FINITE HEISENBERG-WEYL GROUPS AND GOLAY COMPLEMENTARY SEQUENCES

S. D. Howard[1], A. R. Calderbank[2], W. Moran[3]

[1]Defence Science & Technology Organisation, PO BOX 1500, Edinburgh 5111, Australia.
[2]Applied and Computational Mathematics, Princeton University, Princeton, NJ 08540, USA
[3]Department of Electrical and Electronic Engineering, The University of Melbourne, Victoria, 3010, Australia.

Abstract

We provide a new way of understanding Golay pairs (of length N) of sequences in terms of the (2N + 1)-dimensional discrete Heisenberg-Weyl group over the field $\mathbb{Z}_2$. Our methodology provides a different insight into the nature of these sequences, as well as a mechanism for designing sequences with desirable correlation properties. Libraries of waveforms formed using these constructions are able to provide collections of ambiguity functions that cover the range-Doppler plane in an efficient way, and thus provide the basis for a suite of waveforms optimized for extraction of information from the environment in an active sensing context.

1 Introduction

Golay complementary sequences are pairs of sequences of unimodular complex numbers, usually real, with the property that the sum of their individual auto-correlation functions forms a delta spike or thumb tack. They were discovered independently by Golay [7], and by Shapiro [16]. These sequences and variants of them have been considered for use by many authors in the construction of phase-coded radar waveforms and in modulation schemes for communications (see, for example, [9, 8, 15, 14, 11]). They have been used and investigated in numerous situations both in applications and in purely theoretical investigations. Effectively, in a radar context they produce zero range sidelobes at zero Doppler.

Our aim is to introduce a completely new framework for understanding Golay pairs (of length 2^m) in terms of the $(2m+1)$-dimensional discrete Heisenberg-Weyl group over the field $\mathbb{Z}_2$. This group is more familiar in coding theory for communications, where it has been used by Calderbank et. al [4] in the study of Kerdock and Preparata codes. The Heisenberg-Weyl group over $\mathbb{Z}_2$ provides the mathematical framework for construction and analysis of first and second order Reed Muller codes, whereas the more complicated Heisenberg-Weyl group over $\mathbb{Z}_{2^m}$ provides the mathematical framework for the description of Golay pairs. The latter group is the natural finite version of the continuous Weyl-Heisenberg group, which is the basic object for the algebraic treatment of the radar ambiguity function (see [13]). We have been able to show how to pass between the algebras of these two discrete groups, thus allowing us to formulate the Golay property in the simpler group and to analyse the structure of Golay pairs at this level. This transfer property is encapsulated in an apparently novel formula that relates translation in the $\mathbb{Z}_2$ world with translation in the $\mathbb{Z}_{2^m}$ world, in the context of Heisenberg-Weyl groups.

Using this analysis we are able to discuss not only complementary pairs, but also collections of them that relate naturally to each other. These collections have also been discovered previously in the work of Welti [17] and in the so-called Prometheus Orthonormal Set (PONS) of Byrnes [3]. Variants of them obtained by "special" permutations of the Welti-PONS codes have been described and used in a communications context by Popovic [15] and Budisin [2]. These variants share the correlation properties of the original Welti-PONS codes. They form special subgroups of the $\mathbb{Z}_2$-Heisenberg-Weyl group of operators.

Our work shows how all of these collections arise naturally from the algebra of the situation governed by the $\mathbb{Z}_2$ view, even though the Golay property is describable in the $\mathbb{Z}_{2^m}$ world. We have been able to characterize the waveform collections encompassed by the Popovic-Budisin construction, applied to the Welti-PONS waveform collections, thus showing their special nature among waveforms/codes. Our methodology provides new insight into the nature of these codes, and a new technique for their analysis, as well as a mechanism for designing sequences with desirable correlation properties both for communications and sensing applications.

The paper is organised as follows. We begin by describing the general construction and properties of finite Heisenberg-Weyl groups. In Sections 3 and 4 we show how the conditions for a pair of sequences to be Golay complementary can be formulated in terms of two particular Heisenberg-Weyl groups. In Section 5 we give sufficient conditions for orthonormal bases of cyclic or $\mathbb{Z}_{2^m}$-Golay complementary sequences to exist and then demonstrate how to relate this condition back to the usual linear or $\mathbb{Z}$-Golay complementary sequences in Section 6. As an example, in Section 7, we show how the Budisin-Popovic

Golay complementary sequences [2] fit into our scheme.

Finally, we note that this paper is really a summary of results. We have omitted many of the proofs, and derivations have been shortened or left out entirely.

2 Discrete Heisenberg-Weyl Groups

In this section we give a short summary of the construction and properties of finite Heisenberg-Weyl groups. For a more detailed description and further references see [10].

We begin by defining a configuration space $A = \mathbb{Z}_q^m$ consisting of m-tuples of elements from the integers modulo q. In this paper, we will take $q = p^n$, for some prime number p. Under addition, A forms an Abelian group. In radar theory the space A, with $m = 1$ would represent discretized version of the range space, while in discrete quantum mechanics the space A could represent possible discrete positions for a particle.

Define a Hilbert space $\mathcal{H}$, having orthonormal basis

$$\{|\,\mathbf{a}\rangle : \mathbf{a} \in A\}, \tag{1}$$

which we refer to as the *Dirac basis*. Note that we use the "bra-ket" notation for elements of the Hilbert space. An arbitrary element $|\,\phi\rangle \in \mathcal{H}$ can be expanded in this basis as

$$|\,\phi\rangle = \sum_{\mathbf{a}\in A} \langle \mathbf{a}\,|\,\phi\rangle\ |\,\mathbf{a}\rangle, \tag{2}$$

where $\langle\cdot\,|\,\cdot\rangle$ is the inner product on $\mathcal{H}$.

