Close encounters with Boolean functions of three different kinds*

Matthew G. Parker

The Selmer Centre
Department of Informatics, University of Bergen
P.O. Box 7800, N-5020 Bergen, Norway
matthew@ii.uib.no
http://www.ii.uib.no/~matthew/

Abstract. Complex arrays with good aperiodic properties are characterised and it is shown how the joining of dimensions can generate sequences which retain the aperiodic properties of the parent array. For the case of $2 \times 2 \times \ldots \times 2$ arrays we define two new notions of aperiodicity by exploiting a unitary matrix represention. In particular, we apply unitary rotations by members of a size-3 cyclic subgroup of the local Clifford group to the aperiodic description. It is shown how the three notions of aperiodicity relate naturally to the autocorrelations described by the action of the Heisenberg-Weyl group. Finally, after providing some cryptographic motivation for two of the three aperiodic descriptions, we devise new constructions for complementary pairs of Boolean functions of three different kinds, and give explicit examples for each.

Key words: Aperiodic autocorrelation, complementary sequences, local Clifford group, Heisenberg-Weyl group, Boolean functions, Pauli group, quantum codes, graph states

1 Introduction

Boolean functions with desirable properties are required in many fields, and are used, in particular, as components in both cryptosystems and communications systems [17]. In the former, one typically requires the Boolean function to be robust to linear and differential approximations [8], and in the latter, one requires the one-dimensional sequences derived from Boolean functions, to have an 'evenly-spread' Fourier spectrum and low magnitude out-of-phase autocorrelation sidelobes [21]. Such technical demands are often met by Boolean functions and sequences which are spectrally optimal in a periodic sense, that is they have Fourier spectra which are well-controlled at certain spectral points. However, at least for sequences for communications, one often requires an evenly-spread Fourier spectrum over a continuum of points [10]. This translates into a requirement for low magnitude out-of-phase *aperiodic autocorrelation* sidelobes [12].

* This work was supported by the Norwegian Research Council.

Constructions of Boolean functions with good aperiodic properties is not a well-developed area of research in cryptography [12, 9].

In this paper we start by considering the problem of designing bipolar sequences with good aperiodic properties. We then extend this problem to the design of bipolar arrays with good aperiodic properties and show how, for 'perfect' arrays, their aperiodic properties can be carried over to related sequences, where the sequences are obtained from the arrays by recursive *joining* of dimensions [22, 23, 13] We also show how to interpret this relationship in the Fourier domain.

We then focus on the construction of bipolar arrays in $\mathcal{C}_2^n$, which can be described by *generalised Boolean functions*, where these functions have good aperiodic properties [9]. By re-expressing the autocorrelation and Fourier properties of these functions using unitary matrix terminology, we view our problem within a wider context, where the multidimensional continuous discrete Fourier transform is a tensor product of members of an infinite-size set of 2×2 unitary matrices [25, 19, 28]. We call this set of 2×2 unitaries the *type-I* set. We then identify a size-3 cyclic subgroup, $\mathbb{T}$, of the *local Clifford group*, comprising 2×2 unitaries, where $\mathbb{T} = \{I, \lambda, \lambda^2\}$, and, by right-multiplication (rotation) of each member of the type-I set by λ, the generator of $\mathbb{T}$, and by λ^2, we generate two more infinite-size sets of 2×2 unitary matrices, respectively, namely the *type-II* and *type-III* sets. The problem of constructing arrays in $\mathcal{C}_2^n$ (generalised Boolean functions) with good aperiodic autocorrelation properties is related to the flatness of the spectrum resulting from the multiplicative left-action of any matrix which is a tensor product of type-I unitaries on the array. Further, the type-II and type-III matrix sets highlight new 'aperiodic' questions for the array. Therefore we consider three different kinds of aperiodic property of a Boolean function, where the 'type-I' kind relates to conventional aperiodicity.

Having characterised type-I, type-II, and type-III aperiodicity, we then give some cryptographic meaning to the properties possessed by Boolean functions which are type-I or type-II optimal. We also place the three kinds of array into a more general context by considering arrays which are optimal, in some sense, with respect to the action of the *Heisenberg-Weyl* (or *Pauli*) group [11]. Type-I, II, and III properties relate to the action of the Heisenberg-Weyl group under some restrictions. Moreover, those quadratic Boolean functions which represent one-dimensional *quantum codes* with good distance [9, 4] also have good properties with respect to the action of the Heisenberg-Weyl group.

We would particularly like to construct Boolean functions with perfect aperiodic properties (i.e. whose aperiodic autocorrelation sidelobes are of zero magnitude), as applying the joining described above would preserve these perfect properties, but such functions do not exist, so we therefore propose to construct *pairs* of Boolean functions whose out-of-phase aperiodic sidelobes sum to zero. These are, by definition, *Golay complementary array pairs*. A construction exists for complementary sequences, as proposed by Golay [14, 15], and Shapiro-Rudin [31], and later generalised by Turyn [30]. Pairs of Boolean functions constructed via an array form of the Golay-Turyn [24, 23, 13] construction have optimised

type-I properties. We call such a pair a *type-I pair*. By rotating a type-I pair by λ and by λ^2, respectively, we obtain a *type-II pair*, and a *type-III pair*, respectively. But a more general result can be obtained by rotating the Golay-Turyn construction itself. By rotating the Golay-Turyn construction by λ and by λ^2 we obtain two 'new' constructions which we call type-II and type-III complementary constructions, respectively. In particular, in addition to the type-I complementary pairs, this allows us to construct, directly, pairs of Boolean functions which are type-II and type-III complementary, respectively.

We finish by presenting some open problems arising from the paper.

2 Aperiodic autocorrelation and the continuous Fourier transform

Let $\tilde{A} \in \mathcal{C}_N = (\tilde{A}_0, \tilde{A}_1, \ldots, \tilde{A}_{N-1})$ be a finite sequence of N complex numbers, where we take the convention that neither of the two end elements, $\tilde{A}_0$ and $\tilde{A}_{N-1}$, are zero. We represent the sequence $\tilde{A}$ by the polynomial $\tilde{A}(y) = \tilde{A}_0 + \tilde{A}_1 y + \ldots + \tilde{A}_{N-1} y^{N-1}$. The aperiodic autocorrelation of $\tilde{A}$ is then given by the coefficients of $K_{\tilde{A}}(y) = K_{\tilde{A}_{1-N}} y^{1-N} + \ldots + K_{\tilde{A}_{-1}} y^{-1} + K_{\tilde{A}_0} y^0 + K_{\tilde{A}_1} y^1 + \ldots + K_{\tilde{A}_{N-1}} y^{N-1}$, where

$$K_{\tilde{A}}(y) = \frac{\tilde{A}(y)\tilde{A}^*(y)}{||\tilde{A}||^2},$$

where $\tilde{A}^*(y) = \overline{\tilde{A}(y^{-1})}$, and $\overline{x}$ means x with complex-conjugated coefficients. We desire all out-of-phase sidelobes of the aperiodic autocorrelation of $\tilde{A}$ to be of low magnitude, which means that we want $K_{\tilde{A}_j}$ to have low magnitude $\forall j \neq 0$. Ideally we would like all $K_{\tilde{A}_j} = 0$ for $j \neq 0$, in which case $K_{\tilde{A}}(y) = 1$ is called a *δ-function*, independent of y, but this is impossible for $N \geq 2$. We later discuss how to obtain an ideal (δ-function) response for the sum of the aperiodic autocorrelations of a pair of sequences.

