Existence Tests for Binary Complementary Code Sets Using Code Imbalance

Greg Coxson (Coxson Associates)
Bill Haloupek (Raytheon, retired)
Jon Russo (Lockheed Martin ATL, Cherry Hill, NJ)

Algebraic Combinatorics Seminar
Mathematics Department, Colorado State University
14 November 2014

Overview

- Pulse compression and low sidelobes
- Binary Complementary Code Sets
- A Useful Matrix Formulation
- An Existence Condition
    - The Case of Even Length
        - Example
    - The Case of Odd Length
        - Example
- Refining the Existence Condition
    - Examples

An Early Radar Trade-Off

Assuming a radar pulse has fixed transmit power:

Wide pulse:

- Longer range (high "energy on the target").
- Lower ability to resolve closely-spaced targets.

Narrow pulse:

- Greater ability to resolve closely-spaced targets.
- Limited range (limited "energy on the target").

Early Radar designers wanted a signal that would yield both long range and ability to resolve closely spaced objects.

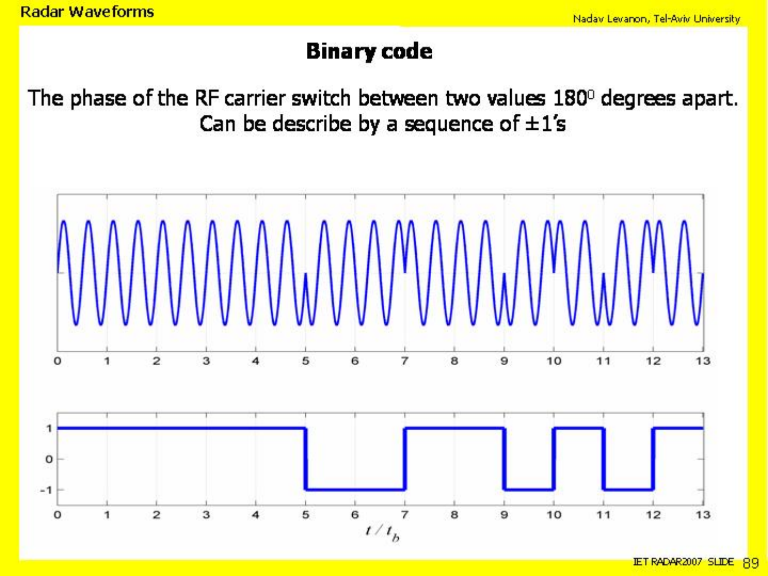
The solution: Pulse compression.

Pulse Compression

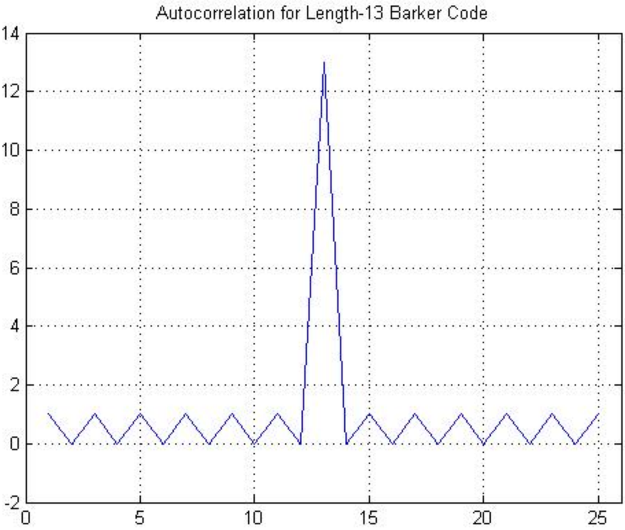
- Divide each pulse into N equal-width subpulses.
- Apply sequence of N multiplicative factors 1 and -1 (equivalently, phases changes of 0 and 180 degrees; this is often called "phase coding").
- Transmit the result.
- On receive, apply "matched filter" using the same "code".

(Result: a long pulse is effectively "compressed" into a narrow spike at the target range)

Phase Coding Illustrated



Matched Filter Output For a Code of Length 13



Some Definitions and Notation

Let x represent an N-length binary sequence ("code"):

$$x = \{x_1, \ldots, x_N\}$$

where $x_i = \pm 1$ for $i = 1, \ldots, N$.

