Hindawi Publishing Corporation
EURASIP Journal on Applied Signal Processing
Volume 2006, Article ID 85685, Pages 1–12
DOI 10.1155/ASP/2006/85685

# The Finite Heisenberg-Weyl Groups in Radar and Communications

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

[1] *Defence Science and Technology Organisation, P.O. Box 1500, Edinburgh 5111, Australia*
[2] *Program in Applied and Computational Mathematics, Princeton University, Princeton, NJ 08544, USA*
[3] *Department of Electrical and Electronic Engineering, The University of Melbourne, Victoria 3010, Australia*

Received 6 April 2005; Accepted 18 April 2005

We investigate the theory of the finite Heisenberg-Weyl group in relation to the development of adaptive radar and to the construction of spreading sequences and error-correcting codes in communications. We contend that this group can form the basis for the representation of the radar environment in terms of operators on the space of waveforms. We also demonstrate, following recent developments in the theory of error-correcting codes, that the finite Heisenberg-Weyl groups provide a unified basis for the construction of useful waveforms/sequences for radar, communications, and the theory of error-correcting codes.



## 1. INTRODUCTION

The continuous Heisenberg-Weyl groups have a long history in physics [1], in the theory of radar detection [2, 3], and in signal processing. However, their discrete variants [4–6] have been scarcely noticed, notable exceptions being [7, 8].

Our interest in the finite Heisenberg-Weyl groups stems from an attempt to develop an information theory of radar that is flexible enough to be applied to modern radars. Such modern radars have the capacity to adaptively switch waveforms on a pulse-to-pulse basis and to retain coherence over many pulses, but these capacities are only just beginning to be exploited. If we are to fully exploit this waveform agility in both modern and future radars two important problems need to be addressed. The first is the representation of the environment as it pertains to the transmission of radar waveforms. This includes both targets and background clutter. The second important problem is to ensure that one has a sufficiently flexible set of waveforms to enable the choice of a waveform optimal for a given situation.

One purpose of the present paper is to show that both of these problems can be approached to a large extent within the same mathematical framework, that is, through the theory of the finite Heisenberg-Weyl groups [4–6]. It is well known that the continuous Heisenberg-Weyl group has application to the theory of radar, for example see [2, 3], but the discrete version of this group has received little attention in radar. Since, in practical terms, the resolution of a radar is finite, by choosing a fine enough discretization in range and Doppler we can treat the radar perfectly well with the one-dimensional finite Heisenberg-Weyl group. This has a number of advantages, one of which is that the radar environment can be represented by a matrix acting on the space of waveforms.

In both radar and communications one is interested in finding unimodular sequences with good auto- and cross-correlation properties. From the perspective of communications one is interested in finding large classes of spreading sequences with minimal interference, or cross-correlation, between the sequences (see [9, 10]). More good spreading sequences means increased system capacity.

The $m$-dimensional finite Heisenberg-Weyl group provides a unifying framework for a number of important sequences significant in the construction of phase-coded radar waveforms, in communications as spreading sequences, and in the theory of error-correcting codes. Among the sequences that can be associated with the Heisenberg-Weyl groups are the first- and second-order Reed-Muller codes, Welti and other Golay complementary sequences [11–13], and the Kerdock and Preparata codes [14, 15], which are nonlinear binary error-correcting codes containing more codewords for a given minimum distance than any linear code. Many of these sequences and codes are associated with decomposition of the Heisenberg-Weyl group into disjoint maximal Abelian subgroups.

The overall purpose of this paper is to introduce the finite Heisenberg-Weyl groups as a useful tool in radar and

communications, and to demonstrate their power to unify and simplify a number of concepts in these areas. Accordingly, in many instances throughout the paper we will merely indicate the relationship of some concepts to the general theory without going into detail.

The paper is organised as follows. In Section 2 we construct the finite Heisenberg-Weyl groups in terms of their irreducible unitary representations on finite-dimensional Hilbert spaces, and discuss some of their properties. Then in Section 3 we briefly develop the theory of discrete radar in terms of the one-dimensional Heisenberg-Weyl group and introduce the concept of an ambiguity function of a waveform within this framework. In Section 4, we discuss the representation of linear operators on the Hilbert space supporting an irreducible representation of the Heisenberg-Weyl group. We define the Weyl transform of an operator and define the ambiguity function of a Hilbert space vector in this general setting.

Section 5 provides the main contribution of the paper; it extends the theory developed in [15] for the extraspecial 2-group, which is the finite Heisenberg-Weyl group of Section 2 corresponding to $p = 2$, to the other Heisenberg-Weyl groups. We develop this theory based on analysis of the ambiguity functions associated with the irreducible representations of the group. We show that the maximal Abelian subgroups of the Heisenberg-Weyl groups can be associated with orthonormal bases in the representation space, and that the angles between the vectors in two such bases are simply determined by the relationship between their associated maximal Abelian subgroups. We then show how the Heisenberg-Weyl can be decomposed into disjoint maximal Abelian subgroups with the help of certain symplectic automorphisms, which are defined in Section 6.

In Sections 7 and 8, we relate the general theory to the known cases of discrete radar and the $\mathbf{Z}_4$-Kerdock codes [15]. We find that the theory that leads to the Kerdock codes in the multidimensional ($p = 2$) Heisenberg-Weyl group leads to linear frequency-modulated waveforms when applied to discrete radar. Finally, in Section 9 we briefly consider the connection between the Kerdock sets and the Welti and Budisin sequences, which are Golay complementary.

## 2. THE FINITE HEISENBERG-WEYL GROUPS [4]

We begin by defining a configuration space $A = \mathbb{Z}_p^m$ consisting of $m$-tuples of elements from the integers modulo $p$. In this paper we will take $p$ to be a prime number. Under elementwise addition $A$ forms an Abelian group. In radar theory the space $A$, with $m = 1$, would represent discrete ranges, while in discrete quantum mechanics the space $A$ might be used to 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" or Dirac 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 by $\widehat{A}$, is comprised of the homomorphisms from the group $A$ into the unit circle $\Pi$ in $\mathbb{C}$, that is, the characters of $A$ (see [16, Chapter 4]). $\widehat{A}$ is also an Abelian group (this time under multiplication), and is, since $A$ is finite, isomorphic to $A$. This isomorphism is made explicit through the identification of each $\mathbf{b} \in A$ with a $\gamma_{\mathbf{b}} \in \widehat{A}$, such that

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

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

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

The set $\{|\,\widehat{\mathbf{a}}\rangle : \mathbf{a} \in A\}$ 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 $A\times\widehat{A} \simeq A\times A$, which is a vector space over the field $\mathbb{Z}_p$, by $\overline{E}$. 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 [17]

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

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

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

where $\dagger$ denotes adjoint and $I$ is the identity operator on $\mathcal{H}$. Since the $D(\mathbf{a},\mathbf{b})$ are unitary operators, (7) implies that

$$D(\mathbf{a},\mathbf{b})^{-1} = D(\mathbf{a},\mathbf{b})^{\dagger} = \omega^{\mathbf{b}\cdot\mathbf{a}}D(-\mathbf{a},-\mathbf{b}). \tag{9}$$

For any of the operators $D(\mathbf{a},\mathbf{b})$, the repeated application of (7) implies

$$D(\mathbf{a},\mathbf{b})^{p} = \omega^{p(p-1)\mathbf{a}\cdot\mathbf{b}/2}I = \begin{cases} I & \text{if } p \neq 2, \\ (-1)^{\mathbf{a}\cdot\mathbf{b}}I & \text{if } p = 2. \end{cases} \tag{10}$$

That is, for $p = 2$, $D(\mathbf{a},\mathbf{b})^2$ can be either $\pm I$. This result points to a difference in structure between the cases $p = 2$ and $p \neq 2$.

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

$$E = \begin{cases} \{T(\lambda,\mathbf{a},\mathbf{b}) = \omega^{\lambda} D(\mathbf{a},\mathbf{b}) : \lambda \in \mathbb{Z}_p,\ (\mathbf{a},\mathbf{b}) \in \overline{E}\} & \text{if } p \neq 2, \\ \{T(\lambda,\mathbf{a},\mathbf{b}) = i^{\lambda} D(\mathbf{a},\mathbf{b}) : \lambda \in \mathbb{Z}_4,\ (\mathbf{a},\mathbf{b}) \in \overline{E}\} & \text{if } p = 2 \end{cases} \tag{11}$$

form a representation of the finite Heisenberg-Weyl group on $\mathcal{H}$. This representation is irreducible [4, 15]. This means that there are no nontrivial subspaces of $\mathcal{H}$ invariant under the action of $E$. This representation is referred to as a multiplier representation of the group $A \times \widehat{A}$. The finite Heisenberg-Weyl group itself can be realised abstractly as a central extension of $A \times \widehat{A}$ by $\mathbb{Z}_p$ ($p \neq 2$) and by $\mathbb{Z}_4$ ($p = 2$).

Now the centre of the group $E$ is

$$Z(E) = \begin{cases} \{\omega^{\lambda} I : \lambda \in \mathbb{Z}_p\} & \text{if } p \neq 2, \\ \{i^{\lambda} I : \lambda \in \mathbb{Z}_4\} & \text{if } p = 2. \end{cases} \tag{12}$$

The factor space $E/Z(E)$ is easily seen to be identified with the phase space $\overline{E}$.

Considering the commutation relation (8), we can define the *symplectic* inner product

$$((\mathbf{a},\mathbf{b}),(\mathbf{a}',\mathbf{b}')) = \mathbf{a}\cdot\mathbf{b}' - \mathbf{a}'\cdot\mathbf{b}, \tag{13}$$

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 of mutually commuting sets of operators $D(\mathbf{a},\mathbf{b})$ with isotropic subspaces of $\overline{E}$. A subspace $\overline{H} \subset \overline{E}$ is isotropic if any pair of points $(\mathbf{a},\mathbf{b}),(\mathbf{a}',\mathbf{b}') \in \overline{H}$ satisfy $((\mathbf{a},\mathbf{b}),(\mathbf{a}',\mathbf{b}')) = 0$. An isotropic subspace $\overline{H}$ of $\overline{E}$ corresponds to the Abelian subgroup $\{D(\mathbf{a},\mathbf{b}) : (\mathbf{a},\mathbf{b}) \in \overline{H}\}$ of $E$. We also define the *symplectic dual*, or just dual, of any subspace $\overline{H} \subseteq \overline{E}$ to be

$$\overline{H}^{\perp} = \{(\mathbf{a},\mathbf{b}) \in \overline{E} : ((\mathbf{a},\mathbf{b}),(\mathbf{a}',\mathbf{b}')) = 0,\ \forall (\mathbf{a}',\mathbf{b}') \in \overline{H}\}. \tag{14}$$

An isotropic subspace satisfies $\overline{H} \subseteq \overline{H}^{\perp}$. It is maximal isotropic if and only if this inclusion is an equality.

