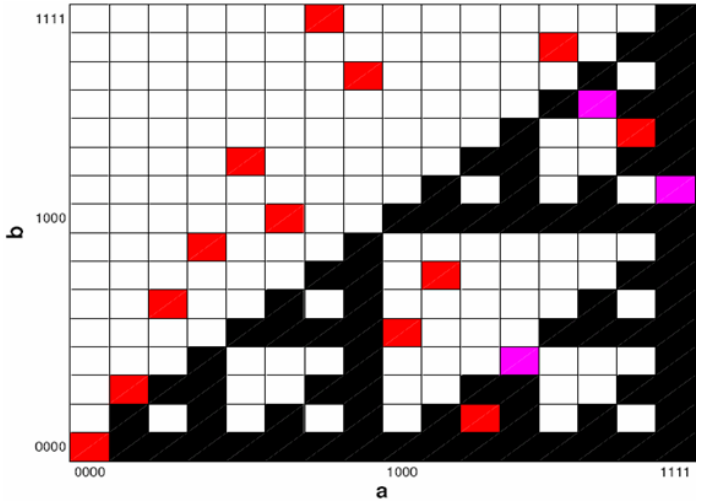
Symmetry and Sequence Design II: Design of Phase Coded Radar Waveforms

Robert Calderbank
Princeton University

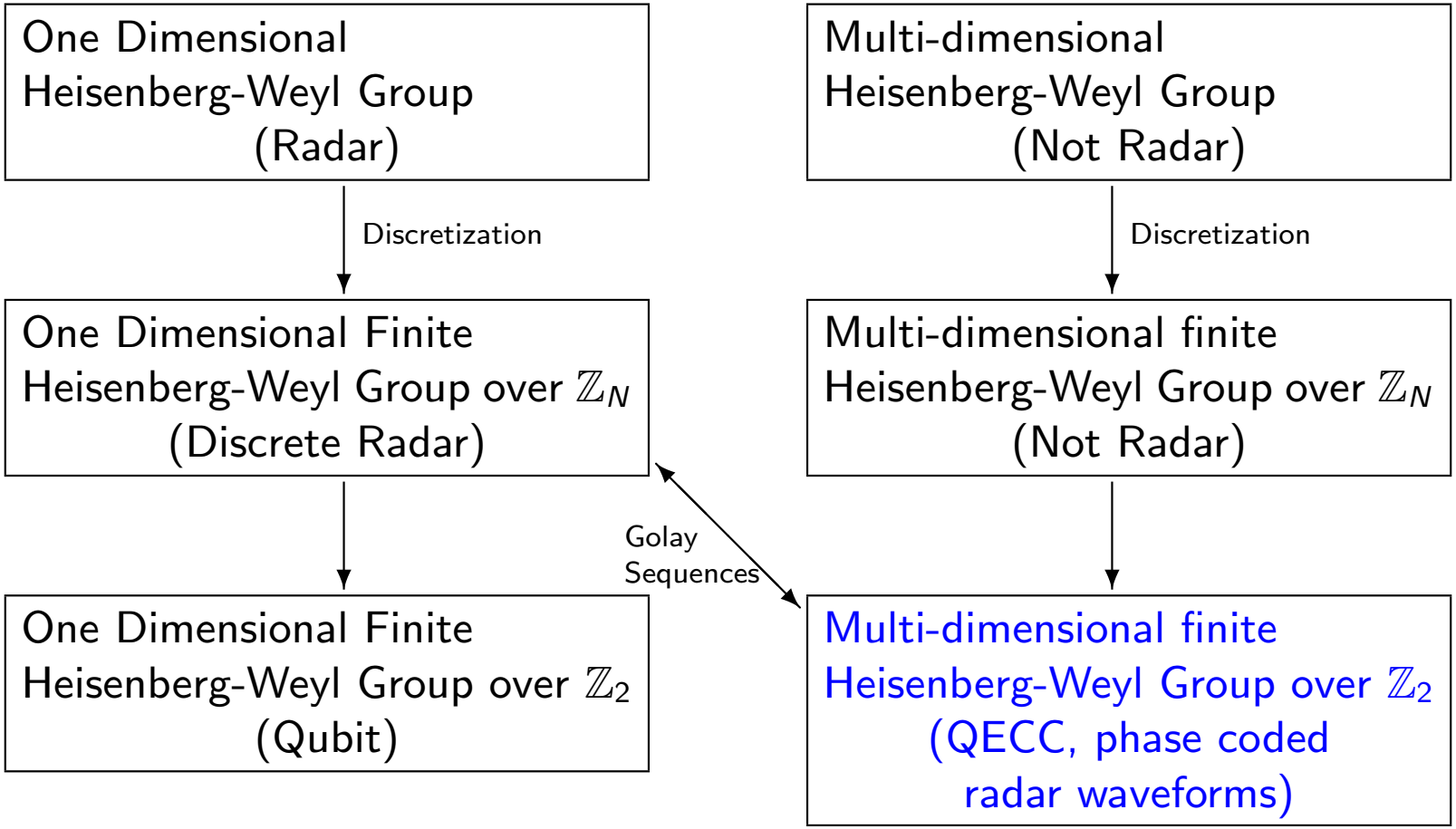
Stephen Howard
Defence Science & Technology Organization Australia

Bill Moran
Melbourne University



Supported by Defense Advanced Research Projects Agency and Air Force Office of Scientific Research

Heisenberg-Weyl Groups and Radar



Perfect Ambiguity Functions and Sets of Equiangular Lines

Moyal's Identity: $\|\theta\|^4 = \frac{1}{N}\sum_{a,b\in\mathbb{Z}_2^m} |A_\theta(a,b)|^2$ with $A_\theta(0,0) = 1$
Impossible to construct an ambiguity function $A_\theta(a,b)$ that is nonzero only at the origin (0,0).

Perfect Ambiguity Function: $|A_\theta(a,b)|$ is constant over $(a,b) \neq (0,0)$

$$|A_\theta(a,b)| = \begin{cases} 1, & \text{if } (a,b) = (0,0) \\ \frac{1}{\sqrt{N+1}}, & \text{if } (a,b) \neq (0,0) \end{cases}$$

Theorem: Perfect ambiguity functions are equivalent to orbits of equiangular lines

Proof: $|(D(a,b)\theta, D(a',b')\theta)| = |(\theta, D(a\oplus a', b\oplus b')\theta)|$

$$= \begin{cases} 1, & \text{if } (a,b) = (a',b') \\ \frac{1}{\sqrt{N+1}}, & \text{if } (a,b) \neq (a',b') \end{cases}$$

Extremal Sets of Euclidean Lines

Lemmens and Seidel (1973): Let L be the number of equiangular lines that can be constructed in a d-dimensional Euclidean space. Then

$$L \leq \frac{1}{2}d(d+1) \text{ in } \mathbb{R}^d \quad \text{and} \quad L \leq d^2 \text{ in } \mathbb{C}^d$$

Proof for $\mathbb{C}^{\mathbf{d}}$: Consider a set $\{s_j\}$ of unit vectors with $|(s_j, s_k)| = \alpha$

Gram matrix $G = [(s_j, s_k)]$

Form the Hadamard or elementwise product of G and G^T

$$G \circ G^T = \alpha^2 J + (1 - \alpha^2) I_L$$

This is nonsingular, since it is the sum of a positive definite matrix and a positive semi-definite matrix.

Matrix rank is Hadamard submultiplicative (see Horn and Johnson)

$$L = \text{rank}(G \circ G^T) \leq \text{rank}(G)\text{rank}(G^T) = d^2$$

64 Equiangular Lines in $\mathbb{C}^8$

Set $\xi = \sqrt{\frac{i}{8}} = \frac{1}{4} + \frac{1}{4}i$ so that $\xi + \bar{\xi} = \frac{1}{2}$ and $\bar{\xi} - \xi = -\frac{i}{2}$

$$\|\xi\mathbf{1} - e_0\|^2 = |-\frac{3}{4} + \frac{i}{4}|^2 + 7\frac{1}{8} = \frac{12}{8} = \frac{3}{2}$$

Proposition: The orbit of the line $7 = \sqrt{\frac{2}{3}}(\xi\mathbf{1} - e_0)$ under $\mathcal{W}(\mathbb{Z}_2^3)$ is a set of 64 equiangular lines in $\mathbb{C}^8$.

Proof:

$$\begin{aligned}
7^\dagger D(a,b)7 &= \frac{2}{3}\left(\frac{1}{8}\mathbf{1}^\dagger D(a,b)\mathbf{1} + e_0^\dagger D(a,b)e_0 - \bar{\xi}\mathbf{1}^\dagger D(a,b)e_0 - \xi e_0^\dagger D(a,b)\mathbf{1}\right) \\
&= \frac{2}{3}\left(\delta_{b,0} + \delta_{a,0} - \left(\bar{\xi} + (-1)^{b.a}\xi\right)\right) \\
&= \frac{1}{3}\begin{cases} 2\delta_{b,0} + 2\delta_{a,0} - 1, & \text{if } b.a = 0 \\ i, & \text{if } b.a = 1 \end{cases}
\end{aligned}$$

Symplectic Symmetries

Hoggar (1998) exhibits 64 lines from a quaternionic polytope that are the orbit of $\frac{1}{\sqrt{6}}(1+i, 0, -1, 1, -i, -1, 0, 0)$ under $\mathcal{W}(\mathbb{Z}_2^3)$

$S_P(6,2)$ symplectic transformations that fix $\mathcal{W}(\mathbb{Z}_2^3)$ by conjugation

135 $\longleftarrow$ 135 equivalent sets of equiangular lines

G symmetry group of the 64 equiangular lines

$GL(\mathbb{Z}_2^3)$ $\longleftarrow$ Given a non-singular matrix A, define $s_A : e_V \longrightarrow e_{vA}$