The dual group of A, denoted $\hat{A}$, consists of the homomorphisms from the group A into the unit circle Π in $\mathbb{C}$. $\hat{A}$ is also an Abelian group (under multiplication) and is (since A is finite) isomorphic to A. This isomorphism is made explicit through identification of each $\mathbf{b} \in A$ with a $\gamma_{\mathbf{b}} \in \hat{A}$, such that

$$\gamma_{\mathbf{b}}(\mathbf{a}) = \omega^{\mathbf{b}\cdot\mathbf{a}}, \tag{3}$$

for all $\mathbf{a} \in A$, where $\omega = \exp(2\pi i/p)$, and $\cdot$ denotes the usual dot product on $\mathbb{Z}_q^m$. We see from (3) that the elements of $\hat{A}$ are just discrete sinusoids, or multi-dimensional versions of such. To each element of $\gamma_{\mathbf{b}} \in \hat{A}$ we can assign a vector in $\mathcal{H}$ by

$$|\,\hat{\mathbf{b}}\rangle = \frac{i^{m/2}}{\sqrt{|A|}} \sum_{\mathbf{a}\in A} \omega^{\mathbf{b}\cdot\mathbf{a}}\ |\,\mathbf{a}\rangle. \tag{4}$$

The set $\{|\,\hat{\mathbf{a}}\rangle : \mathbf{a} \in A\}$ also forms an orthonormal basis for $\mathcal{H}$, which we refer to as the *Fourier basis*. We can define the unitary Fourier transform operator relating this orthonormal basis to (1) by

$$F = \frac{i^{m/2}}{\sqrt{|A|}} \sum_{\mathbf{a},\mathbf{b}\in A} \omega^{\mathbf{b}\cdot\mathbf{a}}\ |\,\mathbf{a}\rangle\langle\mathbf{b}\,|, \tag{5}$$

where $|\,\mathbf{a}\rangle\langle\mathbf{b}\,|$ represents the cross projection operator on $\mathcal{H}$ whose action on $|\,\phi\rangle \in \mathcal{H}$ is $|\,\mathbf{a}\rangle\langle\mathbf{b}\,|\ |\,\phi\rangle = \langle\mathbf{b}\,|\,\phi\rangle|\,\mathbf{a}\rangle$

We will denote the group $A \times \hat{A} \simeq A \times A$, which we regard as a $\mathbb{Z}_q$-module over the ring $\mathbb{Z}_q$, by $\overline{E}$. When q is prime, $\mathbb{Z}_q$ is a field and $\overline{E}$ is a vector space. We will refer to $\overline{E}$ as the *phase space*.

On $\mathcal{H}$ we define the unitary operators $\{D(\mathbf{a},\mathbf{b}) : (\mathbf{a},\mathbf{b}) \in \overline{E}\}$ by

$$D(\mathbf{a},\mathbf{b}) = \sum_{\mathbf{c}\in A} \omega^{\mathbf{b}\cdot\mathbf{c}}\ |\,\mathbf{c}+\mathbf{a}\rangle\langle\mathbf{c}\,|. \tag{6}$$

Two such operators have the multiplication rule

$$D(\mathbf{a},\mathbf{b})D(\mathbf{a}',\mathbf{b}') = \omega^{\mathbf{b}\cdot\mathbf{a}'} D(\mathbf{a}+\mathbf{a}',\mathbf{b}+\mathbf{b}'), \tag{7}$$

from which we have the commutator relation

$$D(\mathbf{a},\mathbf{b})^\dagger D(\mathbf{a}',\mathbf{b}')D(\mathbf{a},\mathbf{b})D(\mathbf{a}',\mathbf{b}')^\dagger = \omega^{\mathbf{a}\cdot\mathbf{b}'-\mathbf{a}'\cdot\mathbf{b}} I, \tag{8}$$

where † denotes adjoint.

The set of unitary operators on $\mathcal{H}$

$$E = \{T(\lambda,\mathbf{a},\mathbf{b}) = \omega^\lambda D(\mathbf{a},\mathbf{b}) : \lambda \in \mathbb{Z}_q, (\mathbf{a},\mathbf{b}) \in \overline{E}\}, \tag{9}$$

if $q \neq 2$, or

$$E = \{T(\lambda,\mathbf{a},\mathbf{b}) = i^\lambda D(\mathbf{a},\mathbf{b}) : \lambda \in \mathbb{Z}_4, (\mathbf{a},\mathbf{b}) \in \overline{E}\}, \tag{10}$$

if $q = 2$, forms an representation of the discrete Heisenberg-Weyl group on $\mathcal{H}$. This representation is irreducible [12, 4]. This means that there are no nontrivial subspaces of $\mathcal{H}$ invariant under the action of E.

The center of the group E, $Z(E)$, consists of the elements $\{\omega^\lambda I : \lambda \in \mathbb{Z}_q\}$, or $\{i^\lambda I : \lambda \in \mathbb{Z}_4\}$ if $q = 2$, where I is the identity operator on $\mathcal{H}$. The factor space $E/Z(E)$ is easily seen to be the phase space $\overline{E}$. Considering the commutation relation (8), we can define the *symplectic* inner product

$$((\mathbf{a},\mathbf{b}),(\mathbf{a}',\mathbf{b}')) = \mathbf{a}\cdot\mathbf{b}' - \mathbf{a}'\cdot\mathbf{b}, \tag{11}$$

on the phase space $\overline{E}$, and note that two operators $D(\mathbf{a},\mathbf{b})$ and $D(\mathbf{a}',\mathbf{b}')$ commute if and only if $((\mathbf{a},\mathbf{b}),(\mathbf{a}',\mathbf{b}')) = 0$. We may then identify subgroups of E consisting mutually commuting sets of operators $D(\mathbf{a},\mathbf{b})$ with isotropic submodules of $\overline{E}$. We also define the *symplectic dual*, or just dual, of any submodule (subspace) $\overline{H} \subseteq \overline{E}$ to be

$$\overline{H}^\perp = \{(\mathbf{a},\mathbf{b}) \in \overline{E} : ((\mathbf{a},\mathbf{b}),(\mathbf{a}',\mathbf{b}')) = 0, \forall\ (\mathbf{a}',\mathbf{b}') \in \overline{H}\}. \tag{12}$$

An isotropic subspace satisfies $\overline{H} \subseteq \overline{H}^\perp$. It is maximal isotropic if and only if this inclusion is an equality. An isotropic submodule (subspace) $\overline{H}$ of $\overline{E}$ corresponds to the Abelian subgroup $\{D(\mathbf{a},\mathbf{b}) : (\mathbf{a},\mathbf{b}) \in \overline{H}\}$ of E.

Finally, in this section, we consider the space of linear operators $\mathcal{O}$ on the Hilbert space $\mathcal{H}$. We have the following theorem, which can be prove by substituting (6) into (13):

Theorem 1. *Any operator $S \in \mathcal{O}$ can be represented as*

$$S = \frac{1}{|A|} \sum_{(\mathbf{a},\mathbf{b}) \in \overline{E}} \mathrm{Tr}(D(\mathbf{a},\mathbf{b})^\dagger S) D(\mathbf{a},\mathbf{b}). \qquad (13)$$

We refer to $s(\mathbf{a},\mathbf{b}) = \mathrm{Tr}(D(\mathbf{a},\mathbf{b})^\dagger S)$ as the Weyl transform of S.