The (aperiodic) **autocorrelation** of binary code x is the Matched (or North) filter response, and is given by:

$$\mathrm{ACF_x} = \mathrm{x} * \overline{\mathrm{x}}$$

where $*$ is aperiodic convolution and $\overline{x}$ is the reversal of x.

If x has length N, then $\mathrm{ACF_x}$ is a sequence of length $2N - 1$.

Autocorrelation Peak and Sidelobes

The **peak** of $\mathrm{ACF_x}$ is $\mathrm{ACF_x(N) = N.}$

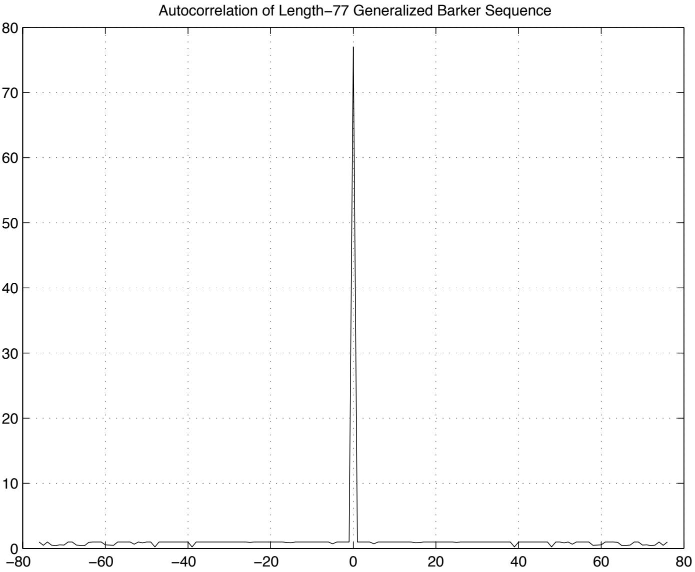
A bit of an annoyance – along with this high peak, the autocorrelation often has unwanted "sidelobes".

Sidelobe k can be found as:

$$\mathrm{ACF_x(k)} = \Sigma_{\mathrm{i=1}}^{\mathrm{N-|N-k|}} \mathrm{x_i x_{i+|k-N|}}$$

for any $k = 1, \ldots, N-1, N+1, \ldots, 2N-1.$

Length-77 Generalized Barker Sequence



A Useful Metric – the PSL

Define for any binary ± 1 codes x, the “peak sidelobe level”:

$$\mathrm{PSL_x} = \max_{\mathrm{k} \neq \mathrm{N}} |\mathrm{ACF_x(k)}|.$$

Code Imbalance

Given a length-N binary code x, its **imbalance** λ_x is the difference between the number of 1 and -1 elements.

It is easy to see that

$$\lambda_x = \sum_{i=1}^{N} x_i.$$

Example:

For $x = \{\ 1 \quad 1 \quad -1 \quad 1\ \}$,

$$\lambda_x = 3 - 1 = 2 = \sum_{i=1}^{N} x_i.$$

Note:

- Imbalance λ_x has the same parity as N.
- Codes with 0 imbalance are said to be **balanced**.

Complementary Sets – Motivation

For any binary ± 1 codes x, PSL_x can never be smaller than 1.

(Reason: the two outermost sidelobes equal $x_1 x_N$, which has magnitude 1).

In radar design, there are ways to get around this fundamental truth. Examine the assumptions:

- Use of a Matched filter
- Use of a single code.

A Lightbulb Goes Off

How about ..

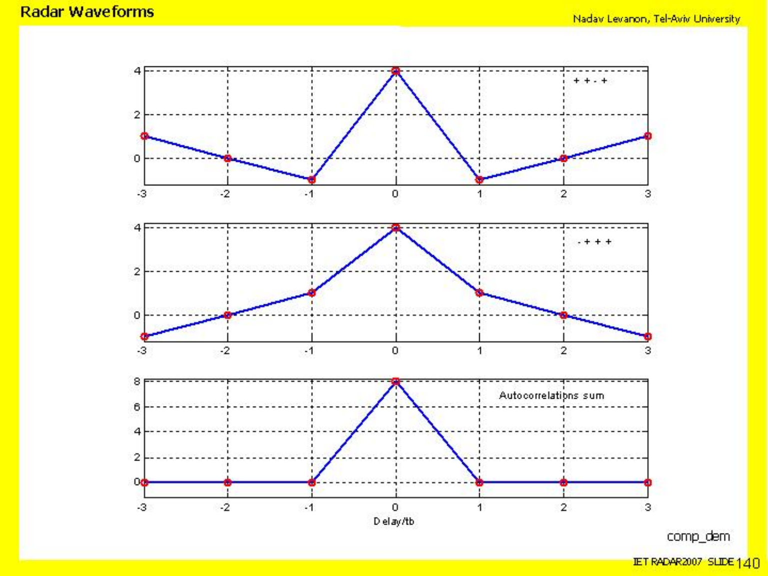
.. instead of one binary code ..