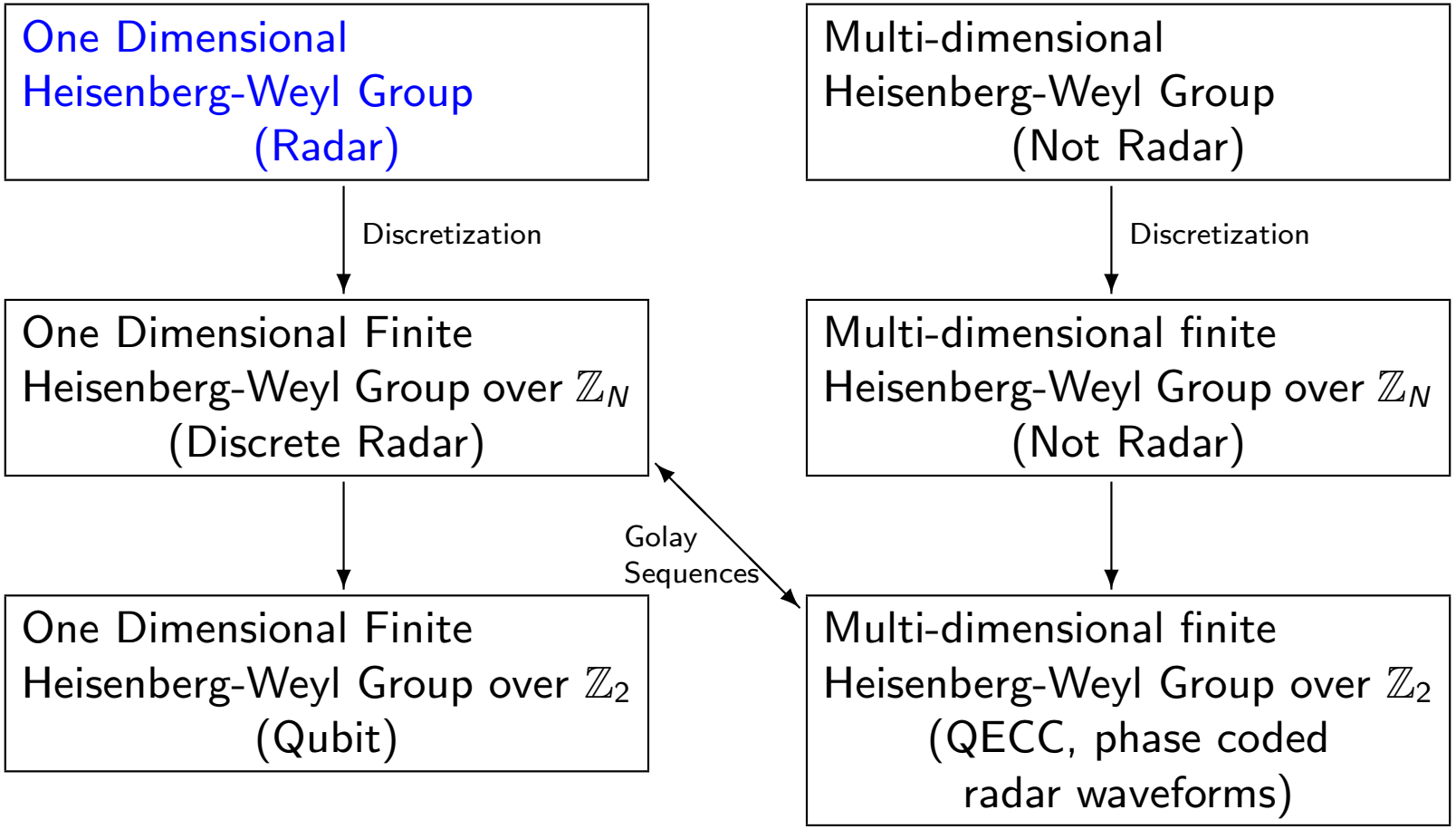
$\mathcal{W}(\mathbb{Z}_2^3)$

Define $S_A : e_v \longrightarrow e_{vA}$ where A is nonsingular

Then S_A fixes $7 = \sqrt{\frac{2}{3}}(\xi\mathbf{1} - e_0)$ and fixes $\mathcal{W}(\mathbb{Z}_2^3)$ by conjugation:

$$S_A^{-1} D(a,0) S_A = D(aA, 0)$$
$$S_A^{-1} D(0,b) S_A = D(0, bA^{-T})$$

Heisenberg-Weyl Groups and Radar



Monostatic and Multistatic Radar

Monostatic Radar: transmitter and receiver are colocated

- single view of the scene
- easy for transmitter and receiver to share a common stable clock (local oscillator) which is required for both range and doppler measurements

Multistatic Radar: widely dispersed antenna elements

- provides multiple views of the scene and a (wide angle) tomographic approach to detection
- complicated by physical, mathematical and engineering challenges of the Time of Arrival coherent combining, and by the computation required to integrate multiple views

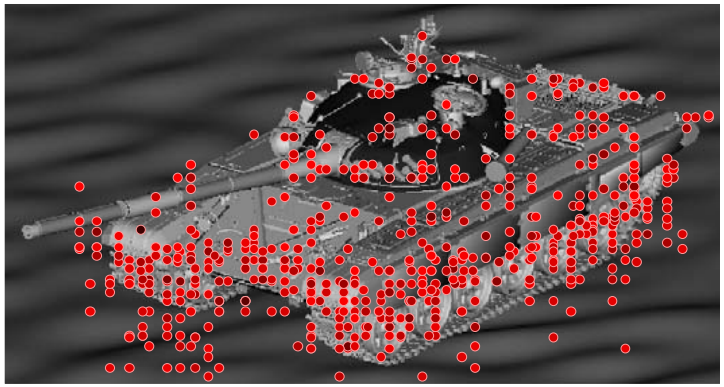
Fully Polarimetric Radar System: Scattering Model

Radar is able to transmit and receive in two orthogonal polarizations simultaneously.

$$\begin{pmatrix} h_{VV} & h_{VH} \\ h_{HV} & h_{HH} \end{pmatrix} = C_{R_X} \begin{pmatrix} \sigma_{VV} & \sigma_{VH} \\ \sigma_{HV} & \sigma_{HH} \end{pmatrix} C_{T_X}$$

$\boldsymbol{\sigma_{VH}}$**:** scattering coefficient into vertical polarization channel from horizontally polarized incident field

$\mathbf{C_{R_X} C_{T_X}}$**:** polarization coupling of T_X and R_X antennas



Physical target represented as a set of complex weighted point scatterers

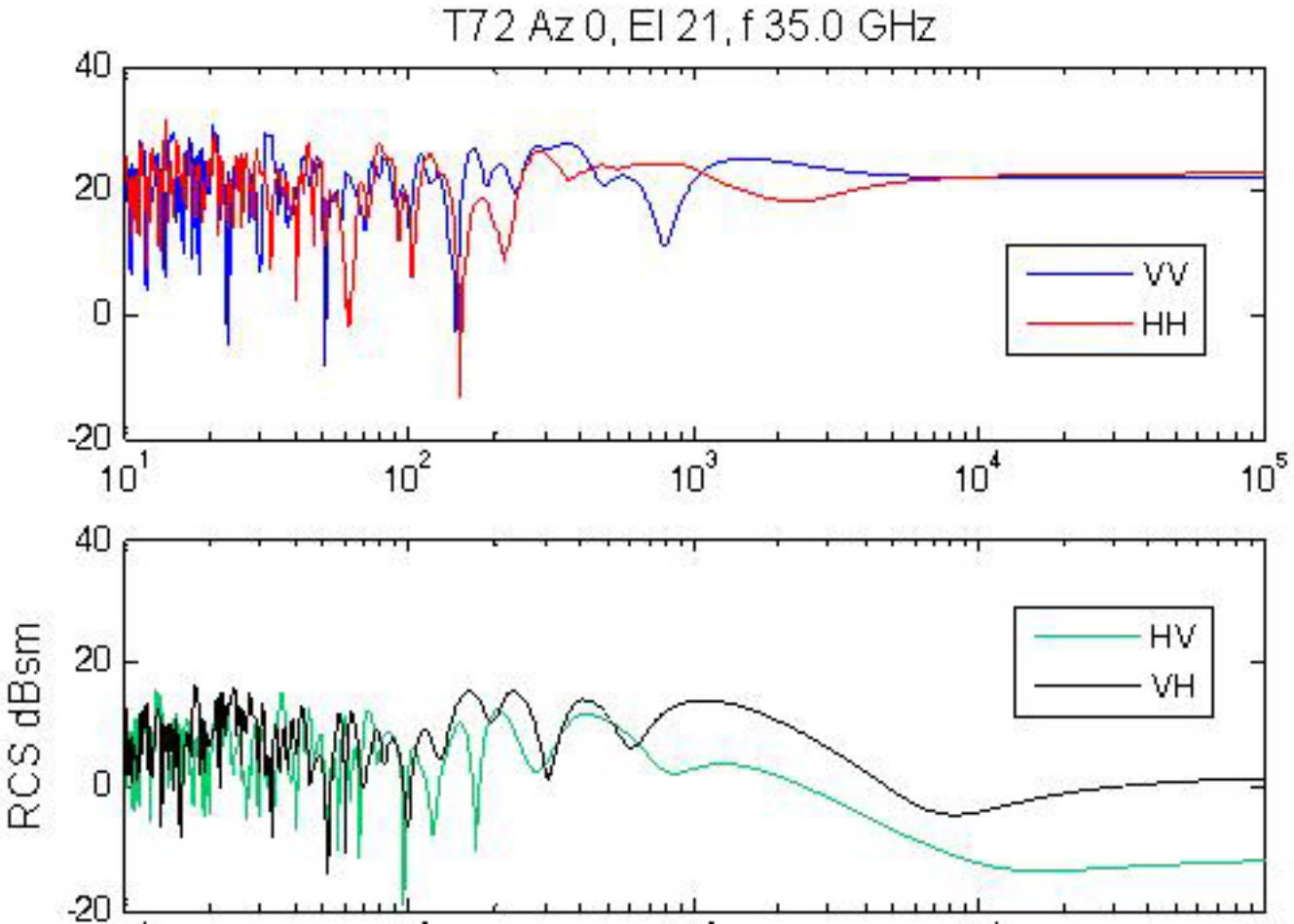
- courtesy Raytheon Missile systems

Intuition about the Scattering Matrix

Two Idealized Models:

$$\begin{pmatrix} h_{VV} & h_{VH} \\ h_{HV} & h_{HH} \end{pmatrix}$$

- entries are zero mean Gaussian iid
- entries h_{HV}, h_{VH} are substantially smaller than h_{HH}, h_{VV}