## 3. DISCRETE RADAR

Let us see how the above theory applies to radar. For radar the configuration space $A = \mathbb{Z}_p$ consists of a large number $p$ of discrete time delays or ranges. To make the development more transparent we label the elements of $A$ by $\tau \in \mathbb{Z}_p$ and $\widehat{A}$ by $\nu \in \mathbb{Z}_p$, rather than by $\mathbf{a}$ and $\mathbf{b}$. $\nu/p$ is the digital frequency. The phase space $\overline{E}$ in this case is the time-frequency plane. The vectors $|\phi\rangle \in \mathcal{H}$ are our waveforms, and their expansion coefficients in the Dirac basis $\phi(\tau) = \langle \tau | \phi \rangle$ give their $p$-periodic time sequences. The Dirac basis waveforms $|\tau\rangle$ correspond to impulses at time $\tau$. The Fourier basis corresponds to fixed frequency sinusoidal waveforms, since these have coefficients $\langle \tau | \widehat{\nu} \rangle = \sqrt{i/p}\,\omega^{\nu\tau}$.

Abstractly, the operation of the radar consists of transmitting a waveform $|\phi\rangle \in \mathcal{H}$, which is reflected by the environment, or radar scene, and returns as the waveform $|\psi\rangle \in \mathcal{H}$. Thus, the radar scene can be considered an operator, $S$, on $\mathcal{H}$.

Physically we can decompose the radar scene into point scatters, each of which delays the waveform by a time $\tau$ and Doppler shifts the waveform by $\nu$, with the return being multiplied by a complex scattering amplitude $\sigma(\tau,\nu)$. Mathematically we write this as

$$S = \sum_{(\tau,\nu)\in\overline{E}} \sigma(\tau,\nu) D(\tau,\nu), \tag{15}$$

where the $D(\tau,\nu) \in E$ are elements of the Heisnberg-Weyl group. Theorem 1, in the next section, implies that the scatterer distribution $\sigma(\tau,\nu) = \mathrm{Tr}(D(\tau,\nu)^{\dagger} S)/|A|$, and that every operator on $\mathcal{H}$ can be written in this form.

Suppose that we have an unknown radar scene $S$ and we would like to learn something about it. We transmit a waveform $|\phi\rangle$ and note the return $|\psi\rangle$. In the absence of noise we now know that $|\psi\rangle = S|\phi\rangle$, or that

$$S = |\psi\rangle\langle\phi| + R, \tag{16}$$

where the operator $R$, which annihilates $|\phi\rangle$, $R|\phi\rangle = 0$, is undetermined. Thus, as a result of transmitting $|\phi\rangle$, we now know the action of the operator

$$\widetilde{S} = S|\phi\rangle\langle\phi|, \tag{17}$$

which in terms of scatterer distributions is

$$\widetilde{S} = \sum_{(\tau,\nu)\in\overline{E}} \widetilde{\sigma}(\tau,\nu) D(\tau,\nu), \tag{18}$$

where

$$\begin{aligned} \widetilde{\sigma}(\tau,\nu) &= \mathrm{Tr}\left(D(\tau,\nu)^{\dagger} S|\phi\rangle\langle\phi|\right) \\ &= \sum_{(\tau',\nu')\in\overline{E}} \sigma(\tau',\nu')\,\mathrm{Tr}\left(D(\tau,\nu)^{\dagger} D(\tau',\nu')|\phi\rangle\langle\phi|\right) \\ &= \sum_{(\tau',\nu')\in\overline{E}} \sigma(\tau',\nu')\mathcal{A}_{\phi}(\tau'-\tau,\nu'-\nu)\omega^{\nu(\tau-\tau')}, \end{aligned} \tag{19}$$

and the *ambiguity function*, $\mathcal{A}$, is given by [2, 3, 18]

$$\mathcal{A}_{\phi}(\tau,\nu) = \mathrm{Tr}\left(D(\tau,\nu)|\phi\rangle\langle\phi|\right) = \langle\phi|D(\tau,\nu)|\phi\rangle. \tag{20}$$

From (19), the ambiguity function can be considered as a point spread function on the scatterer distribution $\sigma(\tau,\nu)$. However, the fact that (19) is a representation of the operator relation (17) should always be kept in mind. We now go back and consider the ambiguity function in the more general setting of Section 2.

## 4. THE AMBIGUITY FUNCTIONS AND THE REPRESENTATION OF OPERATORS

In this section, we consider the space of linear operators $\mathcal{O}$ on the Hilbert space $\mathcal{H}$. These operators form a Hilbert space in

their own right, with the inner product of two operators $R$ and $S \in \mathcal{O}$ defined by

$$(R, S) = \mathrm{Tr}\,(R^\dagger S). \tag{21}$$

This inner product corresponds to the Hilbert-Schmidt or Frobenius norm

$$\|S\| = \mathrm{Tr}\,(S^\dagger S)^{1/2}. \tag{22}$$

The operators

$$\left\{\frac{1}{\sqrt{|A|}} D(\mathbf{a},\mathbf{b}) : (\mathbf{a},\mathbf{b}) \in \overline{E}\right\} \tag{23}$$

form an orthonormal set in $\mathcal{O}$, as

$$\mathrm{Tr}\,(D(\mathbf{a},\mathbf{b})^\dagger D(\mathbf{a}',\mathbf{b}')) = |A|\delta_{\mathbf{a},\mathbf{a}'}\delta_{\mathbf{b},\mathbf{b}'}. \tag{24}$$

Hence, since the set (23) has order $|\overline{E}| = |A|^2$, we have the following theorem.

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

$$S = \frac{1}{|A|} \sum_{(\mathbf{a},\mathbf{b})\in\overline{E}} \mathrm{Tr}\,(D(\mathbf{a},\mathbf{b})^\dagger S) D(\mathbf{a},\mathbf{b}). \tag{25}$$

The corresponding theorem for the continuous Heisenberg-Weyl group is given by Folland (see [1, Chapter 1]) and for the general case of the Heisenberg-Weyl group over locally compact Abelian groups by Feichtinger and Kozek [19].

The expansion (25) implies that the map

$$S \longrightarrow s(\mathbf{a},\mathbf{b}) = \frac{1}{\sqrt{|A|}} \mathrm{Tr}\,(D(\mathbf{a},\mathbf{b})^\dagger S) \tag{26}$$

is an isometry from $\mathcal{O}$ to $L^2(\overline{E})$, with the inner products related by

$$\mathrm{Tr}\,(S^\dagger R) = \sum_{(\mathbf{a},\mathbf{b})\in\overline{E}} \overline{s(\mathbf{a},\mathbf{b})} r(\mathbf{a},\mathbf{b}). \tag{27}$$

We refer to function $s(\mathbf{a},\mathbf{b})$ and the Weyl transform of the operator $S$.

Let $|\phi\rangle \in \mathcal{H}$ be a normalised vector. The projection operator into the one-dimensional subspace spanned by $|\phi\rangle$ is $P_\phi = |\phi\rangle\langle\phi| \in \mathcal{O}$. We assume that $|\phi\rangle$ is normalised so that $P_\phi$ is an orthogonal projection satisfying $P_\phi^2 = P_\phi$. The effect of $P_\phi$ on any vector $|\psi\rangle \in \mathcal{H}$ is

$$P_\phi|\psi\rangle = \langle\phi|\psi\rangle|\phi\rangle. \tag{28}$$

The operator $P_\phi$ has the expansion

$$P_\phi = \frac{1}{|A|} \sum_{(\mathbf{a},\mathbf{b})\in\overline{E}} \overline{\mathcal{A}_\phi(\mathbf{a},\mathbf{b})} D(\mathbf{a},\mathbf{b}), \tag{29}$$

where

$$\mathcal{A}_\phi(\mathbf{a},\mathbf{b}) = \mathrm{Tr}\,(D(\mathbf{a},\mathbf{b})P_\phi) = \langle\phi|D(\mathbf{a},\mathbf{b})|\phi\rangle. \tag{30}$$

As it is a direct generalization of the more usual definition (20) of the ambiguity function for $\mathbb{Z}_p$, we will also refer to the function $\mathcal{A}_\phi \in L^2(\overline{E})$ as the *ambiguity function* of the vector $|\phi\rangle$, or more correctly of the projection $P_\phi$. It is trivially related to the Weyl transformation of $P_\phi$, $p_\phi \in L^2(\overline{E})$, by $\mathcal{A}_\phi = \sqrt{|A|}\overline{p_\phi}$. We note that (30) is identical in form to the short-time Fourier transform when using the same function as input function and as analysis window. However, as we have noted above, we consider the ambiguity function to be a representation of the projection onto the one-dimensional subspace defined by the vector rather than a transformation of the vector itself.

Two properties of ambiguity functions that follow directly from its definition and (9) are

$$\mathcal{A}_\phi(\mathbf{0},\mathbf{0}) = 1, \qquad \overline{\mathcal{A}_\phi(\mathbf{a},\mathbf{b})} = \omega^{\mathbf{a}\cdot\mathbf{b}}\mathcal{A}_\phi(-\mathbf{a},-\mathbf{b}), \tag{31}$$

for all $(\mathbf{a},\mathbf{b}) \in \overline{E}$.

An important property of ambiguity functions is Moyal's identity. This follows from a simple property of projection operators. Suppose that $P_\phi$ and $P_\psi \in \mathcal{O}$ are one-dimensional projection operators. Then

$$\mathrm{Tr}\,(P_\phi P_\psi) = |\langle\phi|\psi\rangle|^2. \tag{32}$$

Substituting the expansion (29) in this equation we obtain Moyal's identity

$$\frac{1}{|A|} \sum_{(\mathbf{a},\mathbf{b})\in\overline{E}} \overline{\mathcal{A}_\phi(\mathbf{a},\mathbf{b})}\mathcal{A}_\psi(\mathbf{a},\mathbf{b}) = |\langle\phi|\psi\rangle|^2. \tag{33}$$

A special case of Moyal's identity is

$$\frac{1}{|A|} \sum_{(\mathbf{a},\mathbf{b})\in\overline{E}} |\mathcal{A}_\phi(\mathbf{a},\mathbf{b})|^2 = 1. \tag{34}$$

Suppose we apply the operator $D(\mathbf{a},\mathbf{b}) \in E$ to the vector $|\phi\rangle \in \mathcal{H}$ to obtain $|\phi'\rangle = D(\mathbf{a},\mathbf{b})|\phi\rangle$. Then the projection $P_{\phi'}$ is related to $P_\phi$ by

$$P_{\phi'} = D(\mathbf{a},\mathbf{b})^\dagger P_\phi D(\mathbf{a},\mathbf{b}), \tag{35}$$

and so, using (30) and the cyclic property of trace, we have

$$\begin{aligned}\mathcal{A}_{\phi'}(\mathbf{a}',\mathbf{b}') &= \mathrm{Tr}\,(D(\mathbf{a},\mathbf{b})D(\mathbf{a}',\mathbf{b}')D(\mathbf{a},\mathbf{b})^\dagger P_\phi)\\ &= \omega^{\mathbf{a}'\cdot\mathbf{b}-\mathbf{a}\cdot\mathbf{b}'}\,\mathrm{Tr}\,(D(\mathbf{a}',\mathbf{b}')P_\phi)\\ &= \omega^{\mathbf{a}'\cdot\mathbf{b}-\mathbf{a}\cdot\mathbf{b}'}\mathcal{A}_\phi(\mathbf{a}',\mathbf{b}'),\end{aligned} \tag{36}$$

for all $(\mathbf{a},\mathbf{b}) \in \overline{E}$. We observe this is just the multiplication of $\mathcal{A}_\phi$ by a character of $E$.