Equation (13) implies that the map $S \to s(\mathbf{a},\mathbf{b}) = Tr(D(\mathbf{a},\mathbf{b})^\dagger S)$ gives an isometry from $\mathcal{O}$ to $\mathrm{L}^2(\overline{E})$, with the inner products related by

$$\mathrm{Tr}(S^\dagger R) = \frac{1}{|A|} \sum_{(\mathbf{a},\mathbf{b}) \in \overline{E}} \overline{s(\mathbf{a},\mathbf{b})} r(\mathbf{a},\mathbf{b}). \qquad (14)$$

We note that the orthogonal projection on to a vector $|\,\phi\rangle$, namely $|\,\phi\rangle\langle\phi\,|$, has the expansion

$$|\,\phi\rangle\langle\phi\,| = \frac{1}{|A|} \sum_{(\mathbf{a},\mathbf{b}) \in \overline{E}} \mathcal{A}_\phi(\mathbf{a},\mathbf{b}) D(\mathbf{a},\mathbf{b}), \qquad (15)$$

where $\mathcal{A}_\phi(\mathbf{a},\mathbf{b}) = \langle\phi|D(\mathbf{a},\mathbf{b})|\,\phi\rangle$ is the ambiguity function of $|\,\phi\rangle$.

3 Golay Sequences

Consider two unimodular sequences of complex numbers $\mathbf{x}$ and $\mathbf{y}$ of length N. Two such sequences are said to be *Golay complementary* if the sum of their respective autocorrelation functions satisfy

$$\mathrm{corr}_k(\mathbf{x}) + \mathrm{corr}_k(\mathbf{y}) = 2N\delta_{k,0}, \qquad (16)$$

for $k = -(N-1), \cdots, (N-1)$. We note that the remaining shifts are automatically zero. Such sequences have an extensive literature, a sample of which are [17, 16, 8, 2, 6, 7, 1, 5]. We can write the condition (16), at least for cyclic convolutions, in terms of a particular finite Heisenberg-Weyl group. We will show how results for linear convolutions can be recovered in Section 6.

We begin by considering the case in which the configuration space, which label positions in the sequence, takes the form $A = \mathbb{Z}_{2^m}$. In this case we define the Hilbert space $\mathcal{H}_m$ with Dirac basis

$$\mathcal{F}_D = \{|\,j\rangle : j \in \mathbb{Z}_{2^m}\}. \qquad (17)$$

We can then define the finite Heisenberg-Weyl group

$$\mathcal{E}_m = \{\omega^\mu \Delta(j,k) : \mu \in \mathbb{Z}_{2^m}, (j,k) \in \overline{\mathcal{E}}_m\}, \qquad (18)$$

where $\overline{\mathcal{E}}_m = \mathbb{Z}_{2^m} \times \mathbb{Z}_{2^m}$, $\omega = \exp(2\pi i/2^m)$ and the unitary operators $\Delta(j,k)$ are defined by

$$\Delta(j,k) = \sum_{l \in \mathbb{Z}_{2^m}} \omega^{kl} |\,l + j\rangle\langle l\,|. \qquad (19)$$

As noted above this is an irreducible representation.

The conditions for two vectors $|\,\phi\rangle$, $|\,\psi\rangle \in \mathcal{H}_m$ to be $\mathbb{Z}_{2^m}$-Golay complementary are,

1. $|\,\phi\rangle$ and $|\,\psi\rangle$ have unimodular coefficients (up to an overall normalising constant), and
2. for all non-zero $j \in \mathbb{Z}_{2^m}$,

$$\langle\phi|\Delta(j,0)|\,\phi\rangle + \langle\psi|\Delta(j,0)|\,\psi\rangle = 0. \qquad (20)$$

The condition (20) can be written equivalently as,

$$\mathrm{Tr}\left((|\,\phi\rangle\langle\phi\,| + |\,\psi\rangle\langle\psi\,|)\,\Delta(j,0)\right) = 0, \qquad (21)$$

which implies that the projector $Q = |\,\phi\rangle\langle\phi\,| + |\,\psi\rangle\langle\psi\,|$ must be orthogonal to the subspace $\mathcal{S}_\Delta$ spanned by the orthonormal set $\{\Delta(j,0) : j \in \mathbb{Z}_{2^m}, j \neq 0\}$ in the Hilbert-Schmidt class $\mathcal{O}$ of operators on $\mathcal{H}_m$.

Suppose, now, that we have bijection $\iota : \mathbb{Z}_{2^m} \to \mathbb{Z}_2^m$. Then each $|\,j\rangle \in \mathcal{F}_D$ can be labelled by a unique $\mathbf{a} \in \mathbb{Z}_{2^m}$; that is, a binary string, so that $|\,j\rangle \equiv |\,\mathbf{a}\rangle$, with $\iota(j) = \mathbf{a}$. We take ι to be the mapping from j to its binary representation. The bijection ι now allows us to define a unitary irreducible representation of the finite Heiseberg-Weyl group with configuration space $\mathbb{Z}_2^m$ on $\mathcal{H}_m$:

$$E_m = \{i^\lambda D(\mathbf{a},\mathbf{b}) : \lambda \in \mathbb{Z}_4, (\mathbf{a},\mathbf{b}) \in \overline{E}_m\}, \qquad (22)$$

where $\overline{E}_m = \mathbb{Z}_2^m \times \mathbb{Z}_2^m$ and the unitary operators $D(\mathbf{a},\mathbf{b})$ are defined by

$$D(\mathbf{a},\mathbf{b}) = \sum_{\mathbf{c} \in \mathbb{Z}_2^m} (-1)^{\mathbf{b}\cdot\mathbf{c}} |\,\mathbf{c} \oplus \mathbf{a}\rangle\langle\mathbf{c}\,|. \qquad (23)$$

Here we denote addition on $\mathbb{Z}_2^m$ by $\oplus$ to distinguish it from addition on $\mathbb{Z}_{2^m}$ in (18). Obviously, the bijection ι induces a bijection $\iota_2 : \overline{E}_m \to \overline{\mathcal{E}}_m$ given by $\iota_2(\mathbf{a},\mathbf{b}) = (j,k)$.