The continuous Fourier power spectrum of $\tilde{A}$ is the set of evaluations of $K_{\tilde{A}}(y)$ on the unit circle and is summarised by

$$\mathcal{F}(\tilde{A}) = \{K_{\tilde{A}}(\upsilon) \quad | \quad |\upsilon| = 1\}.$$

If $\tilde{A}$ had a perfect response then $\mathcal{F}(\tilde{A}) = \{1\}$, i.e. the Fourier power spectrum would be *flat*. More realistically, if $\tilde{A}$ has a near-perfect aperiodic autocorrelation response then, loosely, its Fourier power spectrum is *near-flat*. We later discuss how to obtain a flat power spectrum for the sum of the Fourier power spectra of a pair of sequences, implying that the power spectrum for each member of the pair is near-flat.

3 Aperiodic autocorrelation of arrays and the multi-dimensional continuous Fourier transform

Let $A \in \mathcal{C}_{N_0} \times \mathcal{C}_{N_1} \times \ldots \times \mathcal{C}_{N_{n-1}}$ be an n-dimensional array with $\prod_{j=0}^{n-1} N_j$ complex elements where, to avoid degeneracy, we take the convention that no 'surface' of

the array can have elements which are all zero, i.e. for each dimension index, h, the set of elements $\{A_{0,\ldots,0,k,0,\ldots,0} \quad | \quad \forall k\}$ and $\{A_{N_0-1,\ldots,N_{h-1}-1,k,N_{h+1}-1,\ldots,N_{n-1}-1} \quad | \quad \forall k\}$ must each include at least one non-zero entry. The aperiodic autocorrelation, $K_A(z)$, of A is given by

$$K_A(z) = \frac{A(z)A^*(z)}{||A||^2}, \tag{1}$$

where $z = (z_0, z_1, \ldots, z_{n-1})$, $z^{-1} = (z_0^{-1}, z_1^{-1}, \ldots, z_{n-1}^{-1})$, and the coefficients of $A(z)$ are the array elements of A, i.e. $A(z) = \sum_{j \in \mathcal{Z}_{N_0} \times \mathcal{Z}_{N_1} \times \ldots \times \mathcal{Z}_{N_{n-1}}} A_j z_0^{j_0} z_1^{j_1} \ldots z_{n-1}^{j_{n-1}}$. We desire all out-of-phase sidelobes of the aperiodic autocorrelation of A to be of low magnitude, which means that we want K_{A_j} to have low magnitude $\forall j \in \mathcal{Z}_{N_0} \times \mathcal{Z}_{N_1} \times \ldots \times \mathcal{Z}_{N_{n-1}}$, $j \neq 0$. Ideally we would like all $K_{A_j} = 0$ for $j \neq 0$, in which case $K_A(z) = ||A||^2$ is a *δ-function*, independent of z, but, as with the sequence case, this is impossible. We later discuss how to obtain an ideal (δ-function) response for the sum of the aperiodic autocorrelations of a pair of arrays.

The continuous Fourier power spectrum of the array A is given by the set of evaluations of $K_A(z)$ on the multi-unit circle, and is summarised by

$$\mathcal{F}(A) = \{K_A(\upsilon) \quad | \quad |\upsilon_j| = 1, 0 \leq j < n\}, \tag{2}$$

where $\upsilon = (\upsilon_0, \upsilon_1, \ldots, \upsilon_{n-1})$. If A had a perfect response then $\mathcal{F}(A) = \{1\}$, i.e. the Fourier power spectrum would be *flat* everywhere. More realistically, if A has a near-perfect aperiodic autocorrelation then, loosely, its Fourier power spectrum is *near-flat*. We later discuss how to obtain a flat power spectrum for the sum of the Fourier power spectra of a pair of Golay complementary arrays.

4 Sequences obtained by joining array dimensions

Let A be a $N = N_0 \times N_1 \times \ldots \times N_{n-1}$ complex array of n dimensions, as represented by the polynomial $A(z) = A(z_0, z_1, \ldots, z_{n-1})$. Then, by substituting into $A(z)$ the variables $z_0 = y$, and $z_k = z_{k-1}^{N_{k-1}}$, $\forall k$, $1 \leq k < n$, we obtain the univariate polynomial $\tilde{A}(y)$ whose coefficients represent a sequence of length N. The important point about these substitutions is that they ensure that the elements of both the array, A, and derived sequence, $\tilde{A}$, are taken from the same alphabet [*]. We refer to this series of substitutions as the *joining* of dimensions [13]. By an identical series of substitutions in $K_A(z)$, which is the aperiodic autocorrelation of the array $A(z)$, one obtains the aperiodic autocorrelation, $K_{\tilde{A}}(y)$, of the sequence, $\tilde{A}(y)$. This is not the only possible substitution for $A(z)$ and $K_A(z)$, as, at the array level, the ordering of variables z_0, z_1, ... etc, is arbitrary. Thus, more generally, one can apply the series of substitutions $z_{\pi(0)} = y$, and $z_{\pi(k)} = z_{\pi(k-1)}^{N_{\pi(k-1)}}$, $\forall k$, $1 \leq k < n$, where $\pi \in \mathcal{S}_n$ is any permutation of $\{0, 1, \ldots, n-1\}$. Moreover the ordering of coefficients in one or more

[*] We do not consider, in this paper, the alternative substitution strategy using the Chinese Remainder theorem when the dimensions are relatively prime.

dimensions, j, may be reversed and/or multiplied by a unit phase, α, $|\alpha| = 1$, without changing the aperiodic coefficient magnitudes, and these symmetries can be expressed by replacing z_j by $\alpha_j z_j^{\pm 1}$ for all dimensions to be reversed and/or phase-shifted. Thus, each array, $A(z)$, can generate a family of sequences $\{\tilde{A}\} = \{A(z) \quad | \quad z_{\pi(0)} = y, z_{\pi(k)} = \alpha_k z_{\pi(k-1)}^{\pm N_{\pi(k-1)}}, |\alpha_k| = 1, 1 \leq k < n, \forall \pi \in \mathcal{S}_n\}$, each with the same aperiodic autocorrelation, $K_{\tilde{A}}$, where the number of distinct sequences in the family depends on internal symmetries of the specific array.