We can extend the conjugate action of the Heisenberg-Weyl group on projections (35) to the whole of $\mathcal{O}$. For each $D(\mathbf{a},\mathbf{b}) \in E$, this conjugate action maps $S \to S' \in \mathcal{O}$, such that

$$S' = D(\mathbf{a},\mathbf{b})^\dagger S D(\mathbf{a},\mathbf{b}). \tag{37}$$

Note that the centre of $E$, $Z(E)$, leaves each operator in $\mathcal{O}$ invariant. Under the Weyl transformation (26), the conjugate

action (37) on $\mathcal{O}$ induces the following action on $L^2(\overline{E})$: $s \to s' \in L^2(\overline{E})$, such that

$$s'(\mathbf{a}', \mathbf{b}') = \omega^{\mathbf{a}'\cdot\mathbf{b}-\mathbf{a}\cdot\mathbf{b}'} s(\mathbf{a}', \mathbf{b}'), \tag{38}$$

where $s$ and $s'$ are the Weyl transforms of $S$ and $S'$, respectively. As we have observed above, the action (38) is just a multiplication by a character of $E$.

Ideally in radar one would like to construct an ambiguity function which is nonzero only at the origin $(\mathbf{0}, \mathbf{0})$. However, since any ambiguity function is unity at the origin this violates Moyal's identity (34). We can, however, set our sights lower. We will refer to an ambiguity function $\mathcal{A}_\phi$ as perfect if its absolute value is constant on $\overline{E}/\{(\mathbf{0}, \mathbf{0})\}$. It turns out that at least in some circumstances vectors having such ambiguity functions exist. We will give an example below. Moyal's identity implies that a perfect ambiguity function satisfies

$$|\mathcal{A}_\phi(\mathbf{a}, \mathbf{b})| = \begin{cases} 1 & \text{for } (\mathbf{a}, \mathbf{b}) = (\mathbf{0}, \mathbf{0}), \\ \dfrac{1}{\sqrt{|A|+1}} & \text{for } (\mathbf{a}, \mathbf{b}) \in \overline{E}/\{(\mathbf{0}, \mathbf{0})\}. \end{cases} \tag{39}$$

If a vector $|\phi\rangle \in \mathcal{H}$ has a perfect ambiguity function then the set of vectors

$$\{|\mathbf{a}, \mathbf{b}, \phi\rangle = D(\mathbf{a}, \mathbf{b})|\phi\rangle : (\mathbf{a}, \mathbf{b}) \in \overline{E}\} \tag{40}$$

satisfy

$$\begin{aligned} |\langle \mathbf{a}, \mathbf{b}, \phi | \mathbf{a}', \mathbf{b}', \phi\rangle| &= |\langle \phi | D(\mathbf{a}' - \mathbf{a}, \mathbf{b}' - \mathbf{b}) | \phi\rangle| \\ &= \frac{1}{\sqrt{|A|+1}}, \end{aligned} \tag{41}$$

for $(\mathbf{a}, \mathbf{b}) \neq (\mathbf{a}', \mathbf{b}')$. That is, (40) constitutes a set of equiangular lines in $\mathcal{H}$. Thus, we see that perfect ambiguity functions are equivalent to sets of equiangular lines in $\mathcal{H}$. We note that Delsarte, Goethals, and Seidel originated a method based on orthogonal polynomials that provides upper bounds on the size of set of Euclidean lines with prescribed angles [20]. The special case of equiangular lines is explored by Lemmens and Seidel in [21]. A perfect ambiguity function achieves exactly this bound as there are exactly $|A|^2$ lines. We can construct a set of equiangular lines for the case $A = \mathbb{Z}_2^3$, as follows.

Consider the vector $|\eta\rangle \in \mathcal{H}$,

$$|\eta\rangle = \sqrt{\frac{2}{3}}(F - I)|\mathbf{0}\rangle = \sqrt{\frac{2}{3}}(|\hat{\mathbf{0}}\rangle - |\mathbf{0}\rangle), \tag{42}$$

where $|\mathbf{0}\rangle$ is the Dirac basis vector corresponding to $\mathbf{a} = \mathbf{0}$, $|\hat{\mathbf{0}}\rangle$ is the $\mathbf{a} = \mathbf{0}$ vector in the Fourier basis, and $F$ is the Fourier transform operator (5). Writing $\zeta = \sqrt{i/8}$, we verify that the set $\{|\mathbf{a}, \mathbf{b}, \eta\rangle = D(\mathbf{a}, \mathbf{b})|\eta\rangle : (\mathbf{a}, \mathbf{b}) \in \overline{E}\}$ is indeed equiangular:

$$\begin{aligned} \langle \eta | D(\mathbf{a}, \mathbf{b}) | \eta\rangle &= \frac{2}{3}\big(\langle \hat{\mathbf{0}} | D(\mathbf{a}, \mathbf{b}) | \hat{\mathbf{0}}\rangle + \langle \mathbf{0} | D(\mathbf{a}, \mathbf{b}) | \mathbf{0}\rangle \\ &\qquad - \langle \hat{\mathbf{0}} | D(\mathbf{a}, \mathbf{b}) | \mathbf{0}\rangle - \langle \mathbf{0} | D(\mathbf{a}, \mathbf{b}) | \hat{\mathbf{0}}\rangle\big) \\ &= \frac{2}{3}\delta_{\mathbf{b},\mathbf{0}} + \frac{2}{3}\delta_{\mathbf{a},\mathbf{0}} - \frac{2}{3}\left(\overline{\zeta} + (-1)^{\mathbf{b}\cdot\mathbf{a}}\zeta\right) \\ &= \frac{1}{3}\begin{cases} 2\delta_{\mathbf{b},\mathbf{0}} + 2\delta_{\mathbf{a},\mathbf{0}} - 1 & \text{if } \mathbf{b}\cdot\mathbf{a} = 0, \\ i & \text{if } \mathbf{b}\cdot\mathbf{a} = 1, \end{cases} \end{aligned} \tag{43}$$

where we have used (6) and the fact that $\overline{\zeta} + \zeta = 1/2$ and $\overline{\zeta} - \zeta = -i/2$.

A set of equiangular lines for this situation was given by Hoggar [22]. The utility of the Heisenberg-Weyl approach can be seen by comparing the above construction and verification with Hoggar's. Other sets of equiangular lines have been constructed by Renes et al. [17], for the one-dimensional Heisenberg-Weyl group corresponding to $A = \mathbb{Z}_k$, for specific values of $k$. For more information on the important problem of the construction of sets of equiangular lines and its relation to a number of important problems in mathematics and physics the reader is referred to [23].

Finally, we note that the set (40) is an orbit in $\mathcal{H}$ under the Heisenberg-Weyl group. In the next section we will consider the properties of such orbits in detail.

## 5. COVARIANT TIGHT FRAMES AND AMBIGUITY FUNCTIONS

We can understand a great deal about the structure of ambiguity functions associated with the vectors in $\mathcal{H}$, by understanding the orbits in $\mathcal{H}$ under the action of the Heisenberg-Weyl group $E$. The orbit containing the vector $|\phi\rangle \in \mathcal{H}$ consists of the set of vectors

$$\{|\lambda, \mathbf{a}, \mathbf{b}, \phi\rangle = T(\lambda, \mathbf{a}, \mathbf{b})|\phi\rangle : \lambda \in \mathbb{Z}_q,\ (\mathbf{a}, \mathbf{b}) \in \overline{E}\}, \tag{44}$$

where $q = 4$, for $p = 2$, and $q = p$ otherwise. Such orbits are called *coherent states* in the physics literature [24], and as we demonstrate below they form tight frames [25] of vectors in $\mathcal{H}$. Here we will refer to these as covariant tight frames (CTF) and to $|\phi\rangle$ as the fiducial vector of the CTF.

Of importance in understanding the structure of the orbit (44) is the isotropy subgroup of the fiducial vector $|\phi\rangle$. The isotropy subgroup of $|\phi\rangle$ consists of those $T$ that merely multiply $|\phi\rangle$ by a phase,

$$T(\lambda, \mathbf{a}, \mathbf{b})|\phi\rangle = e^{i\chi(\lambda,\mathbf{a},\mathbf{b})}|\phi\rangle. \tag{45}$$

Obviously, the isotropy subgroup $H_\phi$ of $|\phi\rangle$ is at least $Z(E)$, the centre of $E$, although it may be larger. For example, the Dirac basis vector $|\mathbf{0}\rangle$ has an isotropy subgroup $H = Z(E) \cup \{D(0, \mathbf{b}) : \mathbf{b} \in A\}$. Given an isotropy subgroup $H_\phi$ we can define a corresponding isotropy subspace $\overline{H}_\phi = H_\phi/Z(E) \subseteq \overline{E}$.

An important property of $H_\phi$ is that it is Abelian and so $\overline{H}_\phi$ is isotropic. This can be seen as follows. Suppose $D(\mathbf{a}, \mathbf{b})$

and $D(\mathbf{a}',\mathbf{b}')$ are both in $H_\phi$, then

$$\begin{aligned} e^{i\chi'}e^{i\chi}|\,\phi\rangle &= D(\mathbf{a}',\mathbf{b}')D(\mathbf{a},\mathbf{b})|\,\phi\rangle \\ &= \omega^{\mathbf{a}\cdot\mathbf{b}'-\mathbf{a}'\cdot\mathbf{b}}D(\mathbf{a},\mathbf{b})D(\mathbf{a}',\mathbf{b}')|\,\phi\rangle \\ &= \omega^{\mathbf{a}\cdot\mathbf{b}'-\mathbf{a}'\cdot\mathbf{b}}e^{i\chi'}e^{i\chi}|\,\phi\rangle, \end{aligned} \tag{46}$$

for some $\chi,\chi' \in [0,2\pi)$, which implies that $\mathbf{a}\cdot\mathbf{b}'-\mathbf{a}'\cdot\mathbf{b}=0$.

Let us consider the value of the ambiguity function $\mathcal{A}_\phi$ on the isotropy subspace $\overline{H}_\phi$ of $|\,\phi\rangle$. If $(\mathbf{a},\mathbf{b}) \in \overline{H}_\phi$, then

$$\mathcal{A}_\phi(\mathbf{a},\mathbf{b}) = \langle\phi|D(\mathbf{a},\mathbf{b})|\,\phi\rangle = e^{i\chi}, \tag{47}$$

for some $\chi \in [0,2\pi)$. Thus, $\mathcal{A}_\phi$ is unimodular on $\overline{H}_\phi$. In fact, on $\overline{H}_\phi$,

$$\mathcal{A}_\phi(\mathbf{a},\mathbf{b})^p = \langle\phi|D(\mathbf{a},\mathbf{b})^p|\,\phi\rangle = \begin{cases} 1 & \text{if } p\neq 2, \\ (-1)^{\mathbf{a}\cdot\mathbf{b}} & \text{if } p=2, \end{cases} \tag{48}$$

using (10), and so for $p\neq 2$, $\mathcal{A}_\phi(\overline{H}_\phi)\subseteq\{\omega^\lambda : \lambda\in\mathbb{Z}_p\}$, while for $p=2$, $\mathcal{A}_\phi(\overline{H}_\phi)\subseteq\{i^\lambda : \lambda\in\mathbb{Z}_4\}$.