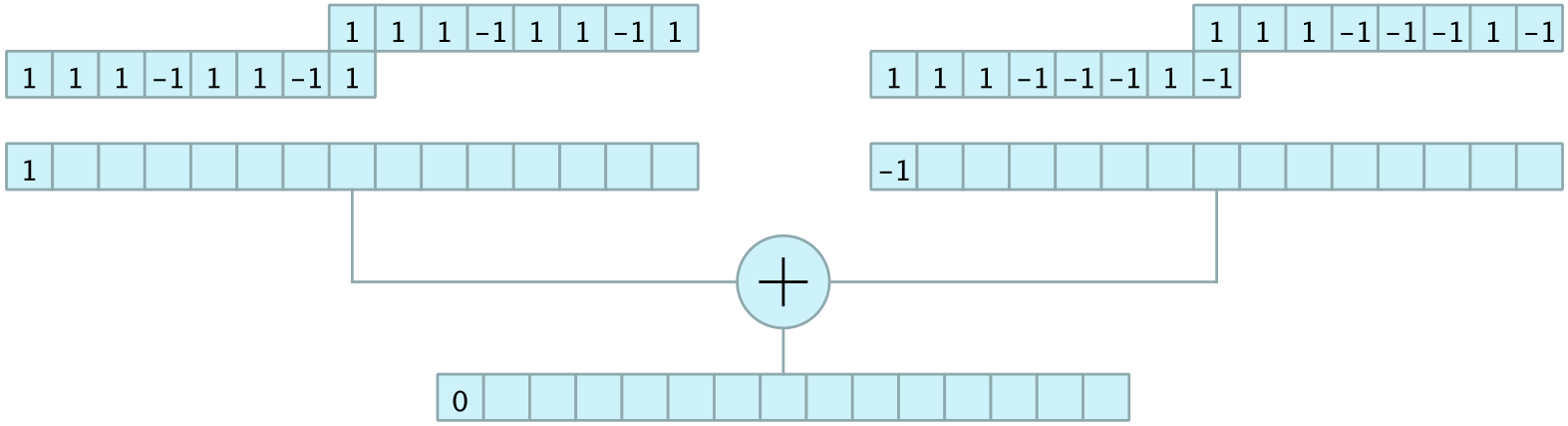


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

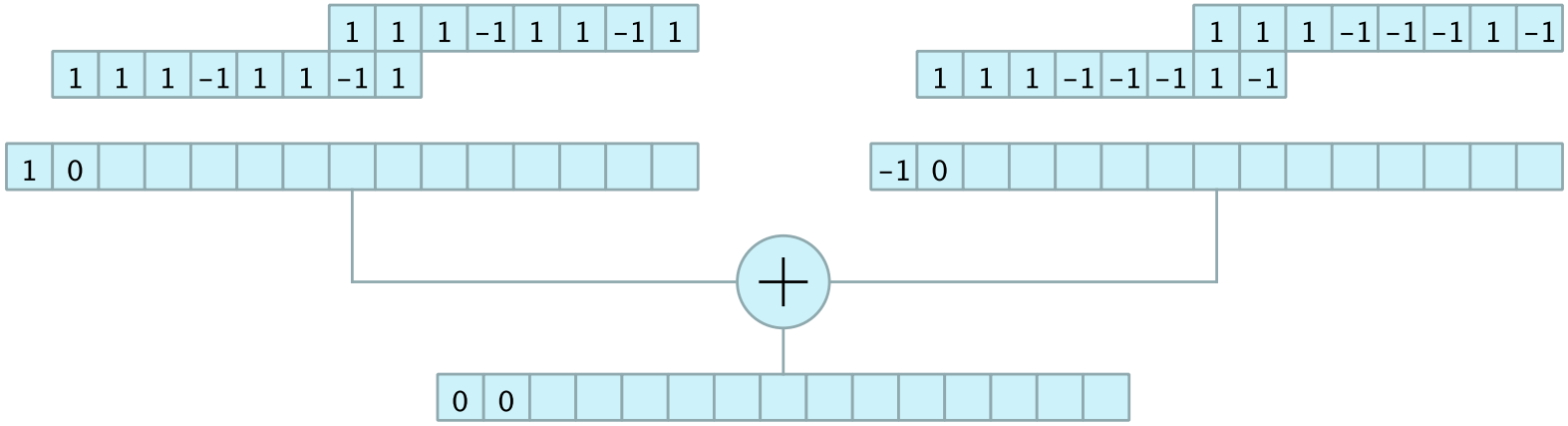


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

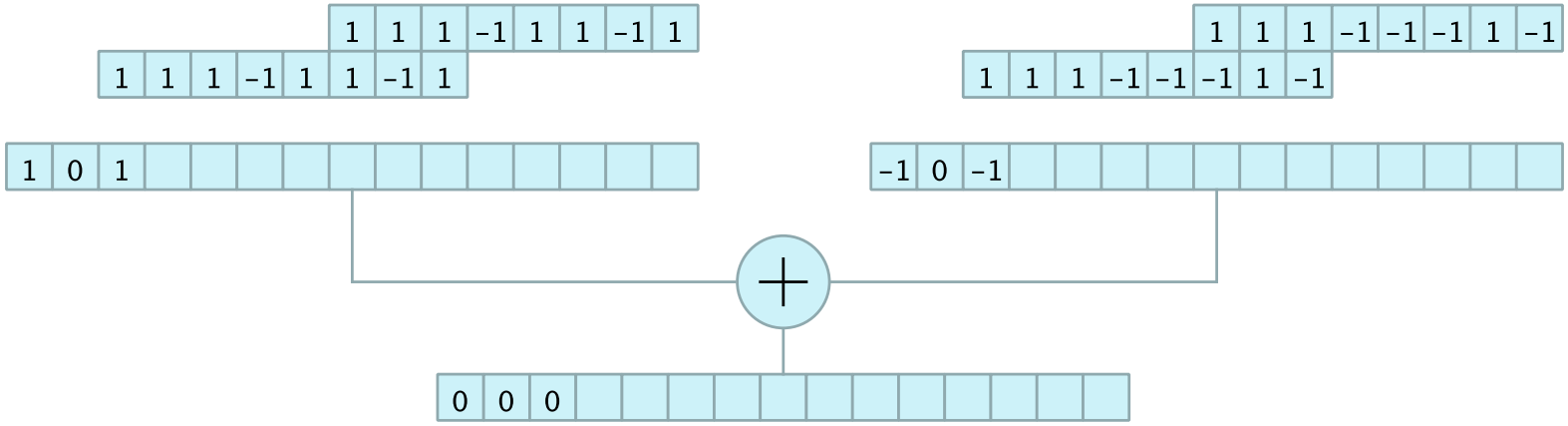


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

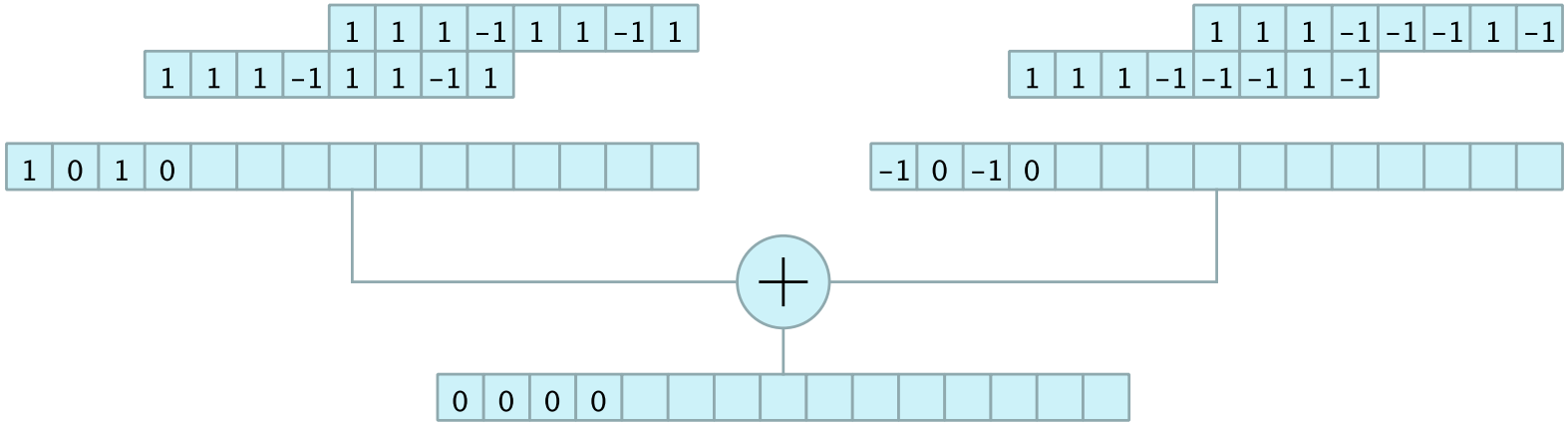


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

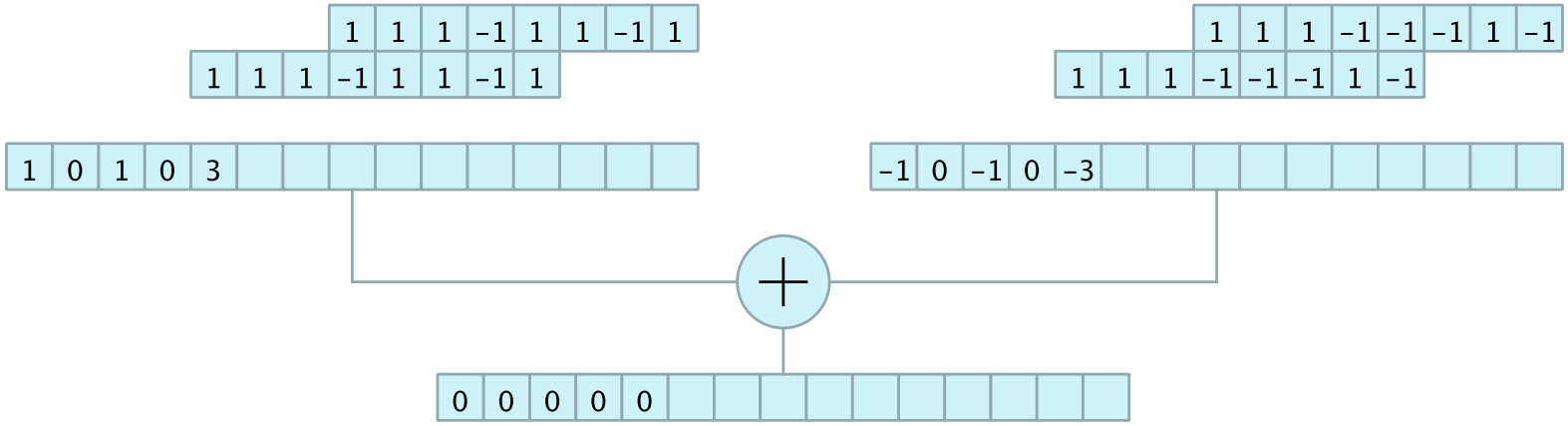


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

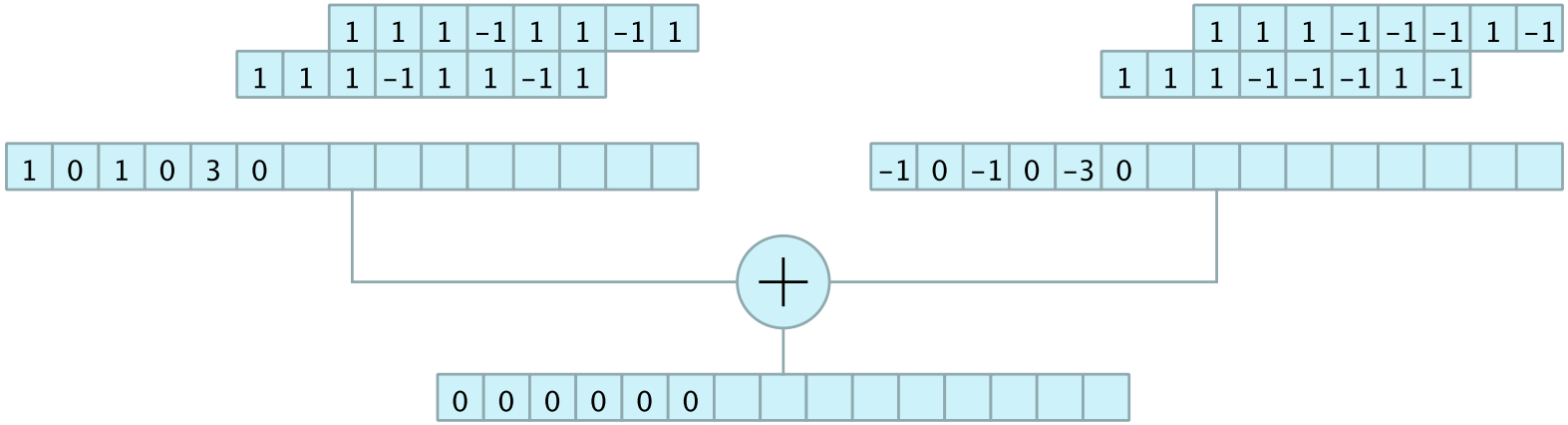


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