All sequences in family $\{\tilde{A}\}$ have an aperiodic autocorrelation, given by $K_{\tilde{A}}$, where the coefficients of $K_{\tilde{A}}$ are a relatively straightforward combination of the coefficients of K_A. In particular, if we had an array, A, with perfect (δ-function) aperiodic autocorrelation, then all sequences in $\{\tilde{A}\}$ would also have a perfect δ-function response. Although such ideal arrays do not exist, there are pairs of Golay complementary arrays whose aperiodic autocorrelations sum to a δ-function and, by joining, one can extract from such array pairs a family of sequence pairs whose aperiodic autocorrelations sum to a δ-function.

The continuous Fourier power spectrum of A is summarised by (2). Likewise, the continuous Fourier power spectrum of $\tilde{A}$ is summarised by,

$$\mathcal{F}(\tilde{A}) = \{K_{\tilde{A}}(\upsilon_0, \upsilon_0^{N_0}, \ldots, \upsilon_{n-1}^{N_0 N_1 \ldots N_{n-2}}) \quad | \quad |\upsilon_0| = 1.\}, \tag{3}$$

By comparing right-hand sides of (2) and (3) one concludes that

$$\mathcal{F}(\tilde{A}) \subseteq \mathcal{F}(A). \tag{4}$$

Let $P(A)$ be the maximum value in $\mathcal{F}(A)$, i.e.

$$P(A) = \max(u \quad | \quad u \in \mathcal{F}(A)). \tag{5}$$

We refer to $P(A)$ as the *peak-to-average power ration* (PAPR) of A. If, for a particular array, A, one has an upper bound, $\mathcal{P}$, on $P(A)$, then, from (4), $\mathcal{P}$ is also an upper bound on $P(\tilde{A})$. If A had a perfect aperiodic autocorrelation then $\mathcal{F}(\tilde{A}) = \mathcal{F}(A) = \{1\}$, i.e. the Fourier power spectrum of the sequence obtained by joining is *flat* everywhere, implying that $P(A) = P(\tilde{A}) = 1$. Although such perfect arrays are impossible, we can obtain a near-flat Fourier power spectrum for $\tilde{A}$ and $\tilde{B}$ by constructing a pair of Golay complementary arrays, (A, B), such that $P(A) = \frac{||A||^2 + ||B||^2}{||A||^2}$ and $P(B) = \frac{||A||^2 + ||B||^2}{||B||^2}$, leading to $P(\tilde{A}) \leq P(A)$ and $P(\tilde{B}) \leq P(B)$ for all possible sequences in families $\{\tilde{A}\}$ and $\{\tilde{B}\}$, respectively.

5 Three kinds of aperiodicity for generalised Boolean functions

We now focus our discussion on characterisation and construction of aperiodic *Boolean functions*. We here consider an n-variable generalised *Boolean function*, $A : \mathbb{F}_2^n \to \mathcal{C}$, which is a $2 \times 2 \times \ldots \times 2$ n-dimensional array, where the kth entry in the array, $k \in \mathbb{F}_2^n$, is given by $A(k) \in \mathcal{C}$. In other words $A \in \mathcal{C}_2^n$.

We characterise the aperiodicity of a generalised Boolean function using unitary matrices. Let

$$V_I = \{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & \alpha\\ 1 & -\alpha\end{pmatrix} \quad | \quad \forall\alpha, |\alpha| = 1\}$$

be an infinite-size class of 2×2 unitary matrices. Then, from (2),

$$\mathcal{F}(A) = \mathcal{F}_I(A) = \{|\hat{A}_{U,k}|^2 \quad | \quad \hat{A}_U = UA, \forall U \in V_I^{\otimes n}, \forall k \in \mathbb{F}_2^n\},$$

where we now refer to $\mathcal{F}(A)$ as $\mathcal{F}_I(A)$ to indicate that all transforms are taken with respect to unitaries from $V_I^{\otimes n}$. In other words, the set of points comprising the continuous Fourier transform of A is equal to the union of the set of squared-magnitudes of the array elements of $\hat{A}_U$, taken over all possible $2^n \times 2^n$ matrices U in $V_I^{\otimes n}$, where $\hat{A}_U$ is the unitary transform of A with respect to U. From the previous section we see that aperiodicity of A can be assessed by examining the 'flatness' of $\mathcal{F}_I(A)$ and, from (5), one measure of this flatness is $P(A)$, the PAPR of A, which from now on we refer to as $P_I(A)$.

The complete class of 2×2 unitary matrices can be given by

$$V = \{\Delta\begin{pmatrix}\cos\theta & \sin\theta\alpha\\ \cos\theta & -\sin\theta\alpha\end{pmatrix} \quad | \quad \forall\alpha, |\alpha| = 1, \forall\theta\}, \tag{6}$$

where Δ is any diagonal or anti-diagonal unitary 2×2 matrix. V_I is only a subclass of V. Are there are any other infinite-size unitary matrix subclasses over which another type of aperiodicity of A could be assessed?

We therefore consider aperiodicity of an n-variable generalised Boolean function, A, with respect to $V_I^{\otimes n}$, $V_{II}^{\otimes n}$ and $V_{III}^{\otimes n}$, where

$$V_{II} = \{\begin{pmatrix}\cos(\theta) & \sin(\theta)\\ \sin(\theta) & -\cos(\theta)\end{pmatrix} \quad | \quad \forall\theta\}$$

and

$$V_{III} = \{\begin{pmatrix}\cos(\theta) & i\sin(\theta)\\ \sin(\theta) & -i\cos(\theta)\end{pmatrix} \quad | \quad \forall\theta\}, \quad \text{where } i = \sqrt{-1}.$$

We refer to these three types of aperiodicity as *type-I, type-II, and type-III aperiodicity*, as characterised by the spectral sets F_I, F_{II}, and F_{III}, where

$$\mathcal{F}_{II}(A) = \{|\hat{A}_{U,k}|^2 \quad | \quad \hat{A}_U = UA, \forall U \in V_{II}^{\otimes n}, \forall k \in \mathbb{F}_2^n\},$$

and

$$\mathcal{F}_{III}(A) = \{|\hat{A}_{U,k}|^2 \quad | \quad \hat{A}_U = UA, \forall U \in V_{III}^{\otimes n}, \forall k \in \mathbb{F}_2^n\}.$$

We define the generalised Boolean function, A, to have optimal type-I, type-II, or type-III aperiodic properties if $P_I(A)$, $P_{II}(A)$, or $P_{III}(A)$ is as small as possible, respectively.