We shall consider the expansion of the $\Delta(j,0)$ in terms of the $D(\mathbf{a},\mathbf{b})$. Let us write this as

$$\Delta(j,0) = \sum_{(\mathbf{a},\mathbf{b}) \in \overline{E}_m} \alpha_j(\mathbf{a},\mathbf{b}) D(\mathbf{a},\mathbf{b}), \qquad (24)$$

where the α_j will be determined later.

In term of the Weyl representation (21) becomes

$$\sum_{(\mathbf{a},\mathbf{b}) \in \overline{E}_m} (\mathcal{A}_\phi + \mathcal{A}_\psi)(\mathbf{a},\mathbf{b})\ \alpha_j(\mathbf{a},\mathbf{b}) = 0, \quad j \neq 0, \qquad (25)$$

where $\mathcal{A}_\phi$ and $\mathcal{A}_\psi$ are the ambiguity functions of $|\,\phi\rangle$ and $|\,\psi\rangle$, and we have used (15). We see that a sufficient condition for the pair $(|\,\phi\rangle, |\,\psi\rangle)$ to be $\mathbb{Z}_{2^m}$-Golay complementary is that the supports of $\mathcal{A}_\phi + \mathcal{A}_\psi$ and α_j be disjoint

for all $j \neq 0$. We will define the support of an operator $S \in \mathcal{O}$ to be the support of its Weyl transform s, i.e., $\operatorname{supp} S = \operatorname{supp} s$, where

$$s(\mathbf{a},\mathbf{b}) = \frac{1}{2^m}\mathrm{Tr}(SD(\mathbf{a},\mathbf{b})^\dagger), \tag{26}$$

and we will further define the support of a subspace $\mathcal{S} \subset \mathcal{O}$ to be

$$\operatorname{supp}\mathcal{S} = \bigcup_{S\in\mathcal{S}} \operatorname{supp} S. \tag{27}$$

Proposition 1. *A sufficient condition for a pair of vectors $(|\phi\rangle, |\psi\rangle)$ to be $\mathbb{Z}_2^m$-Golay complementary is that*

$$\operatorname{supp}\,(\mathcal{A}_\phi + \mathcal{A}_\psi) \cap \operatorname{supp}\mathcal{S}_\Delta = \varnothing. \tag{28}$$

We note that the projector $D(\mathbf{a},\mathbf{b})QD(\mathbf{a},\mathbf{b})^\dagger$ has the same support as Q, for all $(\mathbf{a},\mathbf{b}) \in \overline{E}_m$. Thus, if $(|\phi\rangle, |\psi\rangle)$ satisfies (28), then so do $(D(\mathbf{a},\mathbf{b})|\phi\rangle, D(\mathbf{a},\mathbf{b})|\psi\rangle)$, for all $(\mathbf{a},\mathbf{b}) \in \overline{E}_m$.

Given the last statement it makes sense to try to minimise the support of the projection $Q = |\phi\rangle\langle\phi| + |\psi\rangle\langle\psi|$ or equivalently the function $\mathcal{A}_\phi + \mathcal{A}_\psi$. Now the 1-D projector $|\phi\rangle\langle\phi|$ associated with maximal isotropic subspaces of $\overline{E}_m$ or equivalently maximally commutative subgroups of E_m, have the smallest support of any of 1-D projectors. In fact, each maximal isotropic subspace $\overline{H} \subset \overline{E}_m$ is associated with an orthonormal basis,

$$\mathcal{F} = \{|\mathbf{a},\mathbf{b},\phi\rangle = D(\mathbf{a},\mathbf{b})|\phi\rangle : (\mathbf{a},\mathbf{b}) \in \overline{E}_m/\overline{H}\}. \tag{29}$$

where $|\phi\rangle$ is any normalised vector in $\mathcal{H}_m$ for which

$$D(\mathbf{a},\mathbf{b})|\phi\rangle\langle\phi|D(\mathbf{a},\mathbf{b})^\dagger = |\phi\rangle\langle\phi|, \tag{30}$$

for all $(\mathbf{a},\mathbf{b}) \in \overline{H}$. For all vectors in $|\phi'\rangle \in \mathcal{F}_{\overline{H}}$, the support of $|\phi'\rangle\langle\phi'|$ is $\overline{H}$.

By choosing a pair of vectors associated with the same maximal isotropic subspace $\overline{H}$, that is, taking

$$Q_{\overline{H}} = |\phi\rangle\langle\phi| + D(\mathbf{a}_1,\mathbf{b}_1)|\phi\rangle\langle\phi|D(\mathbf{a}_1,\mathbf{b}_1)^\dagger, \tag{31}$$

for some $(\mathbf{a}_1,\mathbf{b}_1) \in \overline{E}_m/\overline{H}$, we ensure that $\operatorname{supp} Q_{\overline{H}} \subseteq \operatorname{supp}\mathcal{A}_\phi = \overline{H}$. In fact, the Weyl transformation of $Q_{\overline{H}}$ is

$$\mathrm{Tr}(Q_{\overline{H}}D(\mathbf{a},\mathbf{b})^\dagger) = (1+(-1)^{\mathbf{a}_1\cdot\mathbf{b}+\mathbf{a}\cdot\mathbf{b}_1})\overline{\mathcal{A}_\phi(\mathbf{a},\mathbf{b})}, \tag{32}$$

so that, writing $\overline{K} = \{(\mathbf{0},\mathbf{0}),(\mathbf{a}_1,\mathbf{b}_1)\}$,

$$\operatorname{supp} Q_{\overline{H}} = \overline{H} \cap \overline{K}^\perp. \tag{33}$$

Thus, our goal is to find a maximal isotropic subspace $\overline{H}$ and a subspace $\overline{K}$ such that $\overline{H} \cap \overline{K}^\perp \cap \operatorname{supp}\mathcal{S}_\Delta = \varphi$.

We next consider the form of $\operatorname{supp}\mathcal{S}_\Delta$.