Now suppose that $\overline{H}_\phi$ is nontrivial, that is, it contains some $(\mathbf{a}',\mathbf{b}')\neq(\mathbf{0},\mathbf{0})$, and that $(\mathbf{a},\mathbf{b})\notin\overline{H}_\phi$, then

$$\begin{aligned} \mathcal{A}_\phi(\mathbf{a},\mathbf{b}) &= \langle\phi|D(\mathbf{a}',\mathbf{b}')^\dagger D(\mathbf{a},\mathbf{b})D(\mathbf{a}',\mathbf{b}')|\,\phi\rangle \\ &= \omega^{\mathbf{a}'\cdot\mathbf{b}-\mathbf{a}\cdot\mathbf{b}'}\mathcal{A}_\phi(\mathbf{a},\mathbf{b}), \end{aligned} \tag{49}$$

where we have used (8). Thus, unless $D(\mathbf{a},\mathbf{b})$ commutes with every element of $H_\phi$, $\mathcal{A}(\mathbf{a},\mathbf{b})=0$. Thus, the support of $\mathcal{A}_\phi$,

$$\operatorname{supp}\mathcal{A}_\phi \subseteq \overline{H}_\phi^\perp. \tag{50}$$

Furthermore, for all $(\mathbf{a},\mathbf{b})\in\overline{E}$, and all $(\mathbf{a}',\mathbf{b}')\in\overline{H}_\phi$, $|\mathcal{A}_\phi(\mathbf{a}+\mathbf{a}',\mathbf{b}+\mathbf{b}')| = |\mathcal{A}_\phi(\mathbf{a},\mathbf{b})|$, and so $|\mathcal{A}_\phi|$ is constant on any coset of $\overline{H}_\phi$ in $\overline{E}$.

The unimodularity of $\mathcal{A}_\phi$ on $\overline{H}_\phi$ along with Moyal's identity (34), implies that $|\overline{H}_\phi|\leq|A|$. This result can be used to infer that for any isotropic subspace $\overline{H}\subset\overline{E}$, $|\overline{H}|\leq|A|$, for if $|\overline{H}|>|A|$, then by taking $|\,\phi\rangle$ to be one of the common eigenvectors of the Abelian subgroup $H=\{D(\mathbf{a},\mathbf{b}) : (\mathbf{a},\mathbf{b})\in\overline{H}\}$, we would have $\overline{H}_\phi=\overline{H}$ and $|\overline{H}_\phi|>|A|$. Isotropic subspaces which satisfy $|\overline{H}|=|A|$ are called maximal. Such maximal isotropic subspaces are self-dual, that is, $\overline{H}^\perp=\overline{H}$. Thus, if a vector $|\,\phi\rangle\in\mathcal{H}$ has an isotropy subspace which is maximal, then $\operatorname{supp}\mathcal{A}_\phi=\overline{H}_\phi$.

Let us now go back and consider the orbit (44). The isotropy subspace of $|\,\phi\rangle$ is $\overline{H}_\phi=H_\phi/Z(E)\subset\overline{E}$ and the orbit is parameterised by the cosets $\mathcal{C}_\phi=\overline{E}/\overline{H}_\phi$. Thus, given a fiducial vector $|\,\phi\rangle$, we consider the set of vectors

$$\mathcal{F}_\phi = \{|\,\mathbf{a},\mathbf{b},\phi\rangle = D(\mathbf{a},\mathbf{b})|\,\phi\rangle : (\mathbf{a},\mathbf{b})\in\mathcal{C}_\phi\}. \tag{51}$$

We note that if the isotropy subgroup of $|\,\phi\rangle$ is $Z(E)$, then $\mathcal{F}_\phi$ will be parameterised by the whole phase space $\overline{E}$.

Following the standard coherent state theory [24], we construct the operator

$$B = \sum_{(\mathbf{a},\mathbf{b})\in\mathcal{C}_\phi} |\,\mathbf{a},\mathbf{b},\phi\rangle\langle\mathbf{a},\mathbf{b},\phi\,|. \tag{52}$$

Then, we note that

$$D(\mathbf{a},\mathbf{b})BD(\mathbf{a},\mathbf{b})^\dagger = B, \tag{53}$$

and so since $E$ is irreducible, Schur's lemma implies that $B=cI$, a multiple of the identity. Thus, if $c$ is not zero, then the set of vectors (51) forms a tight frame (CTF), with the corresponding resolution of unity given by (52), suitably normalised. In fact, taking the trace of (52) we find $c=|\mathcal{C}_\phi|/|A|$, and so we have the resolution of unity

$$I = \frac{|A|}{|\mathcal{C}_\phi|}\sum_{(\mathbf{a},\mathbf{b})\in\mathcal{C}_\phi} |\,\mathbf{a},\mathbf{b},\phi\rangle\langle\mathbf{a},\mathbf{b},\phi\,|. \tag{54}$$

We can restate this result by saying that the set of vectors $\mathcal{F}_\phi$ form a tight frame. Note that if a set of coherent states as defined by Perelomov [24, 26] forms a frame then it is known that the frame is tight, that is, it gives a resolution of unity.

Now $|\mathcal{C}_\phi| = |\overline{E}|/|\overline{H}_\phi| = |A|^2/|\overline{H}_\phi|$ and so (54) implies that $\mathcal{F}_\phi$ is a tight frame with the redundancy ratio $|\overline{H}_\phi|/|A|$. If $\overline{H}_\phi$ is maximal, then $|\mathcal{C}_\phi| = |\overline{H}_\phi| = |A|$, and so $\mathcal{F}_\phi$ is an orthonormal basis. We note that the restriction that an isotropy subspace must satisfy $|\overline{H}_\phi|\leq|A|$ corresponds to the condition that an orthonormal basis in an $|A|$-dimensional space has no more than $|A|$ elements.

We summarise the above results in the following theorem.

**Theorem 2.** *Let $|\,\phi\rangle\in\mathcal{H}$ be a normalised vector with isotropy subspace $\overline{H}_\phi\subset\overline{E}$. Then,*

(1) *$\mathcal{A}_\phi$ is unimodular on $\overline{H}_\phi$,*
(2) *$\operatorname{supp}\mathcal{A}_\phi=\overline{H}_\phi^\perp$,*
(3) *$|\mathcal{A}_\phi|$ is constant on cosets of $\overline{H}_\phi$ in $\overline{E}$,*
(4) *$\mathcal{F}_\phi$ is a tight frame with the redundancy ratio $|A|/|\overline{H}_\phi|$.*

*In particular, if $\overline{H}_\phi$ is a maximal isotropic subspace, then*

(1) *$\operatorname{supp}\mathcal{A}_\phi=\overline{H}_\phi$,*
(2) *$\mathcal{F}_\phi$ is an orthonormal basis.*

Now suppose that we have two vectors $|\,\phi\rangle, |\,\psi\rangle\in\mathcal{H}$ both with maximal isotropy subspaces $\overline{H}_\phi$ and $\overline{H}_\psi$, respectively. If the intersection $\overline{H}_\phi\cap\overline{H}_\psi$ is nontrivial, what can we say about the values of the ambiguity functions of $|\,\phi\rangle$ and $|\,\psi\rangle$ on $\overline{H}_\phi\cap\overline{H}_\psi$? We know that $|\,\phi\rangle$ and $|\,\psi\rangle$ must both be eigenvectors of any $D(\mathbf{a},\mathbf{b})$, with $(\mathbf{a},\mathbf{b})\in\overline{H}_\phi\cap\overline{H}_\psi$. Since $D(\mathbf{a},\mathbf{b})$ is unitary, this implies that unless $|\,\phi\rangle$ and $|\,\psi\rangle$ are orthogonal they must correspond to the same eigenvalue, in which case

$$\mathcal{A}_\phi(\mathbf{a},\mathbf{b}) = \mathcal{A}_\psi(\mathbf{a},\mathbf{b}), \quad \forall(\mathbf{a},\mathbf{b})\in\overline{H}_\phi\cap\overline{H}_\psi. \tag{55}$$

On the other hand, if $|\,\phi\rangle$ and $|\,\psi\rangle$ are orthogonal, then because $\mathcal{F}_\psi$ is an orthonormal basis, there will exist at least one vector $D(\widetilde{\mathbf{a}},\widetilde{\mathbf{b}})|\,\psi\rangle$, with $(\mathbf{a},\mathbf{b})\in\mathcal{C}_\psi/\{(\mathbf{0},\mathbf{0})\}$, such that $|\,\phi\rangle$ is not orthogonal to $D(\widetilde{\mathbf{a}},\widetilde{\mathbf{b}})|\,\psi\rangle$. Since $D(\widetilde{\mathbf{a}},\widetilde{\mathbf{b}})|\,\psi\rangle$ has the same isotropy subgroup as $|\,\psi\rangle$, we have the general result

$$\mathcal{A}_\phi(\mathbf{a},\mathbf{b}) = \mathcal{A}_\psi(\mathbf{a},\mathbf{b})\omega^{\widetilde{\mathbf{a}}\cdot\mathbf{b}-\mathbf{a}\cdot\widetilde{\mathbf{b}}}, \quad \forall(\mathbf{a},\mathbf{b})\in\overline{H}_\phi\cap\overline{H}_\psi, \tag{56}$$

for some fixed $(\widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}) \in \mathcal{C}_\psi$, such that $\langle \phi | D(\widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}) | \psi \rangle \neq 0$. Note that if we have alternate choices for $(\widetilde{\mathbf{a}}, \widetilde{\mathbf{b}})$, $(\widetilde{\mathbf{a}}_1, \widetilde{\mathbf{b}}_1)$, and $(\widetilde{\mathbf{a}}_2, \widetilde{\mathbf{b}}_2)$, say, then we must have $(\widetilde{\mathbf{a}}_1 - \widetilde{\mathbf{a}}_2, \widetilde{\mathbf{b}}_1 - \widetilde{\mathbf{b}}_2) \in (\overline{H}_\phi \cap \overline{H}_\psi)^\perp$.