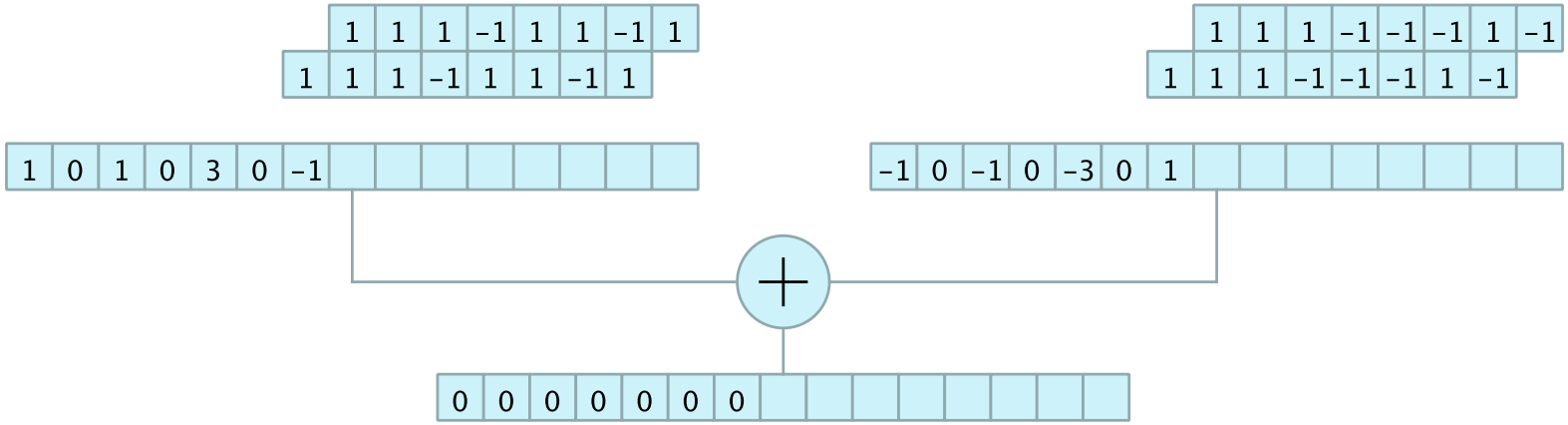


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

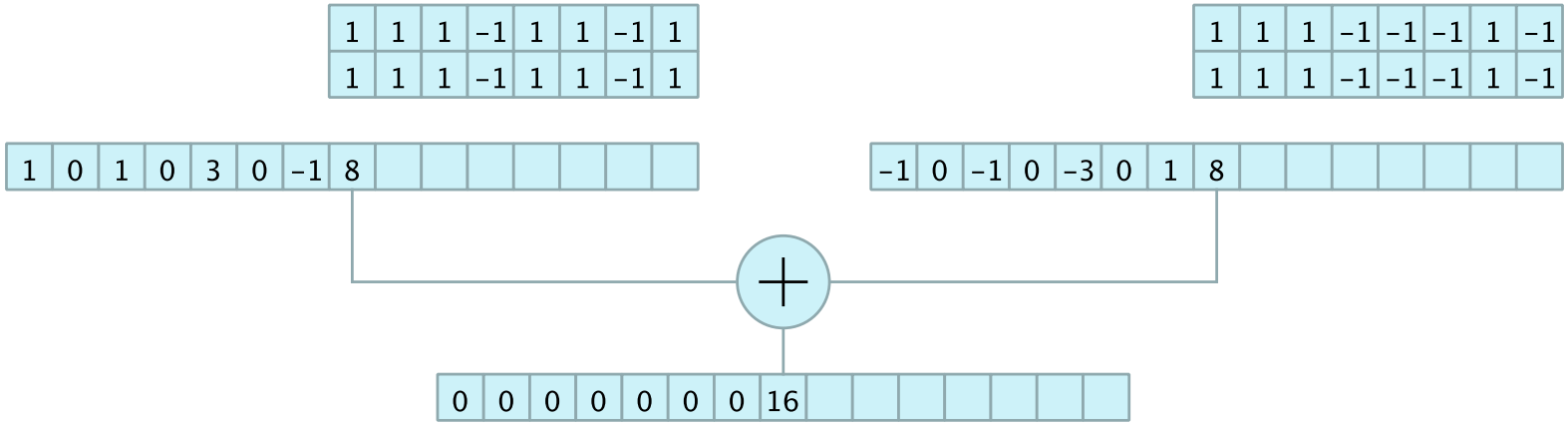


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

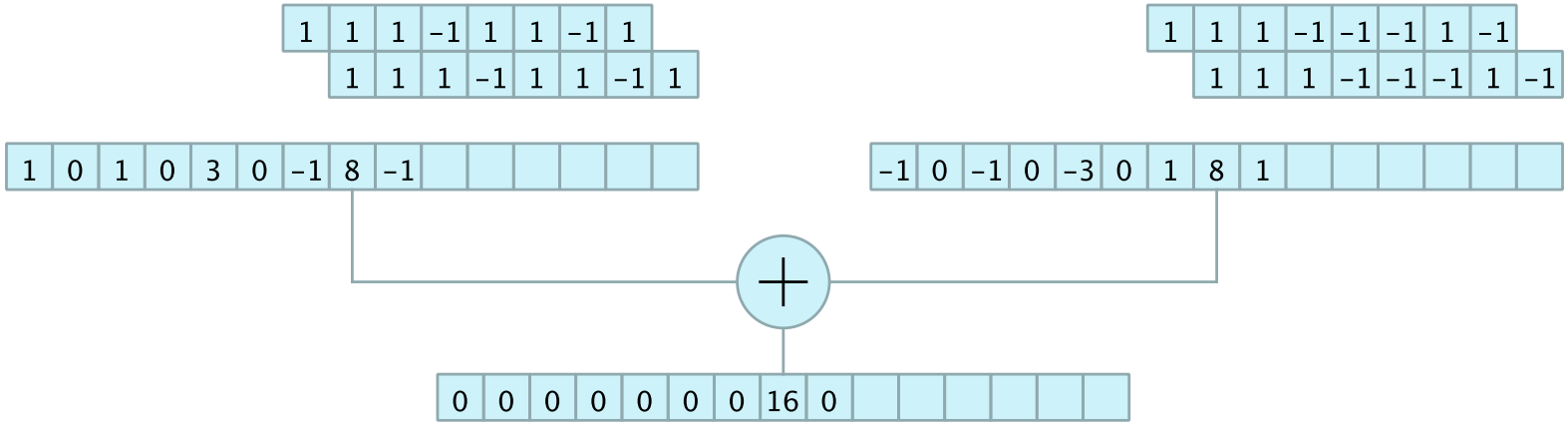


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

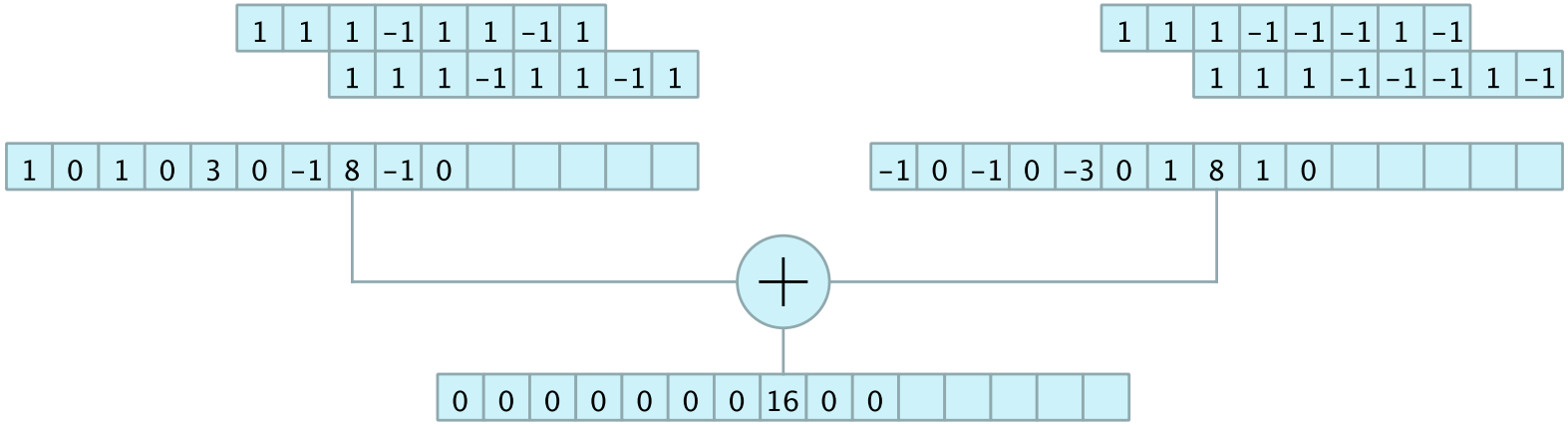


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

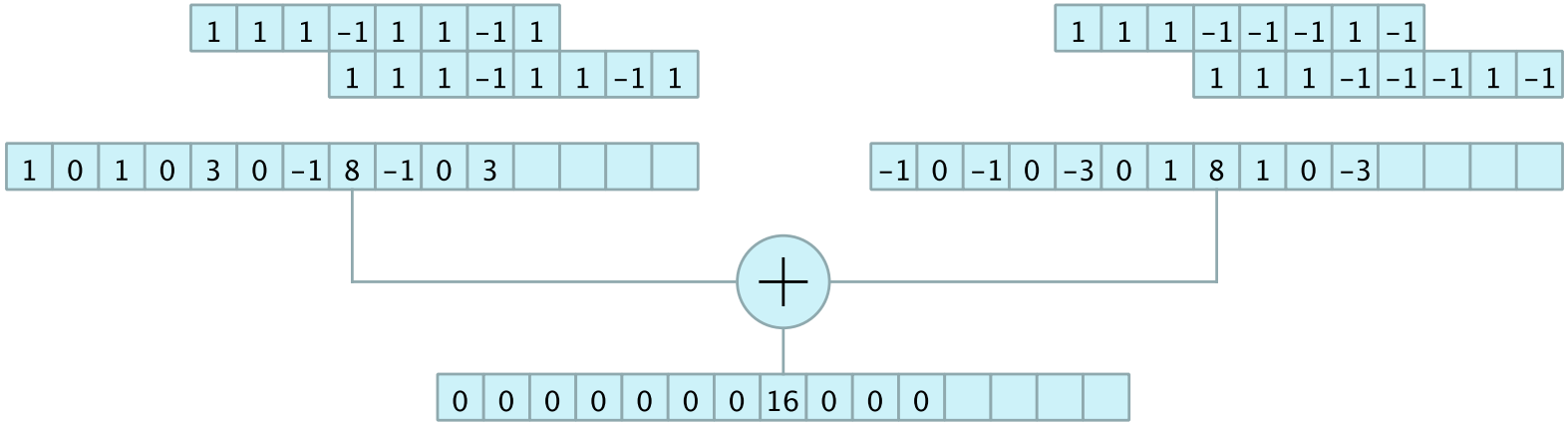


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

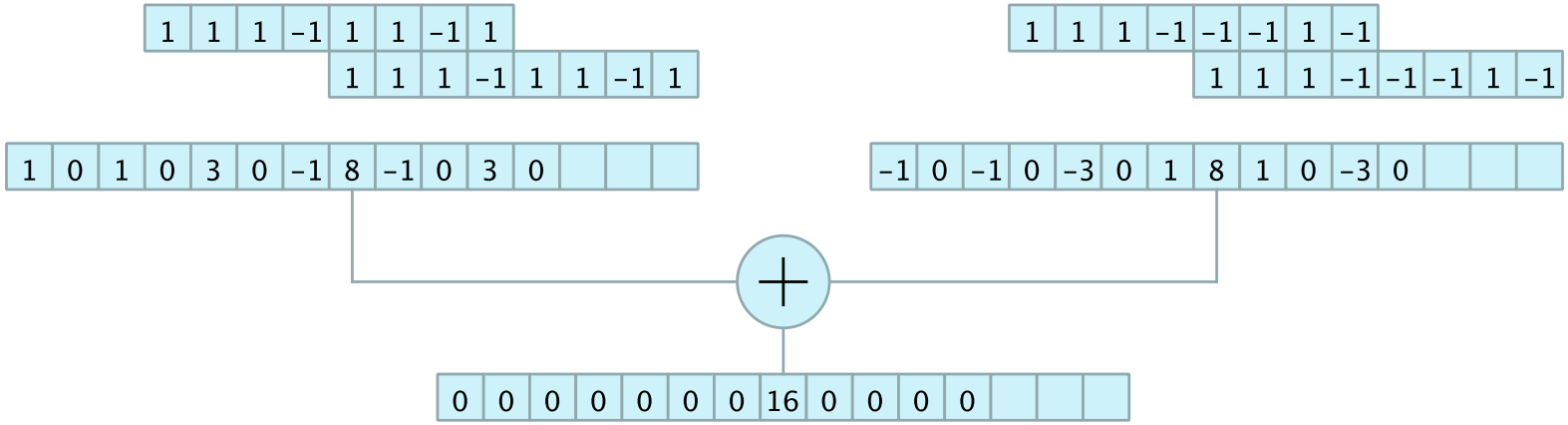