.. use TWO binary codes ..

.. whose autocorrelations sum to give zero sidelobes?

This is the idea behind **Golay Complementary Pairs**.

Complementary Code Pairs Illustrated



Complementary Code Sets

A set of K length-N binary codes $\{x_1, x_2, \ldots, x_K\}$ is a **complementary code set** if

$$\sum_{i=1}^{K} \mathrm{ACF_{x_i}(k)} = 0$$

for all $k \neq N$.

(In other words, the autocorrelation sequences of all K codes sum in such a way that ALL sidelobe sums vanish)

The (N, K) binary complementary code sets are those having K codes of length N.

Marcel Golay

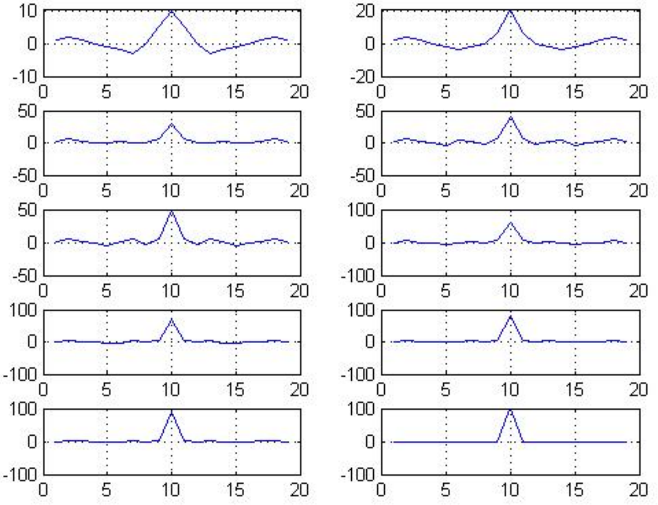
Complementary Code Pairs ($K = 2$) were discovered in 1949 by the Swiss physicist M.J.E. Golay to solve a problem in infrared spectrometry.

Golay focused mainly on binary complementary pairs (known as Golay pairs).

Complementary code sets exist containing more than two codes.

- Note: a set containing multiple complementary pairs (of the same length) remains complementary.
- But there exist sets of more than two codes that cannot be formed that way.
  - These might be called primitive or irreducible complementary code sets

Example of Primitive Complementary Set of 10 Codes



Toward a Useful Matrix Formulation

Consider the $N \times N$ outer product of a code x with itself:

$$xx^T = \begin{pmatrix} 1 & x_1x_2 & \dots & x_1x_N \\ x_2x_1 & 1 & \dots & x_2x_N \\ \vdots & \vdots & \ddots & \vdots \\ x_Nx_1 & x_Nx_2 & \dots & 1 \end{pmatrix}$$

- The peak of $\mathrm{ACF_x}$ is the sum of the main diagonal of xx^T.
- Sidelobe $\mathrm{ACF_x(k)}$ is the sum of the k^{th} diagonal from the main diagonal of xx^T for $k = 1, \dots, N-1$.

Given a set of K binary codes of length N,

$$\{x_1, x_2, \ldots, x_K\},$$

sum their outer products:

$$W = \sum_{i=1}^{K} W_i = \sum_{i=1}^{K} x_i x_i^T.$$

Given any diagonal other than the main diagonal, the sum of its elements is equal to the sum of the corresponding sidelobes of $\mathrm{ACF}_{\mathrm{x_i}}$ for $i = 1 \ldots, K$.

This sum may be written as a matrix product $W = QQ^T$ where

$$Q = \begin{pmatrix} x_1 & x_2 & \ldots & x_K \end{pmatrix}$$

Terminology and a Key Equivalence

The **row Gramian** of an $N \times K$ matrix Q is QQ^T.