As a consequence of Moyal's identity and (56) we also have the following theorem which relates to the inner product between the orthonormal bases associated with two fiducial vectors. Note that the delta function $\delta_{\overline{H}} : \overline{E} \to \{0, 1\}$, for any subset $\overline{H} \subset \overline{E}$, is defined by

$$\delta_{\overline{H}}(\mathbf{a}, \mathbf{b}) = \begin{cases} 1 & \text{if } (\mathbf{a}, \mathbf{b}) \in \overline{H}, \\ 0 & \text{otherwise.} \end{cases} \tag{57}$$

**Theorem 3.** *Let $|\phi\rangle$ and $|\psi\rangle \in \mathcal{H}$ have maximal isotropy subspaces $\overline{H}_\phi$ and $\overline{H}_\psi$ and let $(\mathbf{a}, \mathbf{b}) \in \mathcal{C}_\phi$ and $(\mathbf{a}', \mathbf{b}') \in \mathcal{C}_\psi$. Further, take any $(\widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}) \in \mathcal{C}_\psi$, such that $\langle \phi | \widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}, \psi \rangle \neq 0$, then the inner product $\langle \mathbf{a}, \mathbf{b}, \phi | \mathbf{a}', \mathbf{b}', \psi \rangle$ has magnitude*

$$\begin{aligned} &| \langle \mathbf{a}, \mathbf{b}, \phi | \mathbf{a}', \mathbf{b}', \psi \rangle | \\ &\quad = \sqrt{\frac{|\overline{H}_\phi \cap \overline{H}_\psi|}{|A|}} \delta_{(\overline{H}_\phi \cap \overline{H}_\psi)^\perp}(\mathbf{a}' - \mathbf{a} - \widetilde{\mathbf{a}}, \mathbf{b}' - \mathbf{b} - \widetilde{\mathbf{b}}), \end{aligned} \tag{58}$$

*and, when $|\langle \mathbf{a}, \mathbf{b}, \phi | \mathbf{a}', \mathbf{b}', \psi \rangle| \neq 0$, has phase*

$$\begin{aligned} &\frac{\langle \mathbf{a}, \mathbf{b}, \phi | \mathbf{a}', \mathbf{b}', \psi \rangle}{| \langle \mathbf{a}, \mathbf{b}, \phi | \mathbf{a}', \mathbf{b}', \psi \rangle |} \\ &\quad = \omega^{(\mathbf{a}' - \mathbf{a}) \cdot (\mathbf{b}_\phi - \mathbf{b}) - \mathbf{a}_\psi \cdot \widetilde{\mathbf{b}}} \overline{A_\phi(\mathbf{a}_\phi, \mathbf{b}_\phi)} A_\psi(\mathbf{a}_\psi, \mathbf{b}_\psi) \frac{\langle \phi | \widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}, \psi \rangle}{| \langle \phi | \widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}, \psi \rangle |}, \end{aligned} \tag{59}$$

*where $(\mathbf{a}_\phi, \mathbf{b}_\phi) \in \overline{H}_\phi$ and $(\mathbf{a}_\psi, \mathbf{b}_\psi) \in \overline{H}_\psi$ are any vectors satisfying*

$$(\mathbf{a}' - \mathbf{a} - \widetilde{\mathbf{a}}, \mathbf{b}' - \mathbf{b} - \widetilde{\mathbf{b}}) = (\mathbf{a}_\psi, \mathbf{b}_\psi) - (\mathbf{a}_\phi, \mathbf{b}_\phi). \tag{60}$$

*Proof.* Moyal's identity (33) implies

$$\begin{aligned} &| \langle \phi | D(\mathbf{a}, \mathbf{b}) | \psi \rangle |^2 \\ &\quad = \frac{1}{|A|} \sum_{(\mathbf{a}', \mathbf{b}') \in \overline{E}} \overline{\mathcal{A}_\phi(\mathbf{a}', \mathbf{b}')} \mathcal{A}_\psi(\mathbf{a}', \mathbf{b}') \omega^{\mathbf{a}' \cdot \mathbf{b} - \mathbf{a} \cdot \mathbf{b}'} \\ &\quad = \frac{1}{|A|} \sum_{(\mathbf{a}', \mathbf{b}') \in \overline{H}_\phi \cap \overline{H}_\psi} \overline{\mathcal{A}_\phi(\mathbf{a}', \mathbf{b}')} \mathcal{A}_\psi(\mathbf{a}', \mathbf{b}') \omega^{\mathbf{a}' \cdot \mathbf{b} - \mathbf{a} \cdot \mathbf{b}'} \\ &\quad = \frac{1}{|A|} \sum_{(\mathbf{a}', \mathbf{b}') \in \overline{H}_\phi \cap \overline{H}_\psi} \omega^{\mathbf{a}' \cdot (\mathbf{b} - \widetilde{\mathbf{b}}) - (\mathbf{a} - \widetilde{\mathbf{a}}) \cdot \mathbf{b}'} \\ &\quad = \frac{|\overline{H}_\phi \cap \overline{H}_\psi|}{|A|} \delta_{(\overline{H}_\phi \cap \overline{H}_\psi)^\perp}(\mathbf{a} - \widetilde{\mathbf{a}}, \mathbf{b} - \widetilde{\mathbf{b}}), \end{aligned} \tag{61}$$

for any $(\widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}) \in \mathcal{C}_\psi$, such that $\langle \phi | D(\widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}) | \psi \rangle \neq 0$. Here we have used (56) and the fact that $\mathcal{A}_\phi$ is unimodular on $\overline{H}_\phi$. Thus, since $|\langle \mathbf{a}, \mathbf{b}, \phi | \mathbf{a}', \mathbf{b}', \psi \rangle| = |\langle \phi | D(\mathbf{a}' - \mathbf{a}, \mathbf{b}' - \mathbf{b}) | \psi \rangle|$, we obtain (58).

The second part of the proof follows by first noting that $(\overline{H}_\phi \cap \overline{H}_\psi)^\perp$ is the smallest subspace of $\overline{E}$ containing $\overline{H}_\phi \cup \overline{H}_\psi$. Thus, any $(\mathbf{a}, \mathbf{b})$ for which $\langle \phi | D(\mathbf{a}, \mathbf{b}) | \psi \rangle \neq 0$ can be decomposed as (60). This decomposition is not generally unique as any element of $\overline{H}_\phi \cap \overline{H}_\psi$ can be added to both $(\mathbf{a}_\psi, \mathbf{b}_\psi)$ and $(\mathbf{a}_\phi, \mathbf{b}_\phi)$. We then have

$$\begin{aligned} &\langle \phi | D(\mathbf{a} - \mathbf{a}', \mathbf{b} - \mathbf{b}') | \psi \rangle \\ &\quad = \omega^{(\widetilde{\mathbf{b}} - \mathbf{b} + \mathbf{b}) \cdot \widetilde{\mathbf{a}}} \langle \phi | D(\mathbf{a}_\psi - \mathbf{a}_\phi, \mathbf{b}_\psi - \mathbf{b}_\phi) | \widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}, \psi \rangle \\ &\quad = \omega^{(\mathbf{a}' - \mathbf{a} - \widetilde{\mathbf{a}}) \cdot \mathbf{b}_\phi - (\mathbf{b}' - \mathbf{b} - \widetilde{\mathbf{b}}) \cdot \widetilde{\mathbf{a}}} \langle \phi | D(\mathbf{a}_\phi, \mathbf{b}_\phi)^\dagger D(\mathbf{a}_\psi, \mathbf{b}_\psi) | \widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}, \psi \rangle \\ &\quad = \omega^{(\mathbf{a}' - \mathbf{a}) \cdot \mathbf{b}_\phi - \mathbf{a}_\psi \cdot \widetilde{\mathbf{b}}} \overline{A_\phi(\mathbf{a}_\phi, \mathbf{b}_\phi)} A_\psi(\mathbf{a}_\psi, \mathbf{b}_\psi) \langle \phi | \widetilde{\mathbf{a}}, \widetilde{\mathbf{b}}, \psi \rangle. \end{aligned} \tag{62}$$

The result (59) then follows using (58). □

We will say that two maximal isotropic subspaces $\overline{H}_\phi$ and $\overline{H}_\psi$ are disjoint if $\overline{H}_\phi \cap \overline{H}_\psi = \{(\mathbf{0}, \mathbf{0})\}$. We have the following corollary of Theorem 3 which relates to the "angle" between the orthonormal bases associated with two fiducial vectors having *disjoint* maximal isotropy subspaces. This follows from Theorem 3 by noting that if $\overline{H}_\phi$ and $\overline{H}_\psi$ are disjoint, then $(\overline{H}_\phi \cap \overline{H}_\psi)^\perp = \overline{E}$.

**Corollary 1.** *Let $|\phi\rangle$ and $|\psi\rangle \in \mathcal{H}$ have maximal isotropic isotropy subspaces $\overline{H}_\phi$ and $\overline{H}_\psi$ which are disjoint, then*

$$| \langle \mathbf{a}, \mathbf{b}, \phi | \mathbf{a}', \mathbf{b}', \psi \rangle | = \frac{1}{\sqrt{|A|}}, \tag{63}$$

*for all $(\mathbf{a}, \mathbf{b}) \in \mathcal{C}_\phi$ and $(\mathbf{a}', \mathbf{b}') \in \mathcal{C}_\psi$.*

An example of two disjoint maximal isotropic subspaces is $\overline{H}_D = \{(\mathbf{0}, \mathbf{b}) : \mathbf{b} \in A\}$ and $\overline{H}_F = \{(\mathbf{a}, \mathbf{0}) : \mathbf{a} \in A\}$. $\overline{H}_D$ has the CTF given by the orthonormal basis (1) and can be associated with fiducial vector $|\mathbf{0}\rangle$, while $\overline{H}_F$ has the CTF given by the orthonormal basis (4) with fiducial vector $|\hat{\mathbf{0}}\rangle$.

## 6. SYMPLECTIC TRANSFORMATIONS AND PHASE SPACE COVERINGS

The question arises as to whether it is possible to choose a set of vectors (waveforms) such that the supports of their ambiguity functions are nonintersecting (except at $(\mathbf{0}, \mathbf{0})$), while jointly covering the whole of phase space. This is equivalent to covering the whole of the phase space $\overline{E}$ with disjoint maximal isotropic subspaces. At least in certain instances the answer is yes. The construction in these cases works as follows [15].

We begin by considering the symplectic transformations on $\overline{E}$. Such transformations take the form

$$(\mathbf{a}, \mathbf{b}) \longrightarrow (\mathbf{A}\mathbf{a} + \mathbf{B}\mathbf{b}, \mathbf{C}\mathbf{a} + \mathbf{D}\mathbf{b}) \tag{64}$$

which preserve the symplectic inner product (13). Here $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, and $\mathbf{D}$ are matrices over $\mathbb{Z}_p$. We can write the condition that (13) be preserved in terms of block matrices as

$$\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{pmatrix}^T \begin{pmatrix} \mathbf{0} & \mathbf{I} \\ -\mathbf{I} & \mathbf{0} \end{pmatrix} \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{pmatrix} = \begin{pmatrix} \mathbf{0} & \mathbf{I} \\ -\mathbf{I} & \mathbf{0} \end{pmatrix}, \tag{65}$$

where $\mathbf{I}$ is the $m \times m$ identity matrix on $\mathbb{Z}_p$. The matrices $\left(\begin{smallmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{smallmatrix}\right)$ satisfying (65) form the symplectic group $\mathrm{Sp}(2m, \mathbb{Z}_p)$. For our purposes the importance of symplectic transformations on $\overline{E}$ lies in the fact that they map maximal isotropic subspaces to maximal isotropic subspaces.

Some interesting subgroups of $\mathrm{Sp}(2m, \mathbb{Z}_p)$ are

$$\left\{ \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{A}^{-T} \end{pmatrix} : \mathbf{A} \in \mathrm{GL}\,(m, \mathbb{Z}_p) \right\}, \tag{66}$$

where $\mathrm{GL}(m, \mathbb{Z}_p)$ is the general linear group of $m$-dimensional invertible matrices over $\mathbb{Z}_p$,

$$\left\{ \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{P} & \mathbf{I} \end{pmatrix} : \mathbf{P} \text{ a symmetric matrix over } \mathbb{Z}_p \right\}, \tag{67}$$

$$\left\{ \begin{pmatrix} \mathbf{I} & \mathbf{P} \\ \mathbf{0} & \mathbf{I} \end{pmatrix} : \mathbf{P} \text{ a symmetric matrix over } \mathbb{Z}_p \right\}. \tag{68}$$

The symplectic transformations allow us to transform between maximal isotropic subspaces of $\overline{E}$. Now as we have seen, each maximal isotropic subspace of $\overline{E}$ corresponds to a maximal Abelian subgroup of $E$ and an orthonormal basis for $\mathcal{H}$. Thus given a symplectic map on $\overline{E}$ which maps between subspaces, we need to find unitary operators on $\mathcal{H}$ which map between the corresponding subgroups by conjugation. We now give some examples which we will use to generate phase space coverings.