The relationship between V_I, V_{II}, and V_{III} is via the multiplicative action on V_I of a cyclic group, $\mathbb{T} = \{I, \lambda, \lambda^2\}$, of order 3, where

$$\lambda = \frac{\omega^5}{\sqrt{2}}\begin{pmatrix}1 & i\\ 1 & -i\end{pmatrix}$$

is a generator of $\mathbb{T}$ of order 3, ω is a primitive eighth root of one, and I is the 2×2 identity matrix. Specifically,

$$V_I = \Delta V_{III} \lambda = \Delta' V_{II} \lambda^2 = \Delta'' V_I \lambda^3,$$

where Δ, Δ', and Δ'' are diagonal and/or anti-diagonal 2×2 unitaries. The action of λ *rotates* V_I to V_{II}, V_{II} to V_{III}, and V_{III} to V_I, all modulo the group of diagonal/anti-diagonal matrices $\{\Delta\}$. The reason that we choose to rotate by λ is because we consider $\mathbb{T}$ to be important - the *local Clifford group*, $\mathbb{C}$, for 2×2 unitaries, splits as $\mathbb{D} \times \mathbb{T}$, where $\mathbb{D}$ is a subgroup comprising 64 diagonal and anti-diagonal 2×2 unitaries, and the local Clifford group, $\mathbb{C}$, is defined to be the group of 192 matrices that *stabilizes* the *Pauli group*, $\mathbb{P}$, otherwise known as the *discrete Heisenberg-Weyl group*. For 2×2 unitaries, $\mathbb{P}$ comprises $\{I, X, Z, Y\}$, where

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = -iXZ.$$

The term 'stabilizes' means that $UWU^{-1} = W'$, $\forall U \in \mathbb{C}$, $\forall W, W' \in \mathbb{P}$.

We have introduced three types of aperiodicity in spectral ('frequency' or 'residue') terms by means of the rotation action of $\mathbb{T}$ on the infinite-size set of transforms, V_I, over which conventional aperiodicity is defined. We now give the polynomial equations which reflect the 'time' ('non-residue') viewpoint for this aperiodicity. Specifically, given an n-variable generalised Boolean function, A, and associated multivariate polynomial $A(z) = A(z_0, z_1, \ldots, z_{n-1})$,

Lemma 1

Type-I aperiodic properties of A are expressed by $K_A^I(z) = \frac{A(z)A^*(z)}{||A||^2}$,
Type-II aperiodic properties of A are expressed by $K_A^{II}(z) = \frac{2^n A(z)^2}{||A||^2 \prod_{j=0}^{n-1}(1+z_j^2)}$,
Type-III aperiodic properties of A are expressed by $K_A^{III}(z) = \frac{2^n A(z)A(-z)}{||A||^2 \prod_{j=0}^{n-1}(1-z_j^2)}$.

A is a perfect generalised Boolean function of type-I, II, or III if $K_A^I(z) = 1$, $K_A^{II}(z) = 1$, or $K_A^{III}(z) = 1$, respectively.

Proof. Let $\upsilon = (\upsilon_0, \upsilon_1, \ldots, \upsilon_{n-1})$, and let $\mathcal{R}$ and $\mathcal{I}$ be the sets of real and imaginary values, respectively. One can verify that the sets of spectral power values $\mathcal{F}_I(A)$, $\mathcal{F}_{II}(A)$, and $\mathcal{F}_{III}(A)$ can be obtained via the following evaluations of certain equations in $A(z)$ over the unit circle, real axis, and imaginary axis, respectively,

$$\mathcal{F}_I(A) = \{\tfrac{A(\upsilon)A^*(\upsilon)}{||A||^2} \quad | \quad |\upsilon_j| = 1, 0 \le j < n\},$$
$$\mathcal{F}_{II}(A) = \{\tfrac{2^n A(\upsilon)^2}{||A||^2 \prod_{j=0}^{n-1}(1+\upsilon_j^2)} \quad | \quad \upsilon_j \in \mathcal{R}, 0 \le j < n\},$$
$$\mathcal{F}_{III}(A) = \{\tfrac{2^n A(\upsilon)A(-\upsilon)}{||A||^2 \prod_{j=0}^{n-1}(1-\upsilon_j^2)} \quad | \quad \upsilon_j \in \mathcal{I}, 0 \le j < n\}.$$

A is a perfect aperiodic generalised Boolean function of type-I, II, or III, if $P_I(A) = 1$, $P_{II}(A) = 1$, or $P_{III}(A) = 1$, respectively, which occurs when $\mathcal{F}_I(A) = \{1\}$, $\mathcal{F}_{II}(A) = \{1\}$, or $\mathcal{F}_{III}(A) = \{1\}$, respectively, and this is only possible when the conditions of the lemma are satisfied. QED.

We now apply dimension joining to the Boolean array, A, to obtain two new types of aperiodic sequence action. From the array $A(z_0, z_1, \ldots, z_{n-1})$, via the substitution $z_0 = y$, $z_k = z_{k-1}^2$, $\forall k$, $1 \leq k < n$, one obtains the length 2^n sequence $\tilde{A}$, and applying the same substitutions to the multivariate polynomial equations of lemma 1 gives the following univariate polynomial equation in $\tilde{A}(y)$,

Lemma 2

Type-I aperiodic properties of $\tilde{A}$ *are expressed by* $K_{\tilde{A}}^{I}(y) = \frac{\tilde{A}(y)\tilde{A}^*(y)}{||\tilde{A}||^2}$,
Type-II aperiodic properties of $\tilde{A}$ *are expressed by* $K_{\tilde{A}}^{II}(y) = \frac{2^n \tilde{A}(y)^2}{||\tilde{A}||^2 \prod_{j=0}^{n-1}(1+y^{2^j+1})}$,
Type-III aperiodic properties of $\tilde{A}$ *are expressed by* $K_{\tilde{A}}^{III}(y) = \frac{2^n \tilde{A}(y)\hat{A}(y)}{||\tilde{A}||^2 \prod_{j=0}^{n-1}(1-y^{2^j+1})}$,

where $\hat{A}(y) = \sum_{j=0}^{j=2^n-1} \tilde{A}_j(-1)^{wt(j)}y^j$, *and 'wt' means binary weight* [*] . $\tilde{A}$ *is a perfect complex sequence of length* 2^n *of type-I, II, or III if* $K_{\tilde{A}}^{I}(y) = 1$, $K_{\tilde{A}}^{II}(y) = 1$, *or* $K_{\tilde{A}}^{III}(y) = 1$, *respectively.*

Each array generates a family of type-I sequences, which we shall now call $\{\tilde{A}_I\}$, each member of which generates the same aperiodic autocorrelation, which we shall now call $K_{\tilde{A}}^{I}(y)$. Likewise, each array, $A(z)$, can also generate a family of type-II and type-III sequences, $\{\tilde{A}\}_{II}$, and $\{\tilde{A}\}_{III}$, respectively, where each member of $\{\tilde{A}\}_{II} = \{A(z) \mid z_{\pi(0)} = y, z_{\pi(k)} = \alpha_k z_{\pi(k-1)}^{\pm 2}, \alpha_k \in \mathcal{R}, 1 \leq k < n, \forall \pi \in \mathcal{S}_n\}$, has the same type-II aperiodic profile, $K_{\tilde{A}}^{II}$, and where each member of $\{\tilde{A}\}_{III} = \{A(z) \mid z_{\pi(0)} = y, z_{\pi(k)} = \alpha_k z_{\pi(k-1)}^{\pm 2}, \alpha_k \in \mathcal{R}, 1 \leq k < n, \forall \pi \in \mathcal{S}_n\}$, has the same type-III aperiodic profile, $K_{\tilde{A}}^{III}$.