4 The support of $\mathcal{S}_\Delta$

Let $\mathcal{S}_\Delta \subset \mathcal{O}$ be the subspace spanned by the operators

$$\{\Delta(j,0) : j \in \mathbb{Z}_{2^m}, j \neq 0\}. \tag{34}$$

The operator $\Delta(j,0)$ has expansion coefficients in terms of the operators $D(\mathbf{a},\mathbf{b})$, given by

$$\begin{aligned}\alpha_j(\mathbf{a},\mathbf{b}) &= 2^{-m}\mathrm{Tr}\left(\Delta(j,0)D(\mathbf{a},\mathbf{b})^\dagger\right)\\ &= 2^{-m}\sum_{k\in\mathbb{Z}_{2^m}}\sum_{\mathbf{c}\in\mathbb{Z}_2^m}(-1)^{\mathbf{b}\cdot\mathbf{c}}\langle\mathbf{c}\oplus\mathbf{a}|k+j\rangle\langle k|\mathbf{c}\rangle\\ &= 2^{-m}\sum_{\mathbf{c}\in\mathbb{Z}_2^m}(-1)^{\mathbf{b}\cdot(\mathbf{c}\oplus\mathbf{a})}\langle\mathbf{c}|\mathbf{c}\oplus\mathbf{a}+j\rangle\\ &= 2^{-m}\sum_{\mathbf{c}\in\mathbb{Z}_2^m}(-1)^{\mathbf{b}\cdot(\mathbf{c}\oplus\mathbf{a})}\delta_{\mathbf{c},\mathbf{c}\oplus\mathbf{a}+j}.\end{aligned} \tag{35}$$

We denote by $C_{\mathbf{a}} \subseteq \mathbb{Z}_2^m$ the subspace of elements of $\mathbb{Z}_2^m$ which are covered by $\mathbf{a}$, by which we mean that they have 1 entries only where $\mathbf{a}$ has 1 entries. Write $\mathbf{w} = (1,0,0,\cdots,0) \in \mathbb{Z}_2^m$ and $\overline{\mathbf{w}} = (0,1,1,\cdots,1) \in \mathbb{Z}_2^m$. For $j \in \mathbb{Z}_{2^m}$, let A_j be the set of $\mathbf{a} \in \mathbb{Z}_2^m$ such that

$$\mathbf{c} - \mathbf{c}\oplus\mathbf{a} = j, \tag{36}$$

has a solution $\mathbf{c} \in \mathbb{Z}_2^m$.

Proposition 2.

$$\Delta(j,0) = \sum_{\mathbf{a}\in A_j}\frac{1}{|C_{\mathbf{a}}\cap C_{\overline{\mathbf{w}}}|}\sum_{\mathbf{b}\in C_{\mathbf{a}}\cap C_{\overline{\mathbf{w}}}}(-1)^{\mathbf{b}\cdot(\mathbf{c}_0(\mathbf{a},j)\oplus\mathbf{a})}D(\mathbf{a},\mathbf{b}), \tag{37}$$

where $\mathbf{c}_0(\mathbf{a},j)$ is the unique solution of

$$\mathbf{c}_0 - \mathbf{c}_0\oplus\mathbf{a} = j, \tag{38}$$

with $\mathbf{c}_0 \in C_{\mathbf{a}} \cap C_{\overline{\mathbf{w}}}$.

Now return to the subspace $\mathcal{S}_\Delta$ spanned by the set

$$\{\Delta(j,0) : j \in \mathbb{Z}_{2^m}, j \neq 0\}.$$

We have the following result.

Proposition 3. *The support of the subspace $\mathcal{S}_\Delta$ is*

$$\operatorname{supp}\mathcal{S}_\Delta = \{(\mathbf{a},\mathbf{b}) : \mathbf{a} \in \mathbb{Z}_2^m\backslash\{\mathbf{0}\}.\mathbf{b} \in C_{\mathbf{a}} \cap C_{\overline{\mathbf{w}}}\} \tag{39}$$

Proof. First note that $\mathbf{0} \notin A_j$ for $j \neq 0$. For each $\mathbf{a} \in \mathbb{Z}_2^m/\{\mathbf{0}\}$, there is at least one non-zero $j \in \mathbb{Z}$ such that $\mathbf{a} \in A_j$. For any such j, $\alpha_j(\mathbf{a},\mathbf{b}) \neq 0$, if and only if $\mathbf{b} \in C_{\mathbf{a}} \cap C_{\overline{\mathbf{w}}}$. □

Figure 1 shows the support of the subspace $\mathcal{S}_\Delta$ for $m = 4$ and $m = 5$. We note that the support has the form of a pair of Sierpinski triangles.

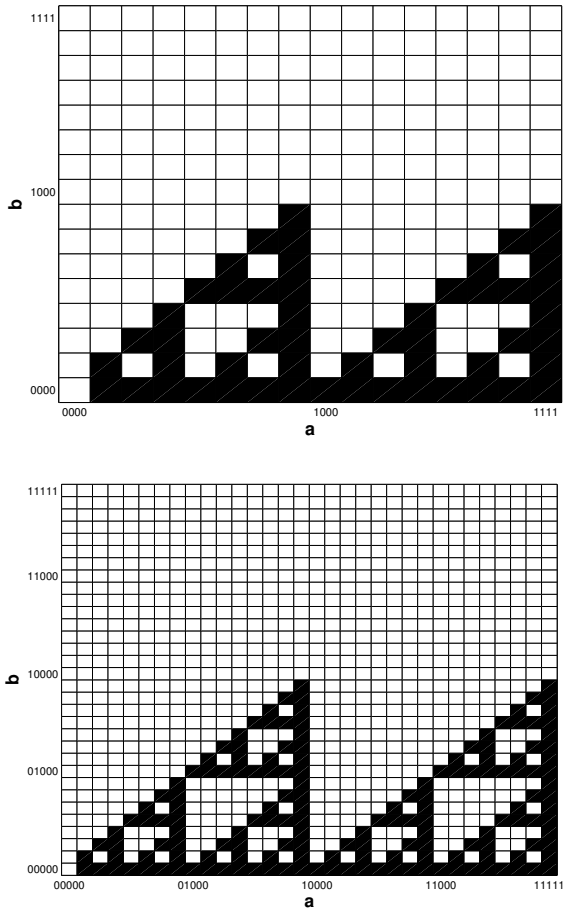

Figure 1: Supports of the subspace $\mathcal{S}_\Delta$ for $m = 4$ and $m = 5$.