A matrix W whose off-diagonals sum to zero is called **diagonally regular**.

An $N \times K$ matrix Q is a **Complementary Code Matrix** (CCM) if and only if its row Gramian $QQ^T = W$ is diagonally regular.

One-to-One Relationship

- (N, K) binary complementary code set

$$\{x_1, x_2, \ldots, x_K\}$$

- $N \times K$ binary complementary code matrix (CCM)

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_K \end{pmatrix}$$

Example

Consider the 5×4 binary matrix

$$Q = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

The row Gramian of Q is

$$QQ^T = \begin{bmatrix} 4 & 4 & 0 & 0 & 0 \\ 4 & 4 & 0 & 0 & 0 \\ 0 & 0 & 4 & -4 & 0 \\ 0 & 0 & -4 & 4 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix},$$

easily seen to be diagonally regular. Hence Q is a CCM.

Example, Continued

The four length-5 column vectors of Q form a (binary) complementary code set. Computing the autocorrelations of the columns in order yields the following four length-9 autocorrelation sequences:

$\mathrm{ACF}_{\mathrm{x}_1}$	$\mathrm{ACF}_{\mathrm{x}_2}$	$\mathrm{ACF}_{\mathrm{x}_3}$	$\mathrm{ACF}_{\mathrm{x}_4}$	$\sum_{k=1}^{4} \mathrm{ACF}_{\mathrm{x}_\mathrm{k}}$
1	-1	-1	1	0
0	0	-2	2	0
1	1	-1	-1	0
0	-2	2	0	0
5	5	5	5	20
0	-2	2	0	0
1	1	-1	-1	0
0	0	-2	2	0
1	-1	-1	1	0

An Important Special Case

A binary $N \times N$ matrix Q for which

$$QQ^T = NI_{N\times N}$$

is a binary **Hadamard matrix**.

Clearly, every binary Hadamard matrix is a binary CCM. The transpose of a binary Hadamard is a CCM as well, so both the set of rows and the set of columns are complementary code sets.

Note that Hadamard matrices are square, while CCMs can be $N \times K$ where $N \neq K$.

Operations Preserving CCM Property

Theorem 1. Suppose that M is an $N \times K$ binary CCM. Then the following operations preserve the CCM property and dimensions of the matrix:

(i) Take any column x of M and replace it with $-x$.

(ii) Take any column x of M and replace it with its reversal $\overline{x}$.

(iii) Form the product AM, where

$$A = \mathrm{Diag}([-1, 1, \ldots, (-1)^{\mathrm{N}}])$$

(iv) Form MP for P any $K \times K$ permutation matrix.

A First Existence Condition

Theorem 2. Suppose Q is an $N \times K$ binary CCM. Then K is even.
Proof.
Let W be the $N \times N$ Row Gramian QQ^T. Then:

- W_{1n} and W_{n1} are the only elements on their diagonals.
- $W_{1n} = W_{n1} = 0$.
- W_{1n} and W_{n1} are inner products of $1 \times K$ rows of Q.
- W_{1n} and W_{n1} are sums of K ones and minus ones.
- K must be even.

Corollary. Any binary complementary code set contains an even number of codes.

An Existence Condition of Feng et. al.

Theorem 3 (Feng *et al* [2]). A necessary condition for existence of an (N, K) binary complementary code set is that $NK = 0 \mod 4$.

If we combine this with necessity that K be even, we conclude:

- If $K \equiv 2 \mod 4$, then N must be even as well.
- If $K \equiv 0 \mod 4$, then N can be either even or odd.

Golay discovered the following corollary in 1961 [1]:

Corollary. There exist no Golay pairs with odd length.

Theorem 4. Let Q be an $N \times K$ Complementary Code Matrix. Then

$$NK = \sum_{i=1}^{K} \lambda_i^2$$

for some set of integers λ_i, $i = 1, \ldots, K$.

Proof.

Let e_N be the $N \times 1$ vector of ones. Since $W = QQ^T$ is diagonally regular,

$$NK = (e_N^T W e_N) = e_N^T (QQ^T) e_N = (Q^T e_N)^T (Q^T e_N) = \sum_{i=1}^{K} \lambda_i^2,$$

where λ_i represents the imbalance of column i, for $i = 1, \ldots, K$).