6 Some cryptographic interpretations and context for type-I, II, and III aperiodicity

Let $a(x)$ be a Boolean function in n variables, where $A_k = (-1)^{a(k)} \in \{-1, 1\}^n$, $k \in \mathbb{F}_2^n$.

6.1 cryptographic motivation

Having characterised three types of aperiodicity for a generalised Boolean function we now provide some cryptographic motivation as to the relevance of these characterisations for Boolean functions of types I and II.

– The conventional *differential* properties of a are measured by the closeness of $a(x)$ to $a(x+s)$, $s \in \mathbb{F}_2^n$, i.e. by the maximum magnitude of $\sigma_s = \sum_{x \in \mathbb{F}_2^n}(-1)^{a(x)+a(x+s)}$, $\forall s \neq 0$ [8]. A differentially perfect function will be

[*] The type-III description in lemma 2 corrects a previous error contained in the published version of this paper.

maximally distant from its differential, for all values of $s \neq 0$, i.e. ideally $\sigma_s = 0$, $\forall s \neq 0$, in which case the differential $a(x) + a(x+s)$ remains completely unbiased $\forall s \neq 0$, on the assumption that x is not known. But type-I aperiodicity measures the biasedness of $a(x) + a(x+s)$ on the assumption that x_j is known for each $s_j = 1$, and a perfect type-I aperiodic function would remain completely unbiased for all $s \neq 0$ even under this assumption [9].

– The conventional *linear* properties of a are measured by the closeness of $a(x)$ to an affine function, $t \cdot z$, $t \in \mathbb{F}_2^n$, i.e. by the maximum magnitude of $\hat{a}_t = \sum_{x \in \mathbb{F}_2^n} (-1)^{a(x)+t \cdot x}$, $\forall t$ [8]. A linearly perfect function will be maximally distant from all affine functions, i.e. $\hat{a}$ will have magnitude $2^{n/2}$, $\forall t$, in which case $a(x) + t \cdot x$ is minimally biased $\forall t$. There is an implicit assumption that each of the input variables $x_0, x_1, \ldots, x_{n-1}$ is '0' with probability $\frac{1}{2}$. But type-II aperiodicity measures the biasedness of $a(x) + t \cdot x$, $\forall t$, where no assumption is made on the input probability of $x_j = 0$, $\forall j$.

6.2 wider context

The autocorrelation action of the Heisenberg-Weyl (HW) group [11] on an n-variable Boolean function, a, can be described by,

$$\mathcal{H}_{s,t}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a(x)+a(x+s)+x \cdot t + s \cdot t} = \quad < A, X^s Z^t A >, \quad s, t \in \mathbb{F}_2^n. \tag{7}$$

There are 4^n coefficients, $\mathcal{H}_{s,t}(a)$. The Boolean function, a, (array A), can be considered to be a good HW function if all magnitudes $|\mathcal{H}_{s,t}(a)|$ are small $\forall s$ and $t \neq 0$. A perfect HW Boolean function would have $\mathcal{H}_{s,t}(a) = 0$ for all $\forall s$ and $t \neq 0$, but this is impossible. Let $s = (s_0, s_1, \ldots, s_{n-1}) \in \mathbb{F}_2^n$ let $\bar{s} = (s_0 + 1, s_1 + 1, \ldots, s_{n-1} + 1)$.

– [9] Type-I aperiodicity is measured by the coefficients $\mathcal{H}_{s,t}(a)$ where $t \preceq s$. A perfect type-I function would have $\mathcal{H}_{s,t}(a) = 0$, $\forall s$ and $t \neq 0$, $t \preceq s$.
– Type-II aperiodicity is measured by the coefficients $\mathcal{H}_{s,t}(a)$ where $t \preceq \bar{s}$. A perfect type-II function would have $\mathcal{H}_{s,t}(a) = 0$, $\forall s$ and $t \neq 0$, $t \preceq \bar{s}$.
– Type-III aperiodicity is measured by the coefficients $\mathcal{H}_{s,t}(a)$ where $s \preceq t$. A perfect type-III function would have $\mathcal{H}_{s,t}(a) = 0$, $\forall s$ and $t \neq 0$, $s \preceq t$.

Each of type-I, II, III identifies 3^n of the 4^n HW coefficients. For the 3^n type-I coefficients and the 4^n HW coefficents we know the following identities.

$$\begin{array}{ll} \sum_{s,t,t \preceq s} |\mathcal{H}_{s,t}(a)|^2 = \int_{|v_j|=1, \forall j} |A(v)|^4, & \text{Wiener-Kinchine} \\ \sum_{s,t} |\mathcal{H}_{s,t}(a)|^2 = 2^n, & \text{Moyal's identity [11].} \end{array}$$

The impossibility of perfect type-I, II, or III functions implies the impossiblity of a perfect HW function. But, in the next section, we identify perfect pairs of type-I, II, and III functions which are also constructible, whereas the far stricter

HW criteria does not appear to allow such pairs. However, recent activity [18, 16] has identified N-element sequences and (one) array which realise the value of $|\mathcal{H}_{s,t}(a)|^2 = \frac{1}{N+1}$ everywhere, which is the theoretical min-max. Such objects are called *equiangular lines* and, in the context of *quantum tomography*, are known as SIC-POVMs. Whilst a number of SIC-POVM sequences have been found over unwieldy alphabets, only one $2 \times 2 \times 2$ SIC-POVM array has been found (the *Hoggar lines*), and this is not over the alphabet $\{1, -1\}$ [16]. Moreover, [16] has shown that SIC-POVM arrays in $\mathcal{C}_2^n$ do not exist for $n > 3$.

When viewing the n-variable Boolean function, a, as a quantum state of n qubits, as described by pure-state vector $|A >= 2^{-n/2}A$, then the action of the HW group on $|A >$ identifies the qubit *bit-flip*, *phase-flip*, and combined phase-flip then bit-flip errors on $|A >$ (the action of unitaries X, Z, and XZ), respectively. Those Boolean functions, a, for which $\mathcal{H}_{s,t}(a) = 0$ when $\mathrm{wt}(s) + \mathrm{wt}(t) - \mathrm{wt}(s + t) < 2d$ ('wt' means Hamming weight) represent one-dimensional *quantum codes* of distance d [6, 4], and include highly-entangled *graph states*, which have been proposed as a resource for *measurement-based quantum computing* [20]. This quantum condition on the $\mathcal{H}_{s,t}(a)$ coefficients is conveniently expressed by the *fixed-aperiodic autocorrelation* of Boolean functions, as proposed and investigated in [9], this comprising the union of coefficients arising from the aperiodic autocorrelation of a, with those from the aperiodic autocorrelation of any function, $a_\downarrow$, obtained by fixing one or more of the input variables of a to '0' or '1' - a total of 5^n coefficients. Related to these 5^n fixed-aperiodic autocorrelation coefficients we have the following conjectured identity.

$$\textstyle\sum_{s,t} \binom{n}{e_{s,t}} 2^{e_{s,t}} |\mathcal{H}_{s,t}(a)|^2 = \int_{U \in V^{\otimes n}} ||U|A > ||^4,$$

where $e_{s,t} = n - \mathrm{wt}(s + t + s \cdot t)$, and V is the set of all 2×2 unitaries, as defined in (6).