5 Orthonormal bases of $\mathbb{Z}_{2^m}$-Golay pairs

Let us now consider the maximal isotropic subspaces $\overline{H}_{\mathsf{P}} \in \overline{E}_m$ which have an associated orthonormal basis consisting of elements whose coefficients have constant modulus. Such maximal isotropic subspaces take the form

$$\overline{H}_{\mathsf{P}} = \{(\mathbf{a}, \mathsf{P}\mathbf{a}) : \mathbf{a} \in \mathbb{Z}_2^m\}, \tag{40}$$

where P is any binary symmetric matrix. In this case we have

$$\overline{H}_{\mathsf{P}} \cap \operatorname{supp} \mathcal{S}_\Delta = \{(\mathbf{a}, \mathsf{P}\mathbf{a}) : \mathbf{a} \in \mathbb{Z}_2^m \backslash \{\mathbf{0}\}, \mathsf{P}\mathbf{a} \in C_{\mathbf{a}} \cap C_{\overline{\mathbf{w}}}\}. \tag{41}$$

The characters of $\mathbb{Z}_2^m \times \mathbb{Z}_2^m$ take the form

$$\gamma_{(\mathbf{a}', \mathbf{b}')}(\mathbf{a}, \mathbf{b}) = (-1)^{\mathbf{a}' \cdot \mathbf{b} \oplus \mathbf{a} \cdot \mathbf{b}'}, \tag{42}$$

where $(\mathbf{a}', \mathbf{b}') \in \mathbb{Z}_2^m \times \mathbb{Z}_2^m$.

Proposition 4. *Let $\overline{H}_{\mathsf{P}} \in \overline{E}_m$ be the maximal isotropic subspace corresponding to the binary symmetric matrix P as defined in* (40)*. If there exists a character $\gamma_{(\mathbf{a}_0, \mathbf{b}_0)}$ of $\mathbb{Z}_2^m \times \mathbb{Z}_2^m$, such that*

$$\gamma_{(\mathbf{a}_0, \mathbf{b}_0)}(\{(\mathbf{a}, \mathsf{P}\mathbf{a}) : \mathbf{a} \in \mathbb{Z}_2^m \backslash \{\mathbf{0}\}, \mathsf{P}\mathbf{a} \in C_{\mathbf{a}} \cap C_{\overline{\mathbf{w}}}\}) = \{-1\}, \tag{43}$$

then for each $|\,\phi\rangle \in \mathcal{F}_{\overline{H}_{\mathsf{P}}}$, the pair $(|\,\phi\rangle, D(\mathbf{a}_0, \mathbf{b}_0)|\,\phi\rangle)$ is $\mathbb{Z}_{2^m}$-Golay complementary.

Proof. This follows from the arguments in Section 3. □

Note that if there exist several characters $\gamma_{(\mathbf{a},\mathbf{b})}$ of $\mathbb{Z}_2^m \times \mathbb{Z}_2^m$, with $(\mathbf{a}, \mathbf{b}) \in \overline{E}_m / \overline{H}_{\mathsf{P}}$ such that (43) is satisfied, then each $|\,\phi\rangle \in \mathcal{F}_{\overline{H}_{\mathsf{P}}}$ will have several Goly complementary partners, one corresponding to each character. Also, the condition (43) is equivalent to stating that we can find an operator $D(\mathbf{a}_0, \mathbf{b}_0)$ which anticommutes with every element of the intersection $\{D(\mathbf{a}, \mathbf{b}) : (\mathbf{a}, \mathbf{b}) \in \overline{H}_{\mathsf{P}} \cap \operatorname{supp} \mathcal{S}_\Delta\}$.

Example For $m = 4$ Figure 2 shows the supports of the maximal isotropic subspaces $\overline{H}_{\mathsf{P}}$ and $\overline{H}_{\mathsf{Q}}$ with

$$\mathsf{P} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \mathsf{Q} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{44}$$

respectively. The maximal isotropic subspaces are show in red and magenta, with magenta at the points of overlap with $\mathcal{S}_\Delta$. $\overline{H}_{\mathsf{Q}}$ has $\mathbb{Z}_{2^m}$-Golay complementary sequences while $\overline{H}_{\mathsf{P}}$ does not. For $\overline{H}_{\mathsf{Q}}$ two characters satisfying (43) are $\gamma_{((0,0,0,0),(0,0,0,1))}$ and $\gamma_{((0,0,0,0),(0,1,0,0))}$.

6 $\mathbb{Z}$-Golay Sequences

We are particularly interested in conventional or $\mathbb{Z}$-Golay sequences, where the autocorrelation of the sequences is calculated on $\mathbb{Z}$ rather than on $\mathbb{Z}_{2^m}$. We now give a method for constructing such sequences from sequences which are Golay on $\mathbb{Z}_{2^{m+1}}$. We decompose $\mathbb{Z}_2^{m+1}$ into two subspaces $\mathbb{Z}_2^{m+1} = L \oplus U$ corresponding to $\mathbf{a} \in \mathbb{Z}_2^{m+1}$ whose most significant digit is a 0 or a 1 respectively. Both L and U are isomorphic to $\mathbb{Z}_2^m$. Consider a vector $|\,\psi\rangle \in \mathcal{H}_m$ of the form

$$|\,\psi\rangle = \sum_{\mathbf{a} \in L} \beta_{\mathbf{a}} |\,\mathbf{a}\rangle. \tag{45}$$

If a pair of vectors $(|\,\psi\rangle, |\,\psi'\rangle)$ of this form are $\mathbb{Z}_{2^m}$-Golay complementary then the sequences $(\{\beta_{\mathbf{a}} : \mathbf{a} \in L\}, \{\beta'_{\mathbf{a}} : \mathbf{a} \in L\})$ will be Golay complementary on $\mathbb{Z}$.

Consider the ambiguity function of a vector of the form (45). We have

$$\mathcal{A}_\psi(\mathbf{a}, \mathbf{b}) = 0, \quad \text{if } \mathbf{a} \in U, \tag{46}$$

