto Rico, May 10–14 1993. Springer-Verlag, Berlin.
56. R.A. Scholtz and L.R. Welch. GMW sequences. *IEEE Trans. Inform. Theory*, IT-30(3): 548–553, Nov. 1984.
57. M.R. Schroeder. *Number Theory in Science and Communication (3rd edition).* Springer, Berlin, 1997.
58. A.G. Shanbag, P.V. Kumar, and T. Helleseth. Upper bound for a hybrid sum over Galois rings with applications to aperiodic correlation for some q-ary sequences. *IEEE Trans. Inform. Theory*, IT-42: 250–254, 1996.
59. V.M. Sidelnikov. On mutual correlation of sequences. *Soviet Math. Dokl.*, 12(1): 197–201, 1971.
60. M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt. *Spread Spectrum Communications, Vol. 1.* Computer Science Press, Rockville, MD, 1985.
61. H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer-Verlag, New York, 1993.
62. A. Tietäväinen. An asymptotic bound on the covering radii of binary bch codes. *IEEE Trans. Inform. Theory.*, IT-36: 211–213, 1990.
63. A. Tietäväinen. Vinogradov's method and some applications. Technical Report TUCS No. 28, Turku Centre for Computer Science, Turku, Finland, 1996.
64. P. Udaya and M.U. Siddiqi. Optimal biphase sequences with large linear complexiy derived from sequences over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory*, IT-42(1): 206–216, Jan. 1996.
65. I.M. Vinogradov. *Elements of Number Theory.* Dover, New York, 1954.
66. A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent, Actualités Sci. et Ind. no. 1041.* Hermann, Paris, 1948.

67. L.R. Welch. Lower bounds on the maximum correlation of signals. *IEEE Trans. Inform. Theory*, IT-20(3): 397–399, May 1974.