A Sufficient Condition for Golay Pair Existence

Theorem 5 (Jedwab and Parker [3]) CCMs exist for $(N, 2)$ whenever $N = 2^a 10^b 26^c$, for any nonnegative integers a, b, c.

Borwein and Ferguson [4] – exhaustive search for $(N, 2)$, $N < 100$.

- Lengths $N < 100$ allowed by necessary conditions ((1) even $N > 1$; (2) $2N$ is the sum of $K = 2$ integers squared):

$$\{1, 2, 4, 10, 16, 20, 26, 32, 34, 40, 50, 52, 58, 64, 68, 74, 80, 82\}$$

- Lengths $N < 100$ yielding Golay pairs by exhaustive search:

$$\{1, 2, 4, 10, 16, 20, 26, 32, 40, 52, 64, 80\}$$

This is precisely the set of $N < 100$ of the form $N = 2^a 10^b 26^c$. (Hence the condition in Theorem 5 is both necessary and sufficient for $K = 2$ and $1 \le N < 100$).

Non-Golay ($K \geq 4$)

Theorem 6 (LaGrange, 1869) Any positive integer can be written as the sum of four squares.

Note that for $K > 4$, we can always pad with $K - 4$ zeros and get a K-length representation.

Adding a Parity Constraint

The waveform designer often knows the parity of N. This is also the parity of the imbalance of every code in a complementary set. So for given (N, K), we really want to know:

- If N is **even**, how many representations of NK are there as sums of K squares of **even** integers?
- If N is **odd**, how many representations of NK are there as a sum of K squares of **odd** integers?

Let's consider these two questions in turn ..

The Case of N Even

Suppose both N and K are even. Then $N = 2M$ and $K = 2L$ for integers M and L.

The necessary condition for existence of an (N, K) binary CCM reduces to

$$4ML = \sum_{i=1}^{K} (2k_i)^2,$$

or equivalently:

$$ML = \sum_{i=1}^{K} (k_i)^2.$$

This is now the familiar sum of squares representation, where there is no constraint on parity.

Define:

- $r_K(ML)$: number of representations of ML using K squares
- $d_i(ML)$: number of divisors of ML congruent to $i \bmod 4$.

Cooper and Hirschhorn (2007) [5] offer tallies for even K from 2 to 12; here are the first four:

- K=2: $r_2(ML) = r_2(M) = 4(d_1(M) - d_3(M))$.
- K=4: $r_4(ML) = r_4(N) = \left(8\sum_{d|N} d\right) - \left(32\sum_{d|(N/4)} d\right)$.
- K=6: $r_6(ML) = r_6(3M) = 4\sum_{\substack{de=3M \\ d \ \ odd}} (-1)^{(d-1)/2}(4e^2 - d^2)$.
- K=8:
  $r_8(ML) = 16\left[\sum_{d|(2N)} d^3 - 2\sum_{d|N} d^3 + 16\sum_{d|(N/2)} d^3\right]$.

($d|N$ means that d is a divisor of N).

A Pause to Reflect

These enumeration formulae apply to **allowable** code imbalance combinations.

There remains work in enumerating imbalance combinations yielding matrices that satisfy the CCM property.

Example

Example. Let $N = 8$ and $K = 4$. The number of ways to represent $NK = 32$ as the sum of 4 even squares is the same as the number of ways to represent $ML = 8$ as the sum of 4 squares (without regard to parity). The appropriate formula gives:

$$r_4(8) = \left(8 \sum_{d|8} d\right) - \left(32 \sum_{d|(8/4)} d\right)$$

or

$$r_4(8) = (8)(1 + 2 + 4 + 8) - (32)(1 + 2) = 24.$$

This tally agrees with the count of six distinct reorderings of each of the four combinations $(k_1, k_2, k_3, k_4) = (\pm 2, \pm 2, 0, 0)$.

Hence, any complementary set of 4 length-8 codes must contain two balanced codes and two codes with imbalance ± 2.

Assume that N is odd (and K even).

By Theorem 3 (Feng et al):

- If $K \equiv 2 \mod 4$, there exist **no** (N,K) binary CCMs.
- If $K \equiv 0 \mod 4$, (N,K) binary CCMs are possible.

So we are interested in representations of NK as sums

$$NK = \sum_{i=1}^{K} n_i^2$$

where N is odd, $K = 4j$ for some integer j, and n_i is **odd** for $i = 1, \ldots, K$.