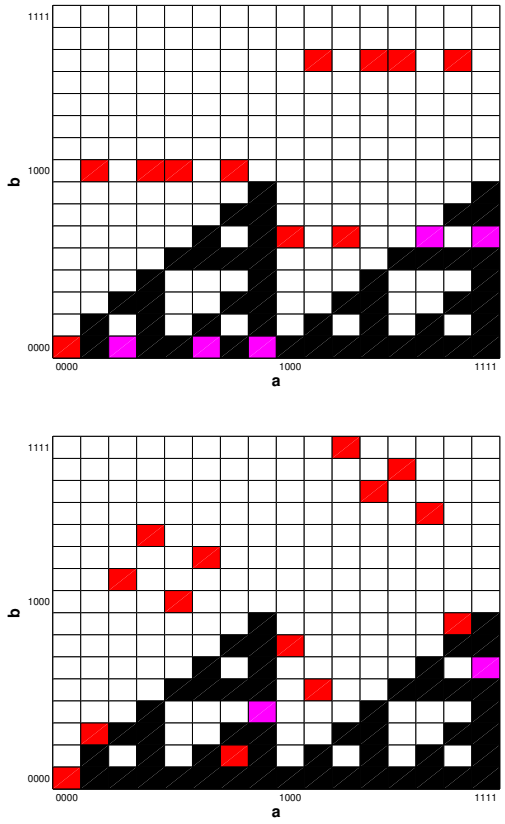

Figure 2: For $m = 4$, the maximal isotropic subspaces $\overline{H}_{\mathsf{P}}$ (upper) and $\overline{H}_{\mathsf{Q}}$ (lower) are shown in red and magenta, with magenta at the points of overlap with $\mathcal{S}_\Delta$. The matrices P and Q are given in (44). $\overline{H}_{\mathsf{Q}}$ has $\mathbb{Z}_{2^m}$-Golay complementary sequences while $\overline{H}_{\mathsf{P}}$ does not.

and

$$\mathcal{A}_\psi(\mathbf{a}, \mathbf{b} \oplus \mathbf{w}) = \mathcal{A}_\psi(\mathbf{a}, \mathbf{b}). \tag{47}$$

Identifying $\overline{E}_m$ with $L \times L$, we only need to ensure that the supports of $\mathcal{A}_\phi + \mathcal{A}_\psi$ do not intersect in $L \times L$. That is, we replace $\operatorname{supp} \mathcal{S}_\Delta$ is the above arguments with the set

$$\mathcal{R}_\Delta = \{(\mathbf{a}, \mathbf{b}) : \mathbf{a} \in \mathbb{Z}_2^m \backslash \{\mathbf{0}\}, \mathbf{b} \in C_{\mathbf{a}}\}, \tag{48}$$

a picture of which is shown in Figure 3 for $m = 4$.

We can state the following sufficient condition for the existence of orthonormal bases of $\mathbb{Z}$-Golay complementary sequences.

Proposition 5. *Let $\overline{H}_{\mathsf{P}} \in \overline{E}_m$ be the maximal isotropic subspace corresponding to the binary symmetric matrix P as defined in* (40)*. If there exists a character $\gamma_{(\mathbf{a}_0, \mathbf{b}_0)}$ of $\mathbb{Z}_2^m \times \mathbb{Z}_2^m$, such that*

$$\gamma_{(\mathbf{a}_0, \mathbf{b}_0)}(\{(\mathbf{a}, \mathsf{P}\mathbf{a}) : \mathbf{a} \in \mathbb{Z}_2^m \backslash \{\mathbf{0}\}, \mathsf{P}\mathbf{a} \in C_{\mathbf{a}}\}) = \{-1\}, \tag{49}$$

then for each $|\phi\rangle \in \mathcal{F}_{\overline{H}_{\mathsf{P}}}$, the pair $(|\phi\rangle, D(\mathbf{a}_0, \mathbf{b}_0)|\phi\rangle)$ is $\mathbb{Z}$-Golay complementary.

We will refer to a maximal isotropic subspace for which such a character exists as $\mathbb{Z}$-Golay. We note here that [6] points out the connection between Golay sequences and certain cosets of the first order Reed-Muller codes in the second order Reed-Muller codes. These cosets are intimately connected with the above maximal isotropic subspaces [4, 10].

This situation is illustrated in Figure 3 for the maximal isotropic subspace $\overline{H}_{\mathsf{P}} \subset \overline{E}_m$ with

$$\mathsf{P} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{50}$$

Two characters satisfying (49) are $\gamma_{((0,0,0,0),(0,0,0,1))}$ and $\gamma_{((0,0,0,0),(1,0,0,0))}$.

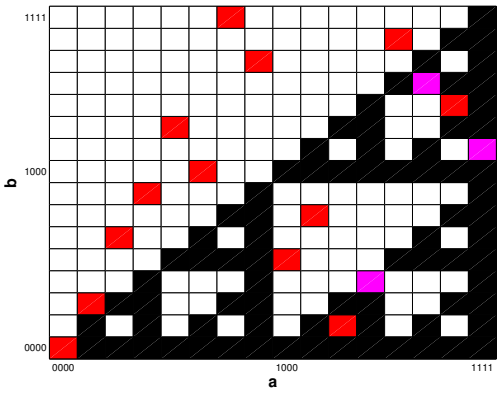

Figure 3: The set $\mathcal{R}_\Delta$ (black and magenta) and the support of the maximal isotropic subspace $\overline{H}_{\mathsf{P}} \in \overline{E}_4$ with P given by (50) (red and magenta). The intersection between the two sets is shown in magenta

7 An Example — Budisin Golay Sequences

In this section we consider the maximal isotropic subspaces associated with binary symmetric matrices of the form (50), in general, matrices with elements of the form

$$[\mathsf{P}_m]_{i,j} = \delta_{i,j+1} + \delta_{i+1,j}, \quad i, j = 1, \cdots, m. \tag{51}$$

wherever the indices make sense. These generate the classical Welti-PONS Golay complementary sequences. We write

$$\mathcal{I}_m = \{(\mathbf{a}, \mathsf{P}_m\mathbf{a}) : \mathbf{a} \in \mathbb{Z}_2^m \backslash \{\mathbf{0}\}, \mathsf{P}_m\mathbf{a} \in C_{\mathbf{a}}\}. \tag{52}$$

For $m = 2$ we have

$$\mathsf{P}_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{53}$$

and

$$\begin{aligned} \mathcal{I}_2 &= \{(\mathbf{a}, \mathsf{P}_2\mathbf{a}) : \mathbf{a} \in \mathbb{Z}_2^2 \backslash \{\mathbf{0}\}, \mathsf{P}_2\mathbf{a} \in C_{\mathbf{a}}\} \\ &= \{((1,1),(1,1))\}. \end{aligned} \tag{54}$$

For $m = 3$ we have

$$\mathsf{P}_3 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \tag{55}$$

and

$$\mathcal{I}_3 = \{((1,0,1),(0,0,0)),((1,1,1),(1,0,1))\}. \tag{56}$$

For $m = 4$ we have

$$\mathsf{P}_4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{57}$$

and

$$\begin{aligned} \mathcal{I}_4 =& \{((1,1,0,1),(1,1,0,0)),((1,0,1,1),(0,0,1,1)), \\ & ((1,1,1,1),(1,0,0,1))\}. \end{aligned} \tag{58}$$