7 Complementary and near-complementary pairs and their construction

Conventional (type-I) Golay complementary sequence pairs, $(\tilde{A}, \tilde{B})$, satisfy the property,

$$K^I_{\tilde{A}}(y) + K^I_{\tilde{B}}(y) = 2. \tag{8}$$

In other words $(\tilde{A}, \tilde{B})$ are ideal as a pair of type-I sequences. But, as shown recently [13], the Golay property is often, primarily, an array property, and a pair of (type-I) Golay arrays, (A, B), satisfy,

$$K^I_A(z) + K^I_B(z) = 2., \tag{9}$$

where $z = (z_0, z_1, \ldots, z_{n-1})$, in which case (A, B) are ideal as a pair of type-I arrays. Let $\{(\tilde{A}, \tilde{B})\}$ be a family of sequence pairs obtained from (A, B) by joining. It follows from the ideal properties of the array pair that,

$$P_I(A) = \frac{||A||^2 + ||B||^2}{||A||^2}, \qquad P_I(B) = \frac{||A||^2 + ||B||^2}{||B||^2}.$$

In particular, if $||A||^2 = ||B||^2$, which is the case for Boolean arrays $A = (-1)^a$, $B = (-1)^b$, then

$$P_I(A) = P_I(B) = 2.$$

It follows from (4) that,

$$P_I(\tilde{A}) \leq P_I(A), \qquad P_I(\tilde{B}) \leq P_I(B).$$

So, if (A, B) is type-I complementary, then so is $(\tilde{A}, \tilde{B})$ for all $(\tilde{A}, \tilde{B}) \in \{(\tilde{A}, \tilde{B})\}$. Complementary array properties imply complementary sequence properties, but a complementary pair of sequences is not necessarily derived from a pair of higher-dimensional arrays. For instance, the length-10 (type-I) complementary pair of sequences over the alphabet $\{1, -1\}$ is not derived from a 2×5 two-dimensional (type-I) complementary array pair over the alphabet $\{1, -1\}$ [23].

We further extend our definition of PAPR to array or sequence pairs. Specifically, let,

$$K^I_{AB}(z) = \frac{A(z)A^*(z) + B(z)B^*(z)}{||A||^2 + ||B||^2},$$

and

$$\mathcal{F}_I(A, B) = \{K^I_{AB}(\upsilon) \quad | \quad |\upsilon_j| = 1, 0 \leq j < n\}.$$

$\mathcal{F}_I(\tilde{A}, \tilde{B})$ is similarly defined, where

$$\mathcal{F}_I(\tilde{A}, \tilde{B}) \subseteq \mathcal{F}_I(A, B).$$

The type-I PAPR of the array pair, (A, B), and sequence pair, $(\tilde{A}, \tilde{B})$, are given by,

$$P_I(A, B) = \max(u \quad | \quad u \in \mathcal{F}_I(A, B)),$$
$$P_I(\tilde{A}, \tilde{B}) = \max(u \quad | \quad u \in \mathcal{F}_I(\tilde{A}, \tilde{B}),$$

and

$$P_I(\tilde{A}, \tilde{B}) \leq P_I(A, B).$$

The (type-I) Golay construction for sequence pairs [14, 15] was generalised by Turyn [30], further generalised by Borwein and Ferguson [5], and has recently been generalised to arrays [13]. We here give a further generalisation to *near-complementary pairs* [27, 29], building on the notation of [5]. Let $x = (z_0, z_1, \ldots, z_{n-1})$, $y = (z_n, z_{n+1}, \ldots, z_{n+m-1})$, and $z = (z_0, z_1, \ldots, z_{n+m-1})$. Let $(A(x), B(x))$, $(C(y), D(y))$, and $(F(z), G(z))$ be three pairs of polynomials of n, m, and $n + m$ variables, respectively.

Lemma 3 *Let*

$$F(z) = C(y)A(x) + D^*(y)B(x), \qquad G(z) = D(y)A(x) - C^*(y)B(x).$$

Then,

$$P_I(F, G) = P_I(A, B)P_I(C, D).$$

In particular, if (A, B) and (C, D) are both (type-I) Golay complementary pairs then, by definition, $P_I(A, B) = P_I(C, D) = 1$ and, therefore, as $P_I(F, G) = 1$, then (F, G) is a (type-I) Golay complementary pair.

From lemma 3 one can derive a similar construction for sequence pairs. We call the construction of lemma 3 a *type-I construction*. If $P_I(A,B) = 1+\epsilon$ and $P_I(C,D) = 1+\epsilon'$, then $P_I(F,G) = 1+\epsilon''$, where ϵ'' is small if ϵ and ϵ' are small, in which case we have a construction for *near-complementary pairs*.

Previously we showed that, for arrays in $\mathcal{C}_2^n$, one can rotate the concept of aperiodicity by successive multiplications of the transform kernel by λ. This also implies a rotated concept of complementarity and we now define type-II and type-III complementarity for arrays in $\mathcal{C}_2^n$, i.e. for generalised Boolean functions. For $A, B \in \mathcal{C}_2^n$,
Type-II complementary array pairs, (A,B), satisfy the property,

$$K_A^{II}(z) + K_B^{II}(z) = 2. \tag{10}$$

Type-III complementary array pairs, (A,B), satisfy the property,

$$K_A^{III}(z) + K_B^{III}(z) = 2. \tag{11}$$

By means of unitary rotation by λ, as described in section 5, we can not only rotate the set of transforms over which aperiodicity and complementarity is determined, but also rotate the (type-I) Turyn construction itself. We obtain the following type-II and type-III constructions for (near-)complementary pairs, where the meanings of $P_{II}(A,B)$ and $P_{III}(A,B)$, ...etc, follow in exactly the same way as for type-I.

Lemma 4 *Let*

$$F(z) = C(y)A(x) + D(y)B(x), \qquad G(z) = D(y)A(x) - C(y)B(x).$$

Then,

$$P_{II}(F,G) = P_{II}(A,B)P_{II}(C,D).$$

In particular, if (A,B) and (C,D) are both type-II complementary pairs then, by definition, $P_{II}(A,B) = P_{II}(C,D) = 1$ and, therefore, as $P_{II}(F,G) = 1$, then (F,G) is a type-II complementary pair.