An Observation

Let n be a given odd positive integer. Then

$$n = 2k + 1$$

for some integer k; then:

$$n^2 = (2k+1)^2 = 8(k^2 + k)/2 + 1,$$

Let

$$t_k = 1 + 2 + 3 + \ldots + k = (k)(k+1)/2.$$

(that is, the k^{th} "triangular number").

This is great! n^2 is linearly related to the t_k:

$$n^2 = 8t_k + 1.$$

Necessary Condition Reformulated for Odd N

Theorem 7 If an (N, K) binary complementary code set $\{x_1, x_2, \ldots, x_K\}$ exists for K even and N an odd integer, then

$$NK = \sum_{i=1}^{K}(1 + 8t_{k_i}) = K + 8\sum_{i=1}^{K} t_{k_i}$$

for some set of K triangular numbers $\{t_{k_1}, t_{k_2}, \ldots, t_{k_K}\}$.

Recent Work on Representations as the sum of triangular numbers:

Ono *et. al.* (1995) [6]: formulae for several even $K \geq 4$ (4, 6, 8, 12 and 24).

(Note that any formula for $K = 6$ is a curiosity only, since no CCMs exist for $K = 6$ when N is odd).

Atanasov *et. al.* (2008) [7]: extends enumeration formulae in Ono *et. al.* for $K \geq 4$, when K divisible by 4, to asymptotic formulae. (This is published in an undergraduate research journal)

Also see the 2003 paper by Zhi-Guo Liu [8].

$K = 4$, Odd N

Assume $K = 4$ and $N - 1 = 2M$ for some integer M. Then we are interested in the number of representations

$$M = \sum_{i=1}^{4} t_{k_i}$$

where the t_{k_i} are triangular numbers.

Using Ono et al [6], the number of possibilities is

$$\delta_4(M) = \sigma_1(1 + 2M) = \sum_{d|(1+2M)} d = \sum_{d|N} d.$$

(the subscript 1 on σ indicates that the divisor is raised to the first power).

The sum is taken over **distinct divisors**

- **Example**: for $N = 9$, the sum of divisors is

$$\sum_{d|N} d = 1 + 3 + 9 = 13.$$

An Extra Step

Recovering imbalance values from triangular numbers involves a square root, so an extra factor of 2^K is needed to find the number of imbalance combinations.

For $K = 4$ and odd N, the number of possible column imbalance combinations is $(2^K)(\sum_{d|N} d) = (16)(\sum_{d|N} d)$.

$\diamond$ The formulae for $K = 4L$, $L > 1$, get more complicated.

Example

Let $K = 4$ and $N = 7$.

The divisor sum of N is $\sum_{d|7} d = 1 + 7 = 8$.

Each representation as a sum of triangular numbers has the form

$$NK = (4)(7) = 28 = \sum_{i=1}^{4} (1 + 8t_{k_i})$$

or

$$3 = \sum_{i=1}^{4} t_{k_i}.$$

Example, Continued

Eight possibilities for representing 3 as a sum of triangular numbers (here we allow 0 as the "first triangular number"):

- $(3, 0, 0, 0)$ and cyclic shifts (4 possibilities)
- $(1, 1, 1, 0)$ and cyclic shifts (4 possibilities).

Converting from triangular numbers to imbalance values:

- $(\pm 5, \pm 1, \pm 1, \pm 1)$ and cyclic shifts
- $(\pm 3, \pm 3, \pm 3, \pm 1)$ and cyclic shifts.

Hence, each of the eight solutions represents $2^4 = 16$ possible imbalance combinations, for a total of 128 possibilities for CCMs.

A Refinement of the Sum-of-Squares Existence Condition

Given a binary code $x = \{x_1, x_2, \ldots, x_N\}$, define :

- x_e: the code formed from the elements of x with even indices
- x_o: the code formed from the elements of x with odd indices

Representing the imbalance values as λ_{x_e} and λ_{x_o}, then

$$\lambda_x = \lambda_{x_e} + \lambda_{x_o}.$$

Example: Given $x = [\ -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad -1\ ]$, $(N = 6)$

- $x_e = [\ 1 \quad 1 \quad -1\ ]$ having imbalance $\lambda_e = 2 - 1 = 1$
- $x_o = [\ -1 \quad -1 \quad -1\ ]$ having imbalance $\lambda_o = 0 - 3 = -3$
- The imbalance of x is $\lambda_x = \lambda_{x_o} + \lambda_{x_e} = 1 - 3 = -2$.