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

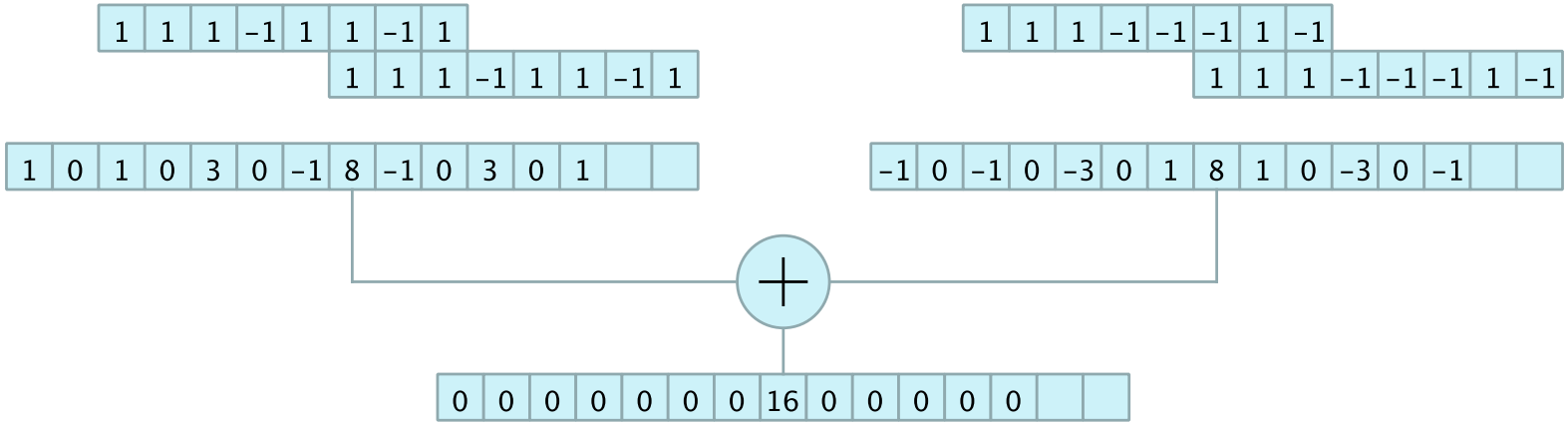


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

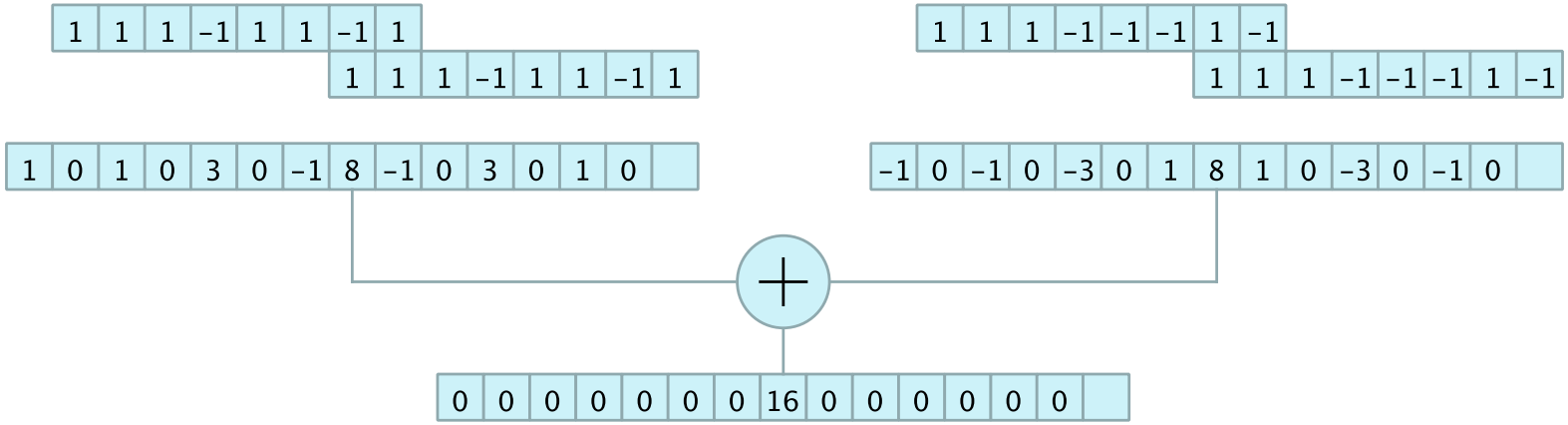


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.

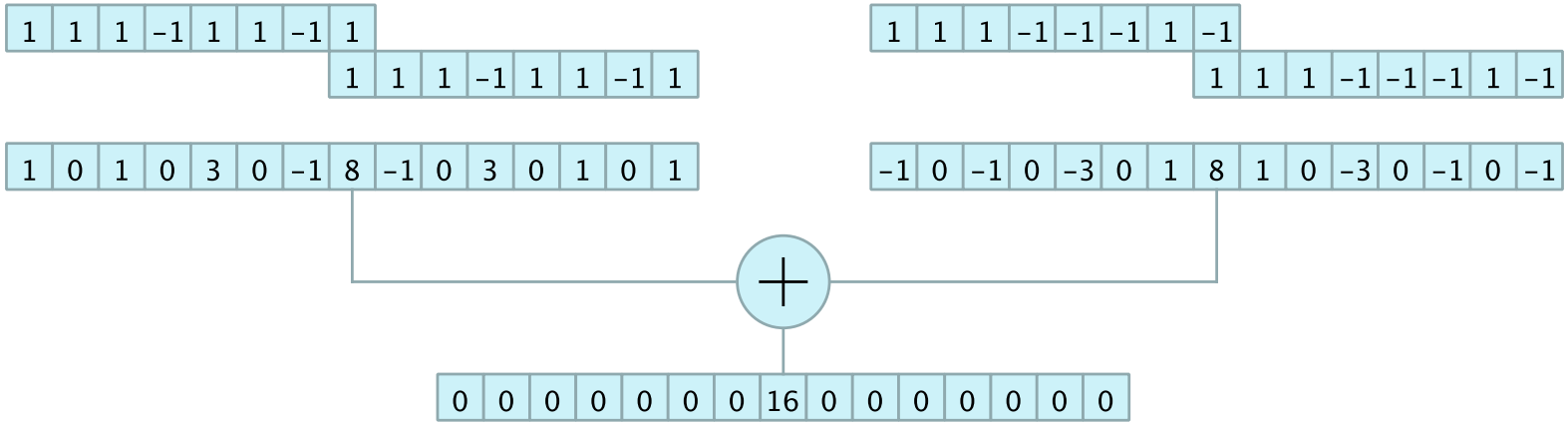


Golay Complementary Sequences

Definition: Two length N unimodular sequences of complex numbers x and y are Golay complementary if the sum of their auto-correlation functions satisfies.

$$corr_k(x) + corr_k(y) = 2N\delta_{k,0}$$

for $k = -(N-1), \cdots, (N-1)$.