Lemma 5 *Let*

$$F(z) = C(y)A(x) + D(-y)B(x), \qquad G(z) = D(y)A(x) - C(-y)B(x).$$

Then,

$$P_{III}(F,G) = P_{III}(A,B)P_{III}(C,D).$$

In particular, if (A,B) and (C,D) are both type-III complementary pairs then, by definition, $P_{III}(A,B) = P_{III}(C,D) = 1$ and, therefore, as $P_{III}(F,G) = 1$, then (F,G) is a type-III complementary pair.

The construction of lemma 3 is valid for arrays of all dimensions, and the constructions of lemmas 4 and 5 are at least valid for arrays in $\mathcal{C}_2^n$, i.e. for generalized Boolean functions. For the special case where the elements of the array are

in the alphabet $\{1, -1\}$, we can express the type-I, II, and III constructions using Boolean functions. Let (a, b), (c, d), and (f, g) be three pairs of Boolean functions of n, m, and $n + m$ disjoint sets of variables, respectively, where $a, b : \mathbb{F}_2^n \to \mathbb{F}_2$, $c, d : \mathbb{F}_2^m \to \mathbb{F}_2$, and $f, g : \mathbb{F}_2^{n+m} \to \mathbb{F}_2$. By $P_I(a, b)$ we mean $P_I(A, B)$. Let $\overleftarrow{a}(x_0, x_1, \ldots, x_{n-1}) = a(x_0 + 1, x_1 + 1, \ldots, x_{n-1} + 1)$.

Lemma 6 *Let*

$$f = (a + b)(c + \overleftarrow{d}) + a + \overleftarrow{d}, \qquad g = (a + b)(\overleftarrow{c} + d) + b + \overleftarrow{c}.$$

Then,

$$P_I(f, g) = P_I(a, b)P_I(c, d).$$

Lemma 7 *Let*

$$f = (a + b)(c + d) + a + d, \qquad g = (a + b)(c + d) + b + c.$$

Then,

$$P_{II}(f, g) = P_{II}(a, b)P_{II}(c, d).$$

Lemma 8 *Let (c, d) be defined over the m binary variables, $(x_0, x_1, \ldots, x_{m-1})$. Let $l_m = \sum_{j=0}^{m-1} x_j$. Let*

$$f = (a + b + l_m)(c + d) + a + d, \qquad g = (a + b + l_m)(c + d) + b + c + l_m.$$

Then,

$$P_{III}(f, g) = P_{III}(a, b)P_{III}(c, d).$$

It is interesting to note that the type-II Boolean construction is identical to a certain construction for bent functions [2, 8, 7], which states that, if a, b, c, and d are bent, then f is bent. Moreover, if a and b are t resilient, and c and d are u resilient, then f is $t + u + 1$ resilient. Finally, if a, b, c, and d are self-dual bent, then f is self-dual bent, and if a and b are bent duals, c is self-dual bent, and d is anti-self-dual bent, then f is self-dual bent [3].

8 Explicit examples of type-I, II, and III complementary pairs of Boolean functions

For type-I there is, to within symmetries discussed previously, only one known [10] class of complementary pairs of Boolean functions, (f, g), as given by,

$$f = \sum_{j=0}^{n-2} x_j x_{j+1}, \qquad g = f + x_0, \quad \text{or} \quad g = f + x_{n-1}.$$

By interpreting the quadratic terms of f as edges of a simple graph we see that f represents the *path graph* of n vertices.

For type-II we have found, to within symmetries discussed previously, only one class of complementary pairs of Boolean functions, (f, g), as given by,

$$f = \sum_{j<k} x_j x_k, \qquad g = f + \sum_j x_j.$$

f represents the *complete graph* of n vertices.

Some type-III pairs were identified by Abdelraheem in [1], as follows. For type-III there is an infinite number of classes of complementary pairs of quadratic or affine Boolean functions, (f, g). To begin with, (f, g) are type-III complementary for any affine f and g. By passing these into the input of the type-III construction of lemma 5, an infinite number of classes of type-III complementary pairs of quadratic Boolean functions arise at the output. However, one particularly interesting class is

$$f = \sum_{j=1}^{n-1} x_0 x_j, \qquad g = f + \sum_{j=1}^{n-1} x_j \quad \text{or } g = f + x_0.$$

For this particular class, f represents the *star graph* of n vertices.

Although we have focused on Boolean complementary pairs we observe that type-I, II, and III pairs from the alphabet $\{1, -1\}$ can be rotated round to type-II, III, and I pairs from the alphabet $\{0, 1, i, -1, -i\}$, respectively, by the multiplicative action of λ on each of the pairs, and round to type-III, I, and II pairs from the alphabet $\{0, 1, i, -1, -i\}$, respectively, by the multiplicative action of λ^2. In particular, this allows us to generate new Golay (type-I) complementary pairs which are defined, indirectly, using type-II or type-III Boolean functions.

9 Conclusion and open problems

The purpose of this paper was, first, to show how aperiodic arrays can be used to generate aperiodic sequences and, secondly, to present a wider notion of aperiodicity for arrays in $\mathcal{C}_2^n$. Three different notions of aperiodicity were defined by exploiting the action of a size-3 cyclic subgroup of the local Clifford group on the aperiodic description. The three types of aperiodicity related to the autocorrelations generated by the Heisenberg-Weyl group. The three aperiodic types also lead to three types of construction for complementary pairs of arrays. Explicit examples of complementary pairs of Boolean functions were given for each of the three types.

We identify some open problems.

- Does another class of complementary $\{1, -1\}$ sequences exist of length 2^n other than the 'path graph' class described in this paper? One can generalise

this question to ask whether (type-I) complementary Boolean functions other than the path graph class exist.
- We only know of one class of type-II complementary Boolean function pair, namely that described by the 'complete graph'. As with type-I, it is an open problem as to whether another class of type-II complementary Boolean function pair exists.
- We know of no complementary pair of Boolean functions of types I, II or III whose component functions have degree greater than 2. Can one prove that higher-degree complementary pairs of Boolean functions do not exist?
- The complementary Boolean functions described in this paper are of algebraic degree ≤ 2. But, for cryptographic purposes, it is usually desirable to construct high-degree Boolean functions. Assuming that complementary pairs of Boolean functions of degree greater than 2 do not exist, how close to complementarity can one get for a pair of Boolean functions of degree d, and how does one construct and/or bound such a pair?
- Is it possible to effectively combine two or more of the type-I, II, or III constructions? Observe that the type-I and type-II constructions differ only in the application of $\overleftarrow{*}$ to c and d for type-I. Thus, if we can find a pair of Boolean functions (c, d) that satisfy the conditions $c = \overleftarrow{c}$ and $d = \overleftarrow{d}$, then we can apply type-I and type-II constructions simultaneously. Unfortunately we do not know of a pair (c, d) which is simultaneously both type-I and type-II complementary (and we do not expect that such a pair exists), but it is possible to find near-complementary pairs that satisfy the conditions.
- It is reasonable to expect that there are no pairs of Boolean functions which are complementary with respect to the Heisenberg-Weyl group. Can this be proved? If we can't find pairs, then what is the smallest size set of Boolean functions which are complementary with respect to the Heisenberg-Weyl group for a non-trivial number of variables, n? Note that it is possible to extract complementary sets from quantum codes, however the size of these sets grows exponentially with the number of binary variables, so they are of little interest.
- Are there any other interesting types of aperiodicity? For instance, the three types of aperiodicity describes herein are for arrays in $\mathcal{C}_2^n$. One expects that more interesting types may turn up as the size of array dimension increases.