The Fourier transform operator $F$ given in (5) transforms $D(\mathbf{a}, \mathbf{b})$ as

$$F^\dagger D(\mathbf{a}, \mathbf{b}) F = \omega^{-\mathbf{a}\cdot\mathbf{b}} D(\mathbf{b}, -\mathbf{a}). \tag{69}$$

Thus, $F$ induces a symplectic action on the phase space given by $f : \overline{E} \to \overline{E}$, such that $f(\mathbf{a}, \mathbf{b}) = (\mathbf{b}, -\mathbf{a})$, corresponding to the element

$$\begin{pmatrix} \mathbf{0} & \mathbf{I} \\ -\mathbf{I} & \mathbf{0} \end{pmatrix} \in \mathrm{Sp}\,(2m, \mathbb{Z}_p). \tag{70}$$

This action exchanges the maximal isotropic subspaces $\overline{H}_D = \{(\mathbf{0}, \mathbf{b}) : \mathbf{b} \in A\}$ and $\overline{H}_F = \{(\mathbf{a}, \mathbf{0}) : \mathbf{a} \in A\}$.

For the moment we will assume that $p \neq 2$. The case $p = 2$ will be considered below. Define a unitary transformation on $\mathcal{H}$ by

$$W(\mathbf{P}) = \sum_{\mathbf{c}\in A} \overline{\omega}^{\mathbf{c}\cdot\mathbf{P}\mathbf{c}}\, |\, \mathbf{c}\rangle\langle \mathbf{c}\,|, \tag{71}$$

where $\mathbf{P}$ is a symmetric matrix on $\mathbb{Z}_p$. We have

$$W(\mathbf{P})^\dagger D(\mathbf{a}, \mathbf{b}) W(\mathbf{P}) = \omega^{\mathbf{a}\cdot\mathbf{P}\mathbf{a}} D(\mathbf{a}, \mathbf{b} + 2\mathbf{P}\mathbf{a}). \tag{72}$$

$W(\mathbf{P})$ induces a symplectic action on the phase space $w_\mathbf{P} : \overline{E} \to \overline{E}$, such that $w_\mathbf{P}(\mathbf{a}, \mathbf{b}) = (\mathbf{a}, \mathbf{b}+2\mathbf{P}\mathbf{a})$. These unitary transformations on $\mathcal{H}$ form a representation of the subgroup (67) of $\mathrm{Sp}(2m, \mathbb{Z}_p)$, which can be seen by making the change of parameterization $\mathbf{P} \to (p+1)\mathbf{P}/2$.

The scheme for constructing phase space coverings then proceeds as follows. Use the operators $W(\mathbf{P})$ to generate new maximal isotropic subspaces $\overline{H}_\mathbf{P}$ as

$$\overline{H}_\mathbf{P} = w_\mathbf{P}(\overline{H}_F) = \{(\mathbf{a}, 2\mathbf{P}\mathbf{a}) : \mathbf{a} \in A\}. \tag{73}$$

Two such subspaces corresponding to symmetric matrices $\mathbf{P}$ and $\mathbf{Q}$ will intersect only at solutions of $(\mathbf{P} - \mathbf{Q})\mathbf{a} = \mathbf{0}$. Thus, the problem of covering $\overline{E}$ with disjoint maximal isotropic subspaces will be solved if we can find a set of $|A| - 1$ nonsingular symmetric matrices $\mathcal{P}$, over $\mathbb{Z}_p$, such that for any pair of matrices $\mathbf{P}, \mathbf{Q} \in \mathcal{P}$, $\mathbf{P} - \mathbf{Q}$ is nonsingular. The covering would then be

$$\overline{E} = \overline{H}_D \cup \overline{H}_F \cup \left( \bigcup_{\mathbf{P}\in\mathcal{P}} w_P(\overline{H}_F) \right). \tag{74}$$

When this occurs the set of vectors

$$\{|\,\mathbf{a}\rangle : \mathbf{a} \in A\} \cup \{|\,\hat{\mathbf{b}}\rangle : \mathbf{b} \in A\} \cup \{W(\mathbf{P})|\,\hat{\mathbf{b}}\rangle : \mathbf{b} \in A,\ \mathbf{P} \in \mathcal{P}\} \tag{75}$$

is such that the magnitude of the inner product of any distinct pair of vectors in the set is either 0 or $1/\sqrt{|A|}$.

If $p = 2$ the construction of operators which perform the function of the $W(\mathbf{P})$s above is somewhat different. In this case we define the operator

$$W_2(\mathbf{P}) = \sum_{\mathbf{c}\in A} i^{\mathbf{c}\cdot\mathbf{P}\mathbf{c}} |\,\mathbf{c}\rangle\langle \mathbf{c}\,|. \tag{76}$$

Here the subtlety is that the quadratic form $T_\mathbf{P}(\mathbf{a}) = \mathbf{c}\cdot\mathbf{P}\mathbf{c}$ is to be interpreted as a $\mathbb{Z}_4$-valued quadratic form. A map $T_\mathbf{P} : \mathbb{Z}_2^m \to \mathbb{Z}_4$ is called a $\mathbb{Z}_4$-valued quadratic form if it satisfies

$$T_\mathbf{P}(\mathbf{a} + \mathbf{a}') = T_\mathbf{P}(\mathbf{a}) + T_\mathbf{P}(\mathbf{a}') + 2\mathbf{a}\cdot P\mathbf{a}', \tag{77}$$

for all $\mathbf{a}, \mathbf{a}' \in \mathbb{Z}_2^m$ [27]. Operationally one just interprets the element of $\mathbf{a}$ and $\mathbf{P}$ to be in $\mathbb{Z}_4$ and computes the result $\mathbf{a}\cdot\mathbf{P}\mathbf{a}$ in $\mathbb{Z}_4$. In this case

$$W_2(\mathbf{P})^\dagger D(\mathbf{a}, \mathbf{b}) W_2(\mathbf{P}) = i^{-\mathbf{a}\cdot\mathbf{P}\mathbf{a}} D(\mathbf{a}, \mathbf{b} + \mathbf{P}\mathbf{a}), \tag{78}$$

and the construction follows the $p \neq 2$ case with $W_2(\mathbf{P})$ replacing $W(\mathbf{P})$.

We discuss two cases in which such a covering can be constructed.

## 7. DISCRETE RADAR REVISITED

We return to the theory of discrete radar as summarised in Section 3. Since $m = 1$ in this case, the matrices in $\mathcal{P}$ are just numbers. In fact, since $p$ is prime, we can take $\mathcal{P} = \{0, 1, \ldots, p-1\}$. The $p+1$ maximal isotropic subspaces consist of the line $\{(0, \tau) : \tau \in \{0, \ldots, p-1\}\}$ along with the lines $\{(\tau, 2n\tau) : \tau \in \{0, \ldots, p-1\}\}$, for $n \in \mathcal{P}$, in the phase space or time-frequency plane. This time-frequency plane covering is displayed in Figure 1, for $p = 11$. Note that the matrix that results from stripping off the all-zero column and all-one row of this figure is a Latin square. In general, the matrices obtained from the different coverings of the time-frequency plane form a set of pairwise orthogonal Latin squares. These find application in cellular systems that employ orthogonal frequency-division multiplexing (OFDM). Each base station has its own hopping matrix (Latin square). There will be exactly one time/subcarrier collision for every pair of virtual

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 11 | 6 | 8 | 9 | 3 | 10 | 4 | 5 | 7 | 2 |
| 0 | 10 | 11 | 4 | 6 | 5 | 8 | 7 | 9 | 2 | 3 |
| 0 | 9 | 5 | 11 | 3 | 7 | 6 | 10 | 2 | 8 | 4 |
| 0 | 8 | 10 | 7 | 11 | 9 | 4 | 2 | 6 | 3 | 5 |
| 0 | 7 | 4 | 3 | 8 | 11 | 2 | 5 | 10 | 9 | 6 |
| 0 | 6 | 9 | 10 | 5 | 2 | 11 | 8 | 3 | 4 | 7 |
| 0 | 5 | 3 | 6 | 2 | 4 | 9 | 11 | 7 | 10 | 8 |
| 0 | 4 | 8 | 2 | 10 | 6 | 7 | 3 | 11 | 5 | 9 |
| 0 | 3 | 2 | 9 | 7 | 8 | 5 | 6 | 4 | 11 | 10 |
| 0 | 2 | 7 | 5 | 4 | 10 | 3 | 9 | 8 | 6 | 11 |
| ⋆ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

$\nu$ (rows) / $\tau$ (columns)

Figure 1: Tiling of the time-frequency plane by maximal isotropic subspaces for $p = 11$.

channels of two base stations that employ these hopping patterns. See for example [28]. In the radar context such frequency coded waveforms are called Costas coded waveforms [29].

The vectors (waveforms) corresponding to the above maximal isotropic subspaces are, for $n \in \mathcal{P}$,

$$|n, \hat{\nu}\rangle = W(n)|\hat{\nu}\rangle = \sqrt{\frac{i}{p}} \sum_{\tau=0}^{p-1} \overline{\omega}^{n\tau^2} \omega^{\nu\tau} |\tau\rangle, \tag{79}$$

for $\nu \in \{0, \ldots, p-1\}$. These are linear frequency-modulated sinusoid or chirps. The ambiguity function of such a chirped waveform $|n, \hat{\nu}\rangle$ is

$$\mathcal{A}_{n,\hat{\nu}}(\tau, \nu') = \overline{\omega}^{n\tau^2} \omega^{\tau\nu} \mathcal{A}_{\hat{\mathbf{0}}}(\tau, \nu' + 2n\tau), \tag{80}$$

for all $(\tau, \nu') \in \mathbb{Z}_p$, where $\mathcal{A}_{\hat{\mathbf{0}}}$ is the ambiguity function of the waveform $|\hat{\mathbf{0}}\rangle$. Thus, the magnitude of the ambiguity (80) is

$$\left|\mathcal{A}_{n,\hat{\nu}}(\tau, \nu')\right| = \left|\mathcal{A}_{\hat{\mathbf{0}}}(\tau, \nu' + 2n\tau)\right| = \delta_{\nu'+2n\tau,0}, \tag{81}$$

for all $(\tau, \nu') \in \mathbb{Z}_p$. We can explicitly see how the waveforms $\{|n, \hat{\nu}\rangle : n \in \mathcal{P},\ \nu \in \{0, \ldots, p-1\}\}$ along with the Dirac basis waveform $\{|\tau\rangle : \tau \in \{0, \ldots, p-1\}\}$ have ambiguity functions which disjointly cover the time-frequency plane. Such sets of waveforms, which have ambiguity functions that cross only at a single point, are of great utility in the operation of adaptive radars. In this context sequences of waveforms are chosen adaptively to obtain optimal results over time.