A Refashioned Necessary Condition

Theorem 8. Given (N, K) binary complementary code set comprised of codes x_i having imbalance λ_{x_i}, with even-index subcode $(x_i)_e$ and odd-index sub-code $(x_i)_o$ having imbalance values $\lambda_{(x_i)_e}$ and $\lambda_{(x_i)_o}$ respectively, then

$$NK = \sum_{i=1}^{K} \lambda^2_{(x_i)_e} + \sum_{i=1}^{K} \lambda^2_{(x_i)_o}$$

and

$$0 = \sum_{i=1}^{K} (\lambda_{(x_i)_e} \lambda_{(x_i)_o}).$$

Since binary Hadamard matrices are binary CCMs, Theorem 8 means that for an $N \times N$ binary Hadamard matrix to exist, there must be:

- N-length vectors E and O with even integer elements where N is a multiple of 4 (binary Hadamard matrix orders are constrained to 1,2 and multiples of 4).
- E and O are orthogonal vectors
- E and O form the sides of a right triangle with hypotenuse length N.

The existence of binary Hadamard matrices of order 668 remains an open question. (Weekend puzzler for Anton Betten: prove there is no order-668 binary Hadamard matrix, and thereby disprove the **Hadamard Conjecture**)

Proof of Theorem 8

If $\{x_1, x_2, \ldots, x_K\}$ is an (N, K) binary complementary set, then

$$NK = \sum_{i=1}^{K} \lambda_{x_i}^2 = \sum_{i=1}^{K} (\lambda_{(x_i)^e} + \lambda_{(x_i)^o})^2.$$

Expanding the square:

$$NK = \sum_{i=1}^{K} \lambda_{(x_i)^e}^2 + \sum_{i=1}^{K} \lambda_{(x_i)^o}^2 + 2\sum_{i=1}^{K} (\lambda_{(x_i)^e} \lambda_{(x_i)^o}). \tag{1}$$

Suppose the sign of every other element of each code is changed

- CCM property is preserved, by Theorem 1(iii).
- The sign of either $\lambda_{(x_i)^e}$ or $\lambda_{(x_i)^o}$ changes, for $i = 1, \ldots, K$, but equation (1) still applies.
- It follows that $0 = \sum_{i=1}^{K} (\lambda_{(x_i)^e} \lambda_{(x_i)^o})$.

This establishes the result.

Example

The example will use a $(15, 4)$ CCM found by Exhaustive Search.

Note:

- By Golay's Corollary to Theorem 3, there exist no Golay Pairs (i.e., K=2) with odd length N.
- It was unclear before our search whether there were any CCMs of odd length N and $K > 2$
- Exhaustive search yielded (15,4) binary CCMs quickly
  - $\rightarrow$ these beasts exist (and might not be that rare)

Example – a $(15, 4)$ Binary CCM

code 1	code 2	code 3	code 4
1	1	-1	-1
1	1	-1	-1
1	-1	1	-1
-1	-1	1	1
1	-1	1	-1
-1	1	1	1
1	-1	1	-1
1	-1	-1	1
-1	1	1	-1
1	-1	-1	-1
1	-1	-1	1
1	1	1	1
-1	-1	-1	-1
-1	-1	-1	-1
-1	-1	-1	-1

Example Continued – Autocorrelation Sidelobes

code 1	code 2	code 3	code 4	Sum
-1	-1	1	1	0
-2	-2	2	2	0
-3	-1	1	3	0
0	2	-2	0	0
1	3	-3	-1	0
4	-2	0	-2	0
-1	1	-3	3	0
0	2	-2	0	0
-1	1	-1	1	0
2	0	-2	0	0
-1	1	-3	3	0
-2	4	2	-4	0
1	-3	1	1	0
0	0	2	-2	0