Acknowledgments: The author would like to acknowledge that any 'new' ideas in this paper owe a lot to joint research and discussions with Lars Eirik Danielsen, Frank Fiedler, Jonathan Jedwab, Constanza Riera, and Mohamed Abdelraheem. In particular, the results on generalised complementary constructions follow naturally from recent joint work on multidimensional complementary arrays with Fiedler and Jedwab.

References

1. Abdelraheem, M.A.A.M.A.: A database for Boolean functions and constructions for generalized complementary pairs. Master's thesis, University of Bergen. June

(2008)
2. Adams, C.M., Tavares, S.E.: Generating and Counting Binary Bent Sequences. IEEE Trans. Inf. Theory. vol. 36, (5) 1170–1173 1990.
3. Carlet, C., Danielsen, L.E., Parker, M.G., Solé, P.: Self-dual bent functions. Fourth International Workshop on Boolean Functions: Cryptography and Applications (BFCA 2008). Copenhagen, Denmark. 19–21 May (2008)
4. Danielsen, L.E., Parker, M.G.: On the classification of all self-dual additive codes over GF(4) of length up to 12. Journal of Combinatorial Theory, Series A. 113, 7, 1351–1367 Oct. (2006)
5. P.B. Borwein, P.B., Ferguson, R.A.: A complete description of Golay pairs for lengths up to 100. Mathematics of Computation. 73 967985 (2003)
6. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum Error Correction Via Codes Over GF(4). IEEE Trans. Information Theory. 44, 1369–1387 (1998)
7. Carlet, C.: On the secondary constructions of resilient and bent functions. Proceedings of the Workshop on Coding, Cryptography and Combinatorics 2003, published by Birkhauser Verlag, K. Feng, H. Niederreiter and C. Xing Eds., 3–28 (2004)
8. Carlet, C.: Boolean functions for cryptography and error correcting codes. Preprint, (2008)
9. Danielsen, L.E., Gulliver, T.A., Parker, M.G.: Aperiodic Propagation Criteria for Boolean Functions. Inform. Comput. 204, 5, 741–770 (2006)
10. Davis, J.A, Jedwab, J.: Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes, IEEE Trans. Information Theory. vol. 45, 2397–2417 (1999)
11. Howard, S.D., Calderbank, A.R., Moran, W.: The finite Heisenberg-Weyl groups in radar and communications. EURASIP Journal on Applied Signal Processing. vol. 2006, (1) Jan. (2006)
12. Dmitriev, D., Jedwab, J.: Bounds on the growth rate of the peak sidelobe level of binary sequences. Advances in Mathematics of Communications. vol. 1, 461–475 (2007)
13. Fiedler, F., Jedwab, J., Parker, M.G.: A multi-dimensional approach to the construction and enumeration of Golay complementary sequences. accepted for Journal of Combinatorial Theory (Series A). (2007)
14. Golay, M.J.E.: Static multislit spectrometry and its application to the panoramic display of infrared spectra. J. Opt. Soc. Amer., 41:468472 (1951)
15. Golay, M.J.E.: Complementary series. IRE Trans. Inform. Theory. IT-7:8287 (1961)
16. Godsil, C., Roy, A.: Equiangular lines, mutually unbiased bases, and spin models. Preprint arXiv:quant-ph/0511004 v2 (2005)
17. Golomb, S.W., Gong, G.: Signal Design for Good Correlation. ISBN: 9780511159466, Cambridge University Press (2005)
18. Grassl, M.: Tomography of quantum states in small dimensions. Electron. Notes Discrete Math. 20, 151–164 (2005)
19. Gulliver, T.A., Parker, M.G.: The Multivariate Merit Factor of a Boolean Function. ITW2005, IEEE ITSOC Information Theory Workshop 2005 on Coding and Complexity, Rotorua, New Zealand. 29th Aug.–1st Sept. (2005)
20. Hein, M., Dur, W., Eisert, J., Raussendorf, R., Van den Nest, M., Briegel, H.-J.: Entanglement in Graph States and its Applications. International School of Physics Enrico Fermi (Varenna, Italy), Quantum computers, algorithms and chaos 162 (Eds.: P. Zoller, G. Casati, D. Shepelyansky, G. Benenti). (2006) http://xxx.soton.ac.uk/abs/quant-ph/0602096

21. Helleseth, T., Kumar, P.V.: Sequences with Low Correlations. Handbook in Coding Theory, V. Pless and G. Huffmann (eds.) Kluwer Acad. Publ. (1998)
22. Jedwab, J., Parker, M.G.: There are no Barker arrays having more than two dimensions. Designs, Codes and Cryptography. 43, 2–3, 79–84 June (2007)
23. Jedwab, J., Parker, M.G.: Golay Complementary Array Pairs. Designs, Codes and Cryptography. 44, 209–216 July (2007)
24. Luke, H.D.: Sets of one and higher dimensional Welti codes and complementary codes. IEEE Trans. Aerospace Electron. Systems. AES-21, 170–179 (1985)
25. Parker, M.G.: Univariate and Multivariate Merit Factors. Proceedings of SETA04. LNCS 3486, 72–100 (2005)
26. Parker, M.G., Paterson, K.G., Tellambura, C.: Golay Complementary Sequences. Wiley Encyclopedia of Telecommunications, Editor: J.G.Proakis, Wiley Interscience. (2002)
27. Parker, M.G., Tellambura, C.: Generalised Rudin-Shapiro Constructions. WCC2001 International Workshop on Coding and Cryptography, Paris(France). Jan 8–12 (2001) Electronic Notes in Discrete Mathematics, 6, April (2001)
28. Riera, C., Parker, M.G.: Generalised Bent Criteria for Boolean Functions (I). IEEE Trans Inform. Theory. 52, 9, 4142–4159 Sept. (2006)
29. Schmidt, K.-U.: On cosets of the generalized first-order Reed-Muller code with low PMEPR. IEEE Trans. Inform. Theory. 52, 3220–3232 (2006)
30. Turyn, R.J.: Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings. J. Combin. Theory (A). 16:313–333 (1974)
31. Shapiro, H.S.: Extremal Problems for Polynomials. M.S. Thesis, M.I.T. (1951)