## 8. $\mathbb{Z}_4$-KERDOCK CODES

Kerdock codes [14, 30] are nonlinear binary error-correcting codes which contain more codewords for a given minimum distance than any linear code. It was shown by Hammons et al. [31] that the Kerdock codes could be constructed as binary images under the Gray map of linear codes over $\mathbb{Z}_4$. The geometry of these codes was studied extensively by Calderbank et al. [15] who demonstrated their relationship to the *extraspecial 2-group*. This group is identical to the finite Heisenberg-Weyl group (11) for $p = 2$, and most of the theory developed in Section 5 can be found in [15] for this case. Note that the different othonormal bases appear as mutually unbiased bases in the theory of quantum measurement [32] for $A = \mathbb{Z}_p$.

Here the configuration space $A = \mathbb{Z}_2^m$ consists of the binary sequences of length $m$. This case has been studied extensively in the theory of error correction codes [15]. The Fourier basis is

$$|\hat{\mathbf{b}}\rangle = \left(\frac{i}{2}\right)^{m/2} \sum_{(\mathbf{a},\mathbf{b})\in\overline{E}} (-1)^{\mathbf{b}\cdot\mathbf{a}} |\mathbf{a}\rangle. \tag{82}$$

Apart from the normalising constant $(i/2)^{m/2}$, the coefficients of the Fourier basis are related to the first-order Reed-Muller code $\mathrm{RM}(1, m+1)$, in the following sense. If we apply group $E$, from (11), to the vector $|\hat{\mathbf{0}}\rangle$ we obtain the set of vectors

$$\{i^\lambda |\hat{\mathbf{b}}\rangle : \lambda \in \mathbb{Z}_4,\ \mathbf{b} \in A\}. \tag{83}$$

In the Dirac basis, neglecting the common normalisation factor $(i/2)^{m/2}$, the coefficients of these vectors form $\mathrm{RM}(1, m+1)$ as a linear code of length $2^m$ over $\mathbb{Z}_4$. If we then apply the Gray map,

$$\{1 \longrightarrow 00, i \longrightarrow 01, (-1) \longrightarrow 11, (-i) \longrightarrow 10\}, \tag{84}$$

we then obtain the conventional form of $\mathrm{RM}(1, m+1)$ as a binary code of length $2^{m+1}$. In a similar way the second-order Reed-Muller code $\mathrm{RM}(2, m+1)$ corresponds to the set of vectors

$$\{i^\lambda W_2(\mathbf{P})|\hat{\mathbf{b}}\rangle : \lambda \in \mathbb{Z}_4,\ \mathbf{b} \in A,\ \mathbf{P} \text{ a binary symmetric matrix}\}. \tag{85}$$

In this case there are many possible sets of binary symmetric matrices $\mathcal{P}$ which lead to a disjoint covering of the phase space with maximal isotropic subspaces [15]. Such sets are referred to as Kerdock sets in this context. One possibility consists of a vector space of nonsingular Hankel matrices, with one binary symmetric matrix with any given diagonal. Sets of vectors of the form

$$\{i^\lambda W_2(\mathbf{P})|\hat{\mathbf{b}}\rangle : \lambda \in \mathbb{Z}_4,\ \mathbf{b} \in A,\ \mathbf{P} \in \mathcal{P}\} \cup \{|\mathbf{a}\rangle,\ \mathbf{a} \in A\} \tag{86}$$

are the Kerdock codes. Note that here the zero matrix is in $\mathcal{P}$ and that $W(0) = I$. Obviously, this set lies within the second-order Reed-Muller code (85).

Let us consider the Gray map in a little more detail. This map takes $\mathbb{Z}_4$-valued quadratic forms $T_{\mathbf{P}}$ on $\mathbb{Z}_2^m$ to quadratic forms on $\mathbb{Z}_2^{m+1}$. If $Q_{\mathbf{M}}$ is a quadratic form on $\mathbb{Z}_2^{m+1}$ for which the associated bilinear form is $\mathbf{u} \cdot \mathbf{M}\mathbf{v}$ then by definition

$$Q_{\mathbf{M}}(\mathbf{u} + \mathbf{v}) = Q_{\mathbf{M}}(\mathbf{u}) + Q_{\mathbf{M}}(\mathbf{v}) + \mathbf{u} \cdot \mathbf{M}\mathbf{v}, \tag{87}$$

for all $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^{m+1}$. Calderbank et al. [15] show that there exists a bijection between $m \times m$ binary symmetric matrices $\mathbf{P}$ and $(m+1) \times (m+1)$ skew-symmetric matrices $\mathbf{M}$ given by

$$\mathbf{M} = \begin{pmatrix} 0 & d_{\mathbf{P}} \\ d_{\mathbf{P}}^T & d_{\mathbf{P}}^T d_{\mathbf{P}} + \mathbf{P} \end{pmatrix}, \tag{88}$$

where $d_{\mathbf{P}}$ is a row vector consisting of the diagonal of the matrix $\mathbf{P}$. Now the code words within the coset of RM$(1, m+1)$ in RM$(2, m+1)$, corresponding to $\mathbf{P}$, are from (85),

$$\left\{\left(i^{\mathbf{a}\cdot\mathbf{P}\mathbf{a}+2\mathbf{b}\cdot\mathbf{a}+\lambda} : \mathbf{a}\in\mathbb{Z}_2^m\right) : \lambda\in\mathbb{Z}_4,\ \mathbf{b}\in\mathbb{Z}_2^m\right\}. \tag{89}$$

If $\mathbf{M}$ is the skew-symmetric matrix corresponding to $\mathbf{P}$ through (88) and we write $\mathbf{M} = \mathbf{U}_{\mathbf{M}} + \mathbf{U}_{\mathbf{M}}^T$, where $\mathbf{U}_{\mathbf{M}}$ is upper triangular, then the $\mathbb{Z}_2$ representation of the set of code words (89) is

$$\left\{\left((-1)^{\mathbf{v}\cdot\mathbf{U}_{\mathbf{M}}\mathbf{v}+\mathbf{u}\cdot\mathbf{v}} : \mathbf{v}\in\mathbb{Z}_2^{m+1}\right) : \mathbf{u}\in\mathbb{Z}_2^{m+1}\right\}. \tag{90}$$

The case $m = 3$ provides an illustrative example. For this case, a phase space covering is defined by the vector space of matrices $\mathcal{K}$ spanned by

$$\mathbf{P}_{001} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \mathbf{P}_{010} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \qquad \mathbf{P}_{100} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{91}$$

Each matrix in the space is specified uniquely by its diagonal. The skew-symmetric matrix corresponding to $\mathbf{P}_{100}$, say, is

$$\mathbf{M}_{100} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{92}$$

One of the quadratic forms associated with $\mathbf{M}_{010}$ is

$$Q_{100}(\mathbf{v}) = \mathbf{v}\cdot\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}\mathbf{v} = v_1v_2 + v_2v_3 + v_3v_4. \tag{93}$$

This particular quadratic form is interesting in that the code words (90) are the Welti sequences [11]. The Welti sequences occur in Golay complementary pairs, as defined in the next section. This connection between Golay complementary pairs and the Kerdock sets has been mentioned in a paper by Davis and Jedwab [33]. We will consider this connection in more detail below.

## 9. GOLAY COMPLEMENTARY PAIRS AND KERDOCK SETS

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

$$\mathrm{corr}_k(\mathbf{x}) + \mathrm{corr}_k(\mathbf{y}) = 2N\delta_{k,0}, \tag{94}$$

for $k = -(N-1), \ldots, (N-1)$. Such sequences have an extensive literature, samples of which are [11–13, 33–37].

The Welti sequences take values in $\{1, -1\}$, and can be written in the form (cf. (90))

$$\left\{\left((-1)^{\mathbf{v}\cdot\mathbf{U}_W\mathbf{v}+\mathbf{u}\cdot\mathbf{v}} : \mathbf{v}\in\mathbb{Z}_2^{m+1}\right) : \mathbf{u}\in\mathbb{Z}_2^{m+1}\right\} \tag{95}$$

for each $m$, where the upper triangular $\mathbf{U}_W$ takes the form

$$\left[\mathbf{U}_W\right]_{i,j} = \delta_{i+1,j}, \quad i, j = 1, \ldots, m+1, \tag{96}$$

corresponding to the binary skew-symmetric matrix $M$, with

$$\left[\mathbf{M}_W\right]_{i,j} = \delta_{i+1,j} + \delta_{i,j+1}, \quad i, j = 1, \ldots, m+1. \tag{97}$$

Each sequence in the set (95) has at least one Golay complementary partner in the set. For each value of $m$ the set (95) corresponds via the Gray map to the maximal isotropic subspace corresponding to the matrix $\mathbf{P}_{1000\cdots0}$, with elements

$$\left[\mathbf{P}_{1000\cdots0}\right]_{i,j} = \delta_{i,1}\delta_{j,1} + \delta_{i,j+1} + \delta_{i+1,j}, \quad i, j = 1, \ldots, m. \tag{98}$$

The Budisin sequences [36] correspond to the permutations of the skew-symmetric matrix $\mathbf{M}_W$ given in (97). That is, denoting by $\mathcal{S}_{m+1}$ the group of $(m+1)\times(m+1)$ permutation matrices, we obtain a set of complementary sequences

$$\left\{\left((-1)^{\mathbf{v}\cdot(\mathbf{S}\mathbf{U}_W\mathbf{S}^T)\mathbf{v}+\mathbf{u}\cdot\mathbf{v}} : \mathbf{v}\in\mathbb{Z}_2^{m+1}\right) : \mathbf{u}\in\mathbb{Z}_2^{m+1}\right\}, \tag{99}$$

corresponding to the binary skew-symmetric matrix

$$\mathbf{M}_{\mathbf{S}} = \mathbf{S}\mathbf{M}_W\mathbf{S}^T, \tag{100}$$

for each $\mathbf{S}\in\mathcal{S}$. As with the Welti sequences, each sequence in the set (99) has at least one Golay complementary partner in the set. Not all of the matrices $\mathbf{M}_{\mathbf{S}}$ in (100) are different. In particular, the permutation matrix $\mathbf{S}_0\in\mathcal{S}_{m+1}$, given by

$$\left[\mathbf{S}_0\right]_{ij} = \delta_{i,m+2-j}, \quad i, j = 1, \ldots, 2^{m+1}, \tag{101}$$

leaves $\mathbf{M}_W$ invariant.

Now as the matrix $\mathbf{M}$ traverses the orbit

$$\left\{\mathbf{S}\mathbf{M}_W\mathbf{S}^T : \mathbf{S}\in\mathcal{S}_{m+1}\right\} \tag{102}$$

the corresponding $m\times m$ binary symmetric $\mathbf{P}$, according to the map (88), traces out some orbit in the space of binary symmetric matrices. For example, for $m = 3$, the orbit (103) has length 12 due to the invariance of $\mathbf{M}_W \equiv \mathbf{M}_{100}$, under the permutation $\mathbf{S}_0$. In this case, the orbit under $\mathcal{S}_4$,

$$\left\{\mathbf{S}\mathbf{M}_{100}\mathbf{S}^T : \mathbf{S}\in\mathcal{S}_4\right\}, \tag{103}$$

corresponds to the orbit in the space of binary symmetric matrices

$$\left\{\mathbf{S}\mathbf{P}_{100}\mathbf{S}^T : \mathbf{S}\in\mathcal{S}_3\right\} \cup \left\{\mathbf{S}\mathbf{P}_{011}\mathbf{S}^T : \mathbf{S}\in\mathcal{S}_3\right\}, \tag{104}$$

which is equivalent to

$$\left\{\mathbf{S}\mathbf{P}_{100}\mathbf{S}^T : \mathbf{S}\in\mathcal{S}_3\right\} \cup \left\{\mathbf{S}\mathbf{P}_{100}{}^{-1}\mathbf{S}^T : \mathbf{S}\in\mathcal{S}_3\right\}, \tag{105}$$

where $\mathbf{P}_{100}, \mathbf{P}_{011}\in\mathcal{K}$ are given by (91).