Now we observe generally that if the first or last element of the vector $\mathbf{a}$ is 0, then $\mathsf{P}\mathbf{a} \in C_{\mathbf{a}}$ if, and only if, $\mathbf{a} = \mathbf{0}$. Furthermore, if $\mathbf{a}$ has a 0 at the $1 < n^{\text{th}} < m$ element and $\mathsf{P}\mathbf{a} \in C_{\mathbf{a}}$, then the $(n-1)^{\text{th}}$ and $(n+1)^{\text{th}}$ elements must be 1, i.e., a 0 always occurs in the combination $1, 0, 1$. This implies that the "$\mathbf{a}$" vectors in $\mathcal{I}_m$ are obtained by appending $0, 1$ to the vectors from $\mathcal{I}_{m-2}$ and appending 1 to the vectors from $\mathcal{I}_{m-1}$. Thus,

$$|\mathcal{I}_m| = |\mathcal{I}_{m-1}| + |\mathcal{I}_{m-2}|, \tag{59}$$

for $m > 3$, and so we see that for the matrices P_m in (51)

$$|\{(\mathbf{a}, \mathsf{P}_m\mathbf{a}) : \mathbf{a} \in \mathbb{Z}_2^m \backslash \{\mathbf{0}\}, \mathsf{P}_m\mathbf{a} \in C_{\mathbf{a}}\}| = F_m, \tag{60}$$

where F_m is the m^{th} term of the Fibonacci sequence ($F_1 = F_2 = 1$). It is also easily seen that for all $m > 1$

$$\gamma_{((0,0,\cdots,0,0),(0,0,\cdots,0,1))}(\mathcal{I}_m) = \{-1\}, \tag{61}$$

and

$$\gamma_{((0,0,\cdots,0,0),(1,0,\cdots,0,0))}(\mathcal{I}_m) = \{-1\}. \tag{62}$$

So for all $m > 1$ the maximal isotropic subspace $\overline{H}_{\mathsf{P}_m} \in \overline{E}_m$ is $\mathbb{Z}$-Golay.

The Budisin Golay complementary sequences correspond to the maximal isotropic subspaces with binary symmetric matrices

$$\mathsf{P}'_m = \mathsf{S}\mathsf{P}_m\mathsf{S}^T, \tag{63}$$

with P_m given by (50) with S any permutation matrix. There are $m!/2$ distinct P'. If we add an arbitrary non-zero binary diagonal matrix to P'_m we also obtain $\mathbb{Z}$-Golay complementary sequences but taking values in $\{1, i, -1, -i\}$ rather than in $\{1, -1\}$.

8 Conclusion

We have show in this paper that the finite Heisenberg-Weyl groups provide a new and fruitful way of viewing the Golay complementary sequences (complementary waveforms) and of understanding the origin of their special properties. The work we have presented here is a summary of particular results in a more general program of work in which the finite Heisenberg-Weyl groups are used as a unifying mathematical structure for analysing the correlation and cross-correlation of unimodular sequences and consequently phase code radar pulses.

Libraries of waveforms formed using these methods are able to provide collections of ambiguity functions that cover the range-Doppler plane in an efficient way, and thus provide the basic idea for a suite of waveforms optimized for extraction of information from the environment in an active sensing context.

Acknowledgements

This work was supported in part by the Defense Advanced Research Projects Agency of the US Department of Defense and was monitored by the Office of Naval Research under Contract No. N00014-02-1-0802. This paper is: Approved for Public Release, Distribution Unlimited.

References

[1] S. Z. Budisin. New complementary pairs of sequences. *Electron. Lett.*, 26:881–883, 1990.

[2] S. Z. Budisin, B. M. Popovic, and I. M. Indjin. Designing radar signals using complementary sequences. *IEEE Transactions on Aerospace and Electronic Systems*, 21(2):170–9, March 1985.

[3] J. S. Byrnes. Quadrature mirror filters, low crest factor arrays, functions achieving optimal uncertainty principle bounds, and complete orthonormal sequences - a unified approach. *Applied And Computational Harmonic Analysis*, 1:261–6, 1994.

[4] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel. Z_4-Kerdock codes, orthogonal spreads, and extremal Euclidian line-sets. *Proc. London Math. Soc.*, 3(75):436–480, 1997.

[5] R. Craigen. Complex Golay sequences. *J. Combin. Math. and Combin. Comput.*, 15:161–169, 1994.

[6] J. A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes. *IEEE Trans. Info. Theory*, 45(7):2397–2417, Nov. 1999.

[7] M. J. E. Golay. Multislit spectrometry. *J. Optical Society Am.*, 39:437, 1949.

[8] M. J. E. Golay. Complementary series. *IRE Transactions on Information Theory*, 7(12):82–87, April 1961.

[9] E. E. Hollis. A property of decomposable golay codes which greatly simplifies sidelobe calculation. *Proceedings of the IEEE*, pages 1727–1728, December 1975.

[10] S. D. Howard, A. R. Calderbank, and W. Moran. The finite Heisenberg-Weyl group in radar and communications. *EURASIP Journal of Applied Signal Processing*, to appear.

[11] J. A. LeMieux and F. M. Ingels. Analysis of FSK/PSK modulated radar signals using Costas arrays and complementary Welti codes. In *IEEE International Radar Conference*, pages 589–594, May 1990.

[12] G. W. Mackey. Some remarks on symplectic automorphisms. *Proc. Amer. Math Soc.*, 16:393–397, Aug. 1965.

[13] W. Miller. Topics in harmonic analysis with applications to radar and sonar. In R. Blahut, W. Miller, and C. Wilcox, editors, *Radar and Sonar, Part I*, IMA Volumes in Mathematics and its Applications. Springer-Verlag, New York, 1991.

[14] A. K. Ojha. Characteristics of complementary coded radar waveforms in noise and target fluctuation. In *Proceedings of IEEE Southeastcon*, Charlotte, NC, April 1993.

[15] B.M. Popović. Efficient golay correlator. *Electronics Letters*, 35(17), August 1999.

[16] H.S. Shapiro. Extremal problems for polynomials and power series. Sc.M. thesis, Massachusetts Institute of Technology, 1951.

[17] G. R. Welti. Quaternary codes for pulsed radar. *IRE Trans. Inf. Theory*, 6:400–408, 1960.