Polarization Diversity, Alamouti Signaling and Golay Pairs

Alamouti space-time block code coordinates transmission on V and H channels – columns represent different slots in time or frequency.

$$R = (r_1, r_2) = \begin{pmatrix} h_{VV} & h_{VH} \\ h_{HV} & h_{HH} \end{pmatrix} \begin{pmatrix} w_V & -\tilde{w}_H \\ w_H & \tilde{w}_V \end{pmatrix} + Z$$

Conjugate Time Reversal:

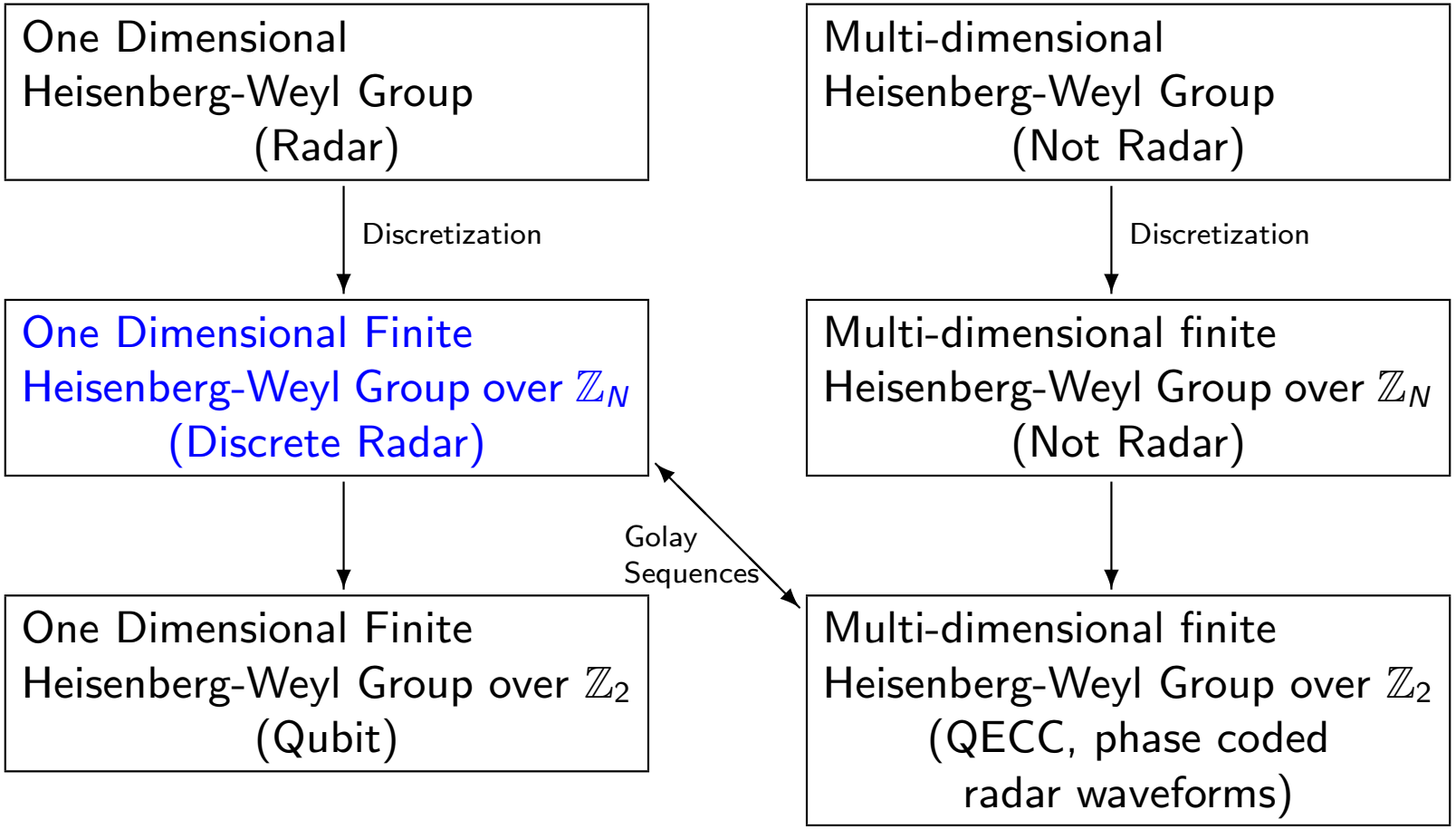
$$w_V = w_V(D) = D^7 + D^6 + D^5 - D^4 + D^3 + D^2 - D + 1$$
$$\tilde{w}_V = \tilde{w}_Y(D) = 1 + D + D^2 - D^3 + D^4 + D^5 - D^6 + D^7 \qquad (w_V(D^{-1})D^7)$$

Golay Property: $w_V \tilde{w}_V + w_H \tilde{w}_H = 2dD^d$

Matched Filtering:

$$R \begin{pmatrix} \tilde{w}_V & \tilde{w}_H \\ -w_H & w_V \end{pmatrix} \text{ provides an estimate of } \begin{pmatrix} h_{VV} & h_{VH} \\ h_{HV} & h_{HH} \end{pmatrix}$$

Heisenberg-Weyl Groups and Radar



The Heisenberg-Weyl Group $\mathcal{W}(\mathbb{Z}_N)$

Radar Scene: Collection of point scatterers each of which delays the waveform by some time τ and Doppler shifts by some ν

Hilbert Space $\mathbb{C}^{\mathbf{N}}$: Dirac basis $e_v, v \in \mathbb{Z}_2^m$ labeled by $N = 2^m$ discrete time delays or ranges

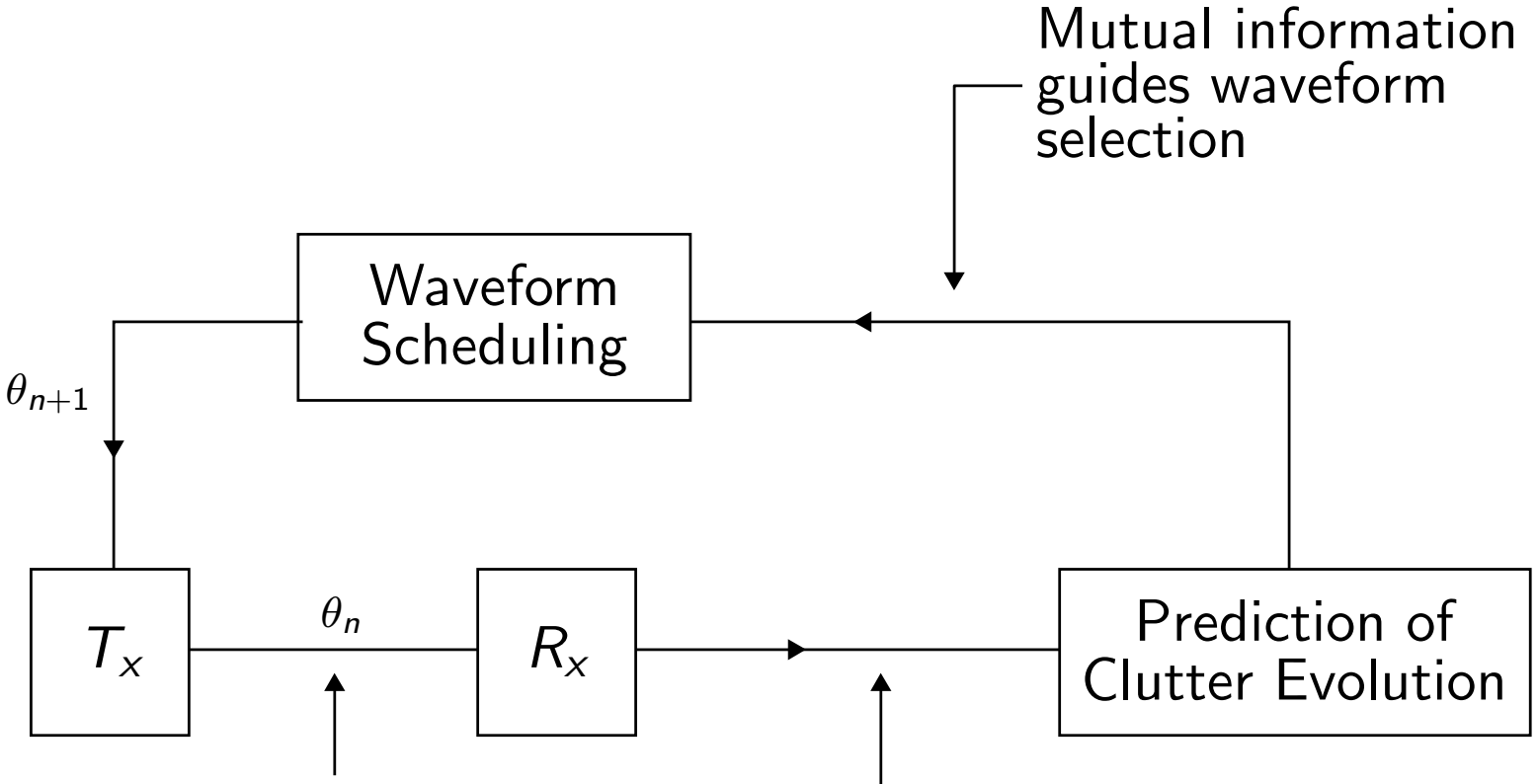
Heisenberg-Weyl Group $\mathcal{W}(\mathbb{Z}_{\mathbf{N}})$: $\Delta(k,j) = \sum_\ell w^{j\ell} e_{\ell+k} e_\ell^\dagger$ where $w = e^{2\pi i/N}$ and addition takes place modulo N

$\mathbb{Z}_{\mathbf{N}}$-Golay Complementary Pairs φ, ψ:

$$\varphi^\dagger \Delta(k,0)\varphi + \psi^\dagger \Delta(k,0)\psi = 0 \qquad \text{for } k \neq 0$$
$$Tr((P_\varphi + P_\psi)\Delta(k,0)) = 0 \qquad \text{for } k \neq 0$$

Note: The orthonormal basis $D(a,b)$ from $\mathcal{W}(\mathbb{Z}_2^m)$ provides a sparse representation of P_φ, P_ψ for many widely used sequences φ, ψ