Example Continued – The Subcode Conditions

The example $(15, 4)$ complementary code set represents sub-code imbalance combinations

$$\{(2,1), (-4,-1), (0,-1), (-6,1)\}$$

The set satisfies the two conditions in Theorem 6:

$$\begin{aligned} NK = (15)(4) = 60 &= (2^2 + (-4)^2 + 0^2 + (-6)^2) \\ &\quad +(1^2 + (-1)^2) + (-1)^2) + 1^2) \\ &= \sum_{i=1}^{4} \lambda^2_{(x_i)^e} + \sum_{i=1}^{4} \lambda^2_{(x_i)^o} \end{aligned}$$

and

$$\begin{aligned} 0 &= (2)(1) + (-4)(-1) + (0)(-1) + (-6)(1) \\ &= \sum_{i=1}^{4} (\lambda_{(x_i)_e} \lambda_{(x_i)_o}) \end{aligned}$$

Golay Subcode Imbalance Combinations for $N < 100$

N	(λ_1, λ_2)	**Sub-code Imbalance Combinations**
1	(1,1)	$\{(\pm 1, 0), (0, \pm 1)\}$
2	(2,0)	$\{(\pm 2, 0), (0, 0)\}$, $\pm\{(1, 1), (1, -1)\}$
4	(2,2)	$\{(\pm 2, 0), (0, \pm 2)\}$
10	(4,2)	$\{(\pm 4, 0), (0, \pm 2)\}$, $\pm\{(3, 1), (1, -3)\}$
16	(4,4)	$\{(\pm 4, 0), (0, \pm 4)\}$
20	(6,2)	$\{(\pm 6, 0), (0, \pm 2)\}$, $\pm\{(4, 2), (2, -4)\}$
26	(6,4)	$\{(\pm 6, 0), (0, \pm 4)\}$, $\pm\{(5, 1), (1, -5)\}$
32	(8,0)	$\{(\pm 8, 0), (0, 0)\}$, $\pm\{(4, 4), (4, -4)\}$
40	(8,4)	$\{(\pm 8, 0), (0, \pm 4)\}$, $\pm\{(6, 2), (2, -6)\}$
52	(10,2)	$\{(\pm 10, 0), (0, \pm 2)\}$, $\pm\{(6, 4), (4, -6)\}$
64	(8,8)	$\{(\pm 8, 0), (0, \pm 8)\}$
80	(12,4)	$\{(\pm 12, 0), (0, \pm 4)\}$, $\pm\{(8, 4), (4, -8)\}$

Summary

- CCMs provide a useful matrix formulation for complementary code sets.
- A necessary condition for existence of (N, K) binary complementary sets in terms of code imbalance values yields enumeration of possible imbalance combinations.
- The Number Theory on which these existence and enumeration tests are based is still developing
- It is possible to identify possible structures of (N, K) binary complementary sets in terms of combinations of half-code imbalance values
- Although there exist no odd-length Golay pairs, it appears that complementary sets of odd-length binary codes with more than two codes can be found readily using computational search.

References

- 1. Golay, M.J.E. (1961). "Complementary series", *IRE Trans. Inform. Theory*, vol. 7, pp. 82-87.
- 2. Feng, K., Shiue, P. J.-S., and Xiang, Q., "On aperiodic and periodic complementary binary sequences," *IEEE Transactions on Information Theory*, vol. 45, no. 1, pp. 296-303, 1999.
- 3. Jedwab, J. and Parker, M.G., "Golay complementary array pairs," *Des. Codes Cryptogr.*, vol. 44, pp. 209-216, 2007.
- 4. Borwein, P. and Ferguson, R., "A complete description of Golay pairs for lengths up to 100," *Mathematics of Computation*, vol. 73, pp. 967-985, 2004.
- 5. Cooper, S. and Hirschhorn, M., "On the number of primitive representations of integers as sums of squares," *Ramanujan Journal*, vol. 13, pp. 7-25, 2007.

More References

- 6. Ono, K., Robins, S., and Wahl, P.T.. “On the representation of integers as sums of triangular numbers,” *Aequationes Mathematicae*, vol. 50, pp. 73-94, 1995.
- 7. Atanasov, A., Bellovin, R., Lougman-Pawelko, I, Peskin, L. and Potash, E., “An asymptotic for the representation of integers as sums of triangular numbers,” *Involve – A Journal of Mathematics*, vol. 1, no. 1, 2008.
- 8. Liu, Z.-G., ”An identity of Ramanujan and the representation of integers as sums of triangular numbers,” *Ramanujan Journal*, vol. 7, no. 4, pp. 407-434, 2003.