Finally, we make the intriguing observation that for $m = 3$, the complex sequences

$$\left\{\left(i^{\mathbf{a}\cdot\mathbf{P}\mathbf{a}+2\mathbf{b}\cdot\mathbf{a}+\lambda} : \mathbf{a} \in \mathbb{Z}_2^3\right) : \lambda \in \mathbb{Z}_4,\ \mathbf{b} \in \mathbb{Z}_2^3\right\} \tag{106}$$

are complex Golay complementary sequences for binary symmetric matrices $\mathbf{P}$ in the union of the cosets of the subspace of diagonal binary matrices with coset representatives given by the Kerdock matrices $\mathbf{P}_{100}$, $\mathbf{P}_{011}$, and $\mathbf{P}_{111}$. The other cosets do not contain any Golay complementary pairs.

## 10. CONCLUSION

The finite Heisenberg-Weyl groups provide a unifying mathematical structure, which has a useful part to play in radar theory and in communications. Many of the unimodular sequences used for spreading sequences in communications, and proposed as waveforms in radar, are related to its maximal Abelian subgroups. This mathematical structure for $A = \mathbb{Z}_2^m$ has already been used in the construction of stabiliser codes for quantum error correction [38] and in the construction of the Kerdock codes over $\mathbb{Z}_4$ [15, 31], and for $A = \mathbb{Z}_k$, in the construction of symmetric informationally complete positive operator values measures (equiangular lines) [17] in quantum information theory.

For mathematical convenience and clarity in this paper, we restricted the configuration space to be $A = \mathbb{Z}_p^m$, with $p$ prime. However, most of the results reported in this paper follow more generally. In particular, all of the major results of Sections 2–6 follow with relatively minor modifications if $A$ is a vector space over a finite field. If $A$ is not a vector space then Sections 2–5 follow in terms of subgroups and annihilators rather than subspaces and symplectic duals.

One particularly intriguing aspect of the Kerdock set is its relationship to the Welti and Budisin sequences, which comprise sequences which are Golay complementary pairs. The relationship of these sequences to the finite Heisenberg-Weyl groups provides a new tool for studying the origin of their special properties.

## ACKNOWLEDGMENTS

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. A summary of the results in this paper was presented at the 2005 IEEE Conference on Acoustics, Speech, and Signal Processing, Philadelphia, Pa.

## REFERENCES

[1] G. B. Folland, *Harmonic Analysis in Phase Space*, Princeton University Press, Princeton, NJ, USA, 1989.

[2] W. Miller, "Topics in harmonic analysis with applications to radar and sonar," in *Radar and Sonar, Part I*, R. Blahut, W. Miller, and C. Wilcox, Eds., IMA Volumes in Mathematics and Its Applications, Springer, New York, NY, USA, 1991.

[3] L. Auslander and R. Tolimieri, "Radar ambiguity functions and group theory," *SIAM Journal on Mathematical Analysis*, vol. 16, no. 3, pp. 577–601, 1985.

[4] G. W. Mackey, "Some remarks on symplectic automorphisms," *Proceedings of the American Mathematical Society*, vol. 16, pp. 393–397, 1965.

[5] I. E. Segal, "Transforms for operators and symplectic automorphisms over a locally compact abelian group," *Mathematica Scandinavica*, vol. 13, pp. 31–43, 1963.

[6] A. Weil, "Sur certains groupes d'opérateurs unitaires," *Acta Mathematica*, vol. 111, pp. 143–211, 1964.

[7] M. S. Richman, T. W. Parks, and R. G. Shenoy, "Discrete-time, discrete-frequency, time-frequency analysis," *IEEE Transactions on Signal Processing*, vol. 46, no. 6, pp. 1517–1527, 1998.

[8] R. Tolimieri and M. An, *Time-Frequency Representations*, Birkhäuser Boston, Boston, Mass, USA, 1998.

[9] G. E. Bottomley, "Signature sequence selection in a CDMA system with orthogonal coding," *IEEE Transactions on Vehicular Technology*, vol. 42, no. 1, pp. 62–68, 1993.

[10] K. Yang, Y.-K. Kim, and P. Vijay Kumar, "Quasi-orthogonal sequences for code-division multiple-access systems," *IEEE Transactions on Information Theory*, vol. 46, no. 3, pp. 982–993, 2000.

[11] G. Welti, "Quaternary codes for pulsed radar," *IEEE Transactions on Information Theory*, vol. 6, no. 3, pp. 400–408, 1960.

[12] M. Golay, "Complementary series," *IEEE Transactions on Information Theory*, vol. 7, no. 2, pp. 82–87, 1961.

[13] S. Z. Budisin, B. M. Popovic, and I. M. Indjin, "Designing radar signals using complementary sequences," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 21, no. 2, pp. 170–179, 1985.

[14] F. J. Macwilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland Elsevier, Amsterdam, The Netherlands, 1983.

[15] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel, "$\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal euclidean line-sets," *Proceedings of the London Mathematical Society*, vol. 75, no. 2, pp. 436–480, 1997.

[16] H. Reiter, *Classical Harmonic Analysis and Locally Compact Groups*, Oxford University Press, London, UK, 1968.

[17] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, "Symmetric informationally complete quantum measurements," *Journal of Mathematical Physics*, vol. 45, no. 6, pp. 2171–2180, 2004.

[18] C. H. Wilcox, "The synthesis problem for radar ambiguity functions," in *Radar and Sonar, Part I*, vol. 32 of *IMA Series in Mathematics and Its Applications*, pp. 229–260, Springer, New York, NY, USA, 1991.

[19] H. G. Feichtinger and W. Kozek, "Quantization of TF lattice-invariant operators on elementary LCA groups," in *Gabor Analysis and Algorithms: Theory and Applications*, H. G. Feichtinger and T. Strohmer, Eds., Applied and Numerical Harmonic Analysis, chapter 7, pp. 233–266, Birkhäuser, Boston, Mass, USA, 1998.

[20] P. Delsarte, J. M. Goethals, and J. J. Seidel, "Bounds for systems of lines and Jacobi polynomials," *Philips Research Reports*, vol. 30, no. 3, pp. 91–105, 1975.

[21] P. W. H. Lemmens and J. J. Seidel, "Equiangular lines," *Journal of Algebra*, vol. 24, no. 3, pp. 494–512, 1973.

[22] S. G. Hoggar, "64 lines from a quaternionic polytope," *Geometriae Dedicata*, vol. 69, no. 3, pp. 287–289, 1998.

[23] T. Strohmer and R. W. Heath Jr., "Grassmannian frames with applications to coding and communication," *Applied and Computational Harmonic Analysis*, vol. 14, no. 3, pp. 257–275, 2003.

[24] A. M. Perelomov, *Generalized Coherent States and Their Applications*, Springer, Berlin, Germany, 1986.

[25] I. Daubechies, *Ten Lectures on Wavelets*, SIAM, Philadelphia, Pa, USA, 1992.
[26] A. M. Perelomov, "Coherent states for arbitrary Lie group," *Communications in Mathematical Physics*, vol. 26, no. 3, pp. 222–236, 1972.
[27] E. H. Brown, "Generalizations of kervaire's invariant," *Annals of Mathematics*, vol. 95, pp. 368–383, 1972.
[28] G. J. Pottie and A. R. Calderbank, "Channel coding strategies for cellular radio," *IEEE Transactions on Vehicular Technology*, vol. 44, no. 4, pp. 763–770, 1995.
[29] J. P. Costas, "A study of a class of detection waveforms having nearly ideal range-Doppler ambiguity properties," *Proceedings of the IEEE*, vol. 72, no. 8, pp. 996–1009, 1984.
[30] A. M. Kerdock, "A class of low rate nonlinear binary codes," *Information and Control*, vol. 20, no. 2, pp. 182–187, 1972.
[31] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $Z_4$-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 301–319, 1994.
[32] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," *Annals of Physics*, vol. 191, no. 2, pp. 363–381, 1989.
[33] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2397–2417, 1999.
[34] H. S. Shapiro, *Extremal problems for polynomials and power series*, Sc.M. thesis, Massachusetts Institute of Technology, Cambridge, Mass, USA, 1951.
[35] M. Golay, "Multislit spectrometry," *Journal of the Optical Society of America*, vol. 39, pp. 437–444, June 1949.
[36] S. Z. Budisin, "New complementary pairs of sequences," *Electronics Letters*, vol. 26, no. 13, pp. 881–883, 1990.
[37] R. Craigen, "Complex golay sequences," *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. 15, pp. 161–169, 1994.
[38] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.

**S. D. Howard** graduated in 1982 from La Trobe University, Melbourne, Australia. He received his M.S. and Ph.D. degrees in mathematics from La Trobe University in 1984 and 1990, respectively. He joined the Australian Defence Science and Technology Organisation (DSTO) in 1991, where he has been involved in the area of electronic surveillance and radar for the past fourteen years. He has led the DSTO research effort into the development of algorithms in all areas of electronic surveillance, including radar pulse train deinterleaving, precision radar parameter estimation and tracking, estimation of radar intrapulse modulation, and advanced geolocation techniques. Since 2003, he has led the DSTO long-range research program in radar resource management and waveform design.

**A. R. Calderbank** is a Professor of electrical engineering and mathematics at Princeton University where he directs the Program in Applied and Computational Mathematics. He joined Princeton from AT&T where he was a Vice President for research and responsible for designing the only research lab in the world where the primary focus is data. Inventions by Dr. Calderbank in his career at Bell Labs and AT&T have transformed communications practice in voice-band modems, and advanced read channels for magnetic recording and wireless systems. He also created the framework for fault-tolerant quantum computation together with Peter Shor. Dr. Calderbank was honored by the IEEE Information Theory Prize Paper Award in 1995 for his work on the Z4-linearity of Kerdock and Preparata codes (joint with A. R. Hammons Jr., P. V. Kumar, N. J. A. Sloane, and P. Sole), and again in 1999 for the invention of space-time codes (joint with V. Tarokh and N. Seshadri). He became an AT&T Fellow in 2000, received the IEEE Millennium Medal in 2000, and was elected to the National Academy of Engineering in 2005.

**W. Moran** is a Professor of electrical engineering at the University of Melbourne, where he is the Technical Director of the Melbourne Systems Laboratory. Previously he has been a Professor of mathematics at the University of Adelaide and at Flinders University. He also serves as a Consultant to the Australian Department of Defence through the Defence Science and Technology Organisation and as a Consultant to Prometheus Inc. of Rhode Island. His main areas of interest are in signal processing, particularly with radar applications, waveform design and radar theory, and sensor management. He also works in various areas of mathematics including harmonic analysis and number theory. He has published widely in these areas.