Detection in Radar: Playing Twenty Questions with an Unknown Operator



$$S_n = \sum_{k,j} s_n(k,j)\Delta(k,j)$$

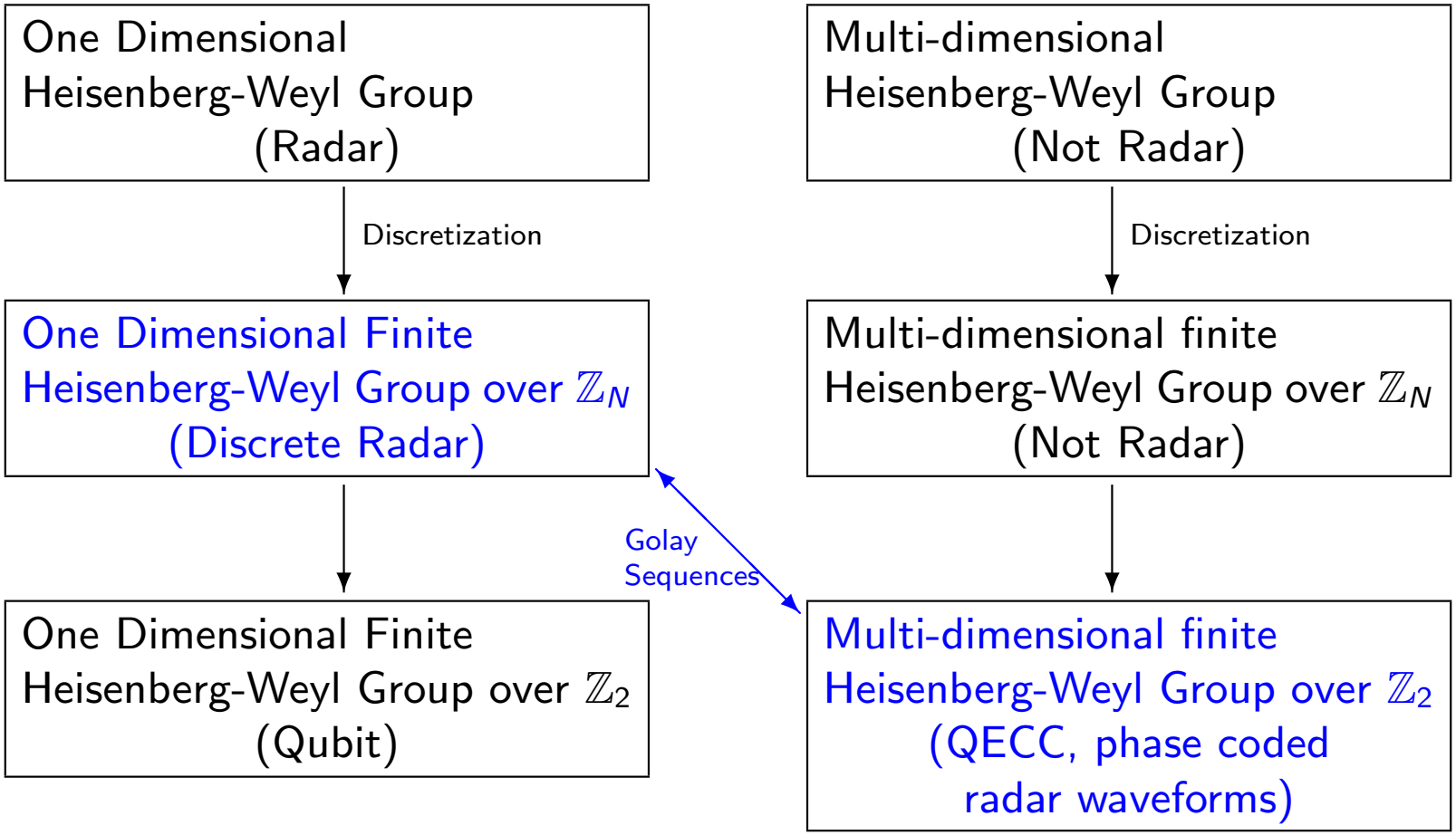
$$\psi_n = s_n\theta_n + z_n$$

$$\psi_n = B_{\theta_n}[s_n(k,j)] + z_n$$

$$S_{n+1} = \Gamma S_n + w_n$$

Kalman filter formalism tracks clutter evolution

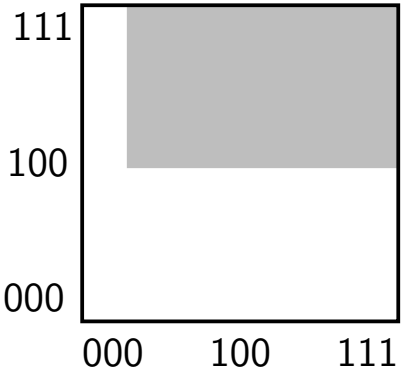
Heisenberg-Weyl Groups and Radar



Representation of the Operators $\Delta(k, j)$

$S_{\Delta,j}$ = support of the subspace spanned by $\Delta(k, j), k \neq 0$

m = 3:



Theorem: If j is odd then

$(a, b) \in S_{\Delta,j}$ if and only if $a \neq 0$ and $b_{m-1} = 1$

Lemma: Let $\omega = e^{2\pi i/N}$ and let $c(x) = \sum_i c_i x^i$ be a polynomial with integer coefficients. Then

$$c(\omega) = 0 \text{ if and only if } c_i = c_{i+N/2}$$

Proof: $p(x) = x^{N/2} + 1$ is the minimal polynomial of ω
To see that $p(x)$ is irreducible, change variables $x \to y + 1$ and apply the Eisenstein irreducibility criterion for the prime 2.

The Subspace $S_{\Delta,j}$ for j odd

$$(a,b) \in S_{k,j}\ j \text{ odd } \langle = \rangle\, Tr(D(a,b)^\dagger \Delta(k,j)) \neq 0$$

$(\mathbf{a},\mathbf{b}) \notin \mathbf{S_{\Delta,j}}$ when $\mathbf{a = 0}$: $D(a,b)$ is diagonal and $\Delta(k,j)$ has zero diagonal

Define $\ell(i)$ as the column in $\Delta(k,j)$ containing ω^i and note that ℓ is a permutation since j is odd.

$$Tr(D(a,b)^\dagger \Delta(k,j)) = \sum_{i=0}^{N-1} c_i \omega^i = \sum_{\ell} (D(a,b)e_\ell, \Delta(k,j)e_\ell)$$

$$c_i = e^\dagger_{\ell(i)+k} D(a,b) e_{\ell(i)}$$

$\mathbf{b_{m-1} = 0}$: $D(a,b) = \left(\begin{array}{c|c} A & \\ \hline & A \end{array}\right)$ or $\left(\begin{array}{c|c} & A \\ \hline A & \end{array}\right)$

$$e^\dagger_{\ell(i)+k+N/2} D(a,b) e_{\ell(i)+N/2} = e^\dagger_{\ell(i)+k} D(a,b) e_{\ell(i)}$$

Hence $c_i = c_{i+N/2}$ and $Tr(D(a,b)^\dagger \Delta(k,j)) = 0$

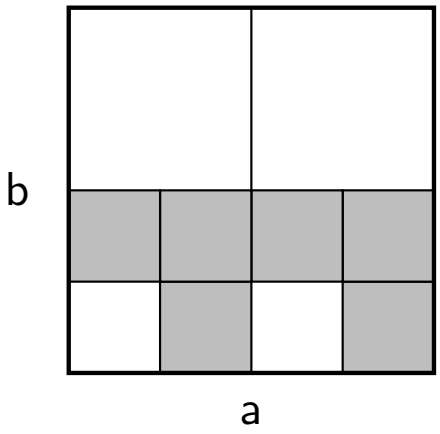
The Subspace $S_{\Delta,j}$ for j odd (contd.)

$\mathbf{b_{m-1} = 1}$**:** Now $D(a,b) = \left(\begin{array}{c|c} A & \\ \hline & -A \end{array}\right)$ or $\left(\begin{array}{c|c} & A \\ \hline -A & \end{array}\right)$

$$c_i = e^{\dagger}_{\ell(i)+k} D(a,b) e_{\ell(i)} = -c_{i+N/2}$$

As k runs through $\mathbb{Z}_N$ so does $\ell(i) + k$

Hence $c_i \neq 0$ for some $\Delta(k,j)$ and $(a,b) \in S_{\Delta,j}$



Theorem: If $j = 2 \pmod 4$ then

$$(a,b) \in S_{\Delta,j} \langle = \rangle a \neq 0, b_{m-1} = 0$$
$$\text{and either } b_{m-2} = 1 \text{ or } a_{m-2} = 1$$

The Subspace $S_{\Delta,j}$ for $j \equiv 2 \pmod 4$

Define $\ell(i) = \{d \in \mathbb{Z}_N | \omega^i$ appears in column d of $\Delta(k,j)\}$
The sets $\ell(i)$ consist of pairs $d, d + N/2$ and these pairs are disjoint

$$Tr(D(a,b)^\dagger \Delta(k,j)) = \sum_{i=0}^{N-1} c_i \omega^i \qquad \text{(polynomial in } \omega^2\text{)}$$

$$c_i = \sum_{d \in \ell(i)} e_{d+k}^\dagger D(a,b) e_d$$

$$c_{i+N/2} = \sum_{d \in \ell(i)} e_{d+N/4+k}^\dagger D(a,b) e_{d+N/4}$$

$\mathbf{0, b \notin S_{\Delta,j}}$**:** $D(0,b)$ is diagonal and $\Delta(k,j)$ has zero diagonal

$\mathbf{(a,b) \notin S_{\Delta,j}}$ **if** $\mathbf{b_{m-1} = 1}$**:**

$$D(a,b) = \left(\begin{array}{c|c} A & \\ \hline & -A \end{array}\right) \text{ or } \left(\begin{array}{c|c} & A \\ \hline -A & \end{array}\right)$$

$$e_{d+k}^\dagger D(a,b) e_d + e_{d+N/2+k}^\dagger D(a,b) e_{d+N/2} = 0$$

The Subspace $S_{\Delta,j}$ for $j \equiv 2 \pmod 4$

$\mathbf{b_{m-1} = 0, b_{m-2} = 1}$:

A			
	$-A$		
		A	
			$-A$

00

	$-A$		
A			
			$-A$
		A	

01

		A	
			$-A$
A			
	$-A$		

10

			A
		$-A$	
	A		
$-A$			

11

$a_{m-1}a_{m-2}$

$$e^{\dagger}_{d+k} D(a,b) e_d = -c^{\dagger}_{d+N/4+k} D(a,b) e_d \text{ and } c_i = -c_{i+N/2}$$

$\mathbf{b_{m-1} = 0, b_{m-2} = 0}$:

A			
	A		
		A	
			A

00

		A	
			A
A			
	A		

10

	A		
A			
			A
		A	

01

			A
		A	
	A		
A			

11

$a_{m-1}a_{m-2}$

The Subspace $S_{\Delta,j}$ for j even

$\mathbf{a_{m-2} = 0}$: $e^{\dagger}_{d+k} D(a,b) e_d = e^{\dagger}_{d+N/4+k} D(a,b) e_d$ and
$c_i = c_{i+N/2}$

$\mathbf{a_{m-2} = 1}$: $e^{\dagger}_{d+k} D(a,b) e_d = e^{\dagger}_{d+N/2+k} D(a,b) e_d$
If $c_i \neq 0$ then $c_{i+N/2} = 0$

Theorem: Let $j = 2^t j'$ where $0 < t < m$ and j' is odd. Then $(a,b) \in S_{\Delta,j}$ if and only if the following hold:

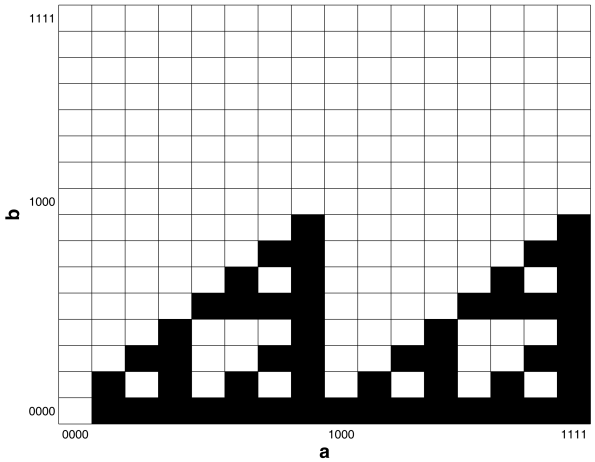
1. $a \neq 0$
2. $b_{m-1} = 0$
3. either $b_{m-t-1} = 1$ or $a_{m-t-1} = 1$
4. $b_{m-2} \ldots b_{m-t}$ is covered by $a_{m-2} \ldots a_{m-t}$

(here $x = (x_i)$ is covered by $y = (y_i)$ if the support of x is contained in the support of y: that is $y_i = 0$ implies $x_i = 0$)

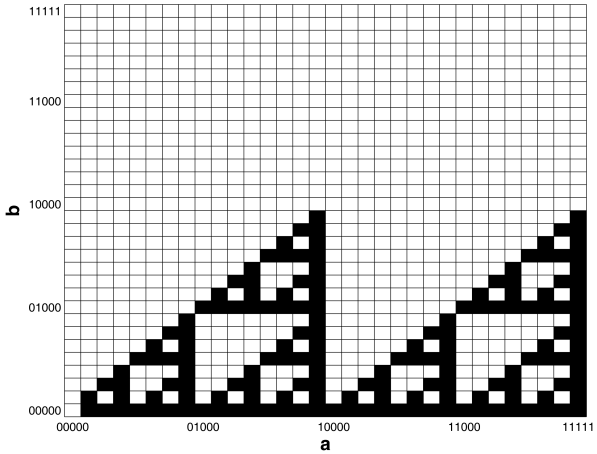
Representation of the Shift Operators $\Delta(k, 0)$

Theorem: $(a, b) \in S_{\Delta,0} \Leftrightarrow a \neq 0, b_{m-1} = 0$ and a covers b.
The support takes the form of a pair of Sirpinski triangles

$m = 4$:



$m = 5$:



$(\mathbf{a}, \mathbf{b}) \notin \mathbf{S}_{\Delta,0}$ if $\mathbf{b}_{\mathbf{m}-1} = \mathbf{1}$:

$$D(a, b) = \left(\begin{array}{c|c} A & \\ \hline & -A \end{array}\right) \text{ or } \left(\begin{array}{c|c} & A \\ \hline -A & \end{array}\right)$$

$$e^{\dagger}_{d+k} D(a, b) e_d = -e_{d+N/2+k} D(a, b) e_{d+N/2}$$

$$\text{so } Tr(D(a, b)^{\dagger} \Delta(k, 0)) = 0$$

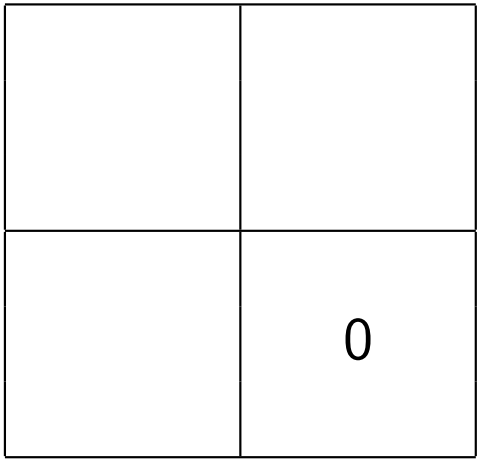
$\mathbb{Z}$-Golay Sequences from $\mathbb{Z}_N$-Golay Sequences

Let $\theta = \sum_{v, v_{m-1}=0} \theta_v e_v$ and $\varphi = \sum_{v, v_{m-1}=0} \varphi_v e_v$
We may view θ, φ as sequences $\bar{\theta}, \bar{\varphi}$ of length 2^{m-1} or as sequences of length 2^m obtained by padding with zeros.

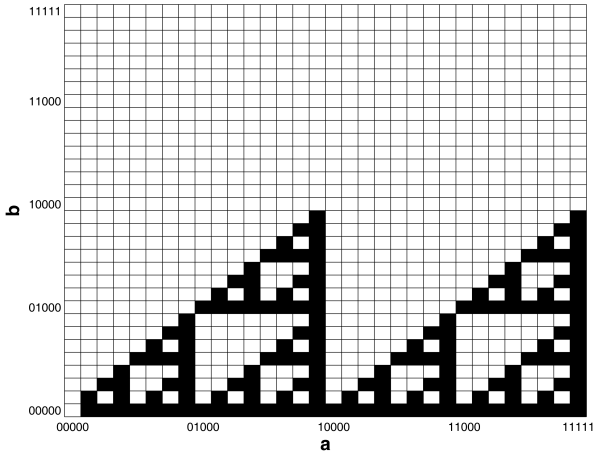
Proposition: $\bar{\theta}, \bar{\varphi}$ are $\mathbb{Z}$-Golay complementary if θ, φ are $\mathbb{Z}_N$-Golay complementary

Proof: Look at the Weyl transform of P_θ, P_φ and $\Delta(k, 0)$

P_θ, P_φ :



$\Delta(k, 0)$:



$\uparrow A_\theta(a, b) = (\theta, D(a, b)\theta) = 0$

Budisin Golay Sequences

Found in orthonormal bases associated with particular maximal commutative subgroups X_P – the interaction with $\Delta(k,0)$ is determined by pairs (v, vP) where v covers vP

$$m = 2 : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad (v, vP) = (11, 11)$$

$$m = 3 : \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad (v, vP) = (101, 010) \text{ or } (111, 101)$$

$$m = 4 : \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad (v, vP) = (1101, 1100), (1011, 0011), (1111, 1001)$$

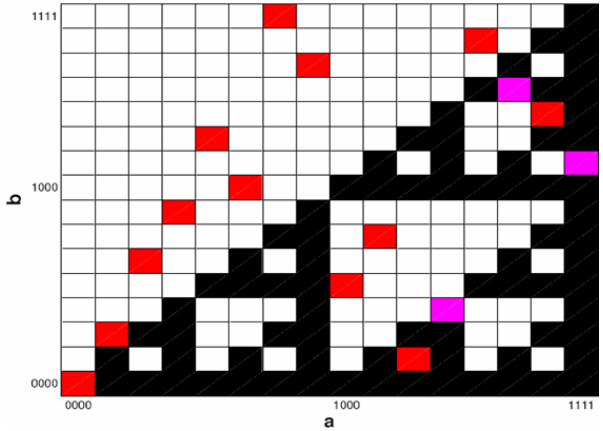
Fibonacci sequence counts the number of pairs (v, vP)

- $D(v, vP)$ anticommutes with $D(0\ldots0, 10\ldots0)$

Picturing the Golay Property

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\varphi = D(0\ldots0, 10\ldots0)\theta$$



P minimizes overlap (magenta) between the support of P_θ, P_φ (the subgroup X_P shown in red) and the support of $S_{\Delta,0}$ (black)
$D(0\ldots0, 10\ldots0)$ removes overlap between the support of $P_\theta + P_\varphi$ and the support of $S_{\Delta,0}$

$$(A_\varphi + A_\theta)(v, vP) = ((-1) + 1)A_\theta(v, vP) = 0$$

Symmetries of the Support of the Shift Operator

- $d_Q^{-1} D(a,b) d_Q = D(a, b + aQ)$

If a covers b and Q is diagonal then a covers $b + aQ$. Conjugation by d_Q fixes the support of the shift operators

- $S_A : e_v \to e_{vA}$ where A is a permutation matrix

$$S_A^{-1} D(a, aP) S_A = D(aA, aPA) = D(a', a' A^T PA)$$

Conjugation by S_A fixes the support of the shift operator

$$\begin{array}{ccc} \mathcal{F}_P & & \text{Golay pairing determined by } D(a_0, b_0) \\ \downarrow & & \downarrow \\ \mathcal{F}_{P'} & & \text{Golay pairing determined by} \\ (P' = A^T PA + Q) & & D(a_0 A^T, b_0 A^T + a_0 Q) \end{array}$$

Classification of Golay Pairs in $RM(2, m)$

$\alpha(P)$: the equivalence class of all binary symmetric matrices that can be obtained from P by simultaneous permutation of rows and columns and by changing the diagonal

Φ: the Golay-Budisin equivalence class

Golay Property: Follows from the existence of a hyperplane disjoint from all non-zero pairs (v, vP) where v covers vP

Theorem: Φ is the only equivalance class with the Golay property

Proof: Induction on m

It is enough to prove that Φ is the only equivalence class with the property that every matrix in the class has rank $m-1$ or m.

- if $vP = wP = (v+w)P = 0$ then every hyperplane contains at least one of v, w and $v+w$

Golay Quads and Beyond

$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

If v covers vP then $D(v, vP)$ anticommutes with either $D(0\ldots0, 0\ldots01)$ or $D(0\ldots0, 10\ldots0)$

Pairs (v, vP) are disjoint from a space of codimension 2

Golay Quads: $Tr((\theta_1\theta_1^\dagger + \theta_2\theta_2^\dagger + \theta_3\theta_3^\dagger + \theta_4\theta_4^\dagger)\Delta(k, 0)) = 0$ for $k \neq 0$

Golay Number: Given an orthonormal basis $\mathcal{F}_P$ this is the codimension of the largest subspace disjoint from all non-zero pairs (v, vP) where v covers vP

Remark: Diagonal matrices have Golay number m

Unimodular Sequences and Orthonormal Bases

$$\Phi = \frac{1}{\sqrt{N}} \sum_{v} \lambda_v e_v$$

Proposition: Vectors $D(0,b)\theta$ form an orthonormal basis if and only if $|\lambda_v| = 1$ for all $v \in \mathbb{Z}_2^m$

Proof: Moyal's Identity gives

$$|(\theta, e_v)|^2 = \frac{1}{N} = \frac{1}{N} \sum_{a,b} \overline{A_\theta(a,b)} A_{e_v}(a,b)$$

$A_\theta(a,b)$:

1	

$A_{e_v}(a,b)$:

*	0
1	

Hence $A_\theta(a,b) = (\theta, D(0,b)\theta) = 0$

The Geometry of Phase Coded Waveforms with the Golay Property

Proposition: θ and φ are a Golay pair if and only if

$$|(x,\theta)|^2 + |(x,\varphi)|^2 = \frac{2}{\sqrt{N}}$$

where x is any vector in any orthonormal basis associated with a diagonal maximal commutative subgroup X_Q

Remark: Q has Golay number m, so x is as far from Golay as is possible.