Intersections of Golay codes with higher order Kerdock codes

Mohammed Abouzaid Nick Gurski

July 20, 1999

Abstract

Golay codewords are useful for transmission schemes such as OFDM, and [MacWilliams/Sloane] demonstrated that these codewords are bent functions contained in second order Reed-Muller codes. This paper investigates the intersection between these codes and Kerdock-like codes.

1 Introduction

1.1 Purpose

This paper examines the union of cosets of first order Reed-Muller in the second order Reed-Muller code. One version of the Nordstrom-Robinson Code contains six cosets with Golay cosets and this example motivates the work done in this paper. We investigate collections of Golay cosets, the sum of whose elements is always bent, and try to maximize the number of cosets that have Golay representatives. The fact that the sum of any two codewords is bent guarantees a minimum distance between any two codewords, and thus a set error correcting capability, while the presence of a maximum number of Golay codewords minimizes the power profile of the code when transmitted.

The two cases of length 2^6 and 2^8 are examined in this paper. The paper attempts to solve the problem from two perspectives. By using the property that the Kerdock code, which is linear in $\mathbb{Z}_4$, can be expressed in binary as a union of cosets with the property that the sum of any two codewords is bent, the number of these cosets that had quadratic Golay representatives was maximized. From another perspective, quadratic Golay codewords were generated with the condition that the sum of the codewords was bent.

1.2 Background

1.2.1 Reed-Muller Codes

Reed-Muller codes are binary linear codes. A binary linear code is the row space of a particular generator matrix. The generator matrix for the first order Reed-Muller codes of length 2^m has $m+1$ rows. The first row is always $\mathbf{1}$, the all one codeword. The next row has 2^{m-1} 0's followed by 2^{m-1} 1's, and the ith row is written as 2^{m-i} 0's followed by 2^{m-i} 1's repeated i times. The generator matrix for the first order Reed-Muller code of length $2^4 = 16$ contains 5 rows:

$$\begin{array}{c} \mathbf{1} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

The Reed-Muller code of order r and length 2^m, $\mathcal{R}(r, m)$, has a generator matrix that includes all the vectors in the generator matrix of the first order Reed-Muller code of the same length and all the products of these basis vectors up to order r. For example, the generator matrix for $\mathcal{R}(2, 4)$ includes all possible linear and quadratic

terms:

$$\begin{array}{c} \\ \mathbf{1} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_1v_2 \\ v_1v_3 \\ v_1v_4 \\ v_2v_3 \\ v_2v_4 \\ v_3v_4 \end{array} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Theorem 1 *The properties of the $\mathcal{R}(r,m)$, $0 \leq r \leq m$, are as follows:*
Each codeword has length $n = 2^m$.
The minimum distance between codewords is $d = 2^{m-r}$.
The number of codewords is $2^{\sum_{i=0}^{r} \binom{m}{i}}$.
Let $\mathbf{v}_i$ denote the ith row of the generator matrix of $\mathcal{R}(1,m)$. Any codeword in $\mathcal{R}(1,m)$ can be written

$$u_0\mathbf{1} + \sum_{i=1}^{m} u_i\mathbf{v}_i$$

or as a linear combination of these rows $\mathbf{v}_i$ such that $u_i \in \{0,1\}$.

Proof: For proof of these properties, consult [MacWilliams/Sloane]. □

There are many codes that, while they may look different, have the same properties (such as length and minimum distance between codewords) as the Reed-Muller code. All of these codes are equivalent. For our purposes, we only consider the Reed-Muller code as we have defined it, and it is important that the codewords and generator matrix be exactly as we have constructed them.

1.2.2 Boolean functions

Let $v = (v_1, ..., v_m)$ be the set of all binary m-tuples. A Boolean function is any function $f(v) = f(v_1, ..., v_m)$ that takes on the values of either 0 or 1 for each v. A Boolean function can be represented by a truth table which shows the value of f at each of its $n = 2^m$ positions. The binary vector $\mathbf{f}$ is a vector of length $n = 2^m$ that shows all the values of f.

A Boolean function can also be represented by a polynomial of the terms $v_1, ..., v_m$. The following theorem, see [Dillon] for details, gives an algorithm for finding that polynomial.

Theorem 2 *Every Boolean function*

$$f : F^n \mapsto F$$

is given by a unique reduced polynomial

$$f(v) = \sum_{x \in F^m} g(x) v_1^{x_1} v_2^{x_2} \dots v_n^{x_n}$$

in the n coordinate variables $v_1, v_2, \dots, v_n$. *Where*

$$g(x) = \sum_{u \subset x} f(u), \text{ for all } x \in F^m,$$

and $u \subset v$ *means* $u_i = 1 \Rightarrow v_i = 1, i \leq n$.

1.2.3 Hadamard transforms

A Hadamard matrix of order n is an $n \times n$ matrix of ± 1's such that

$$HH^T = nI$$

or any two distinct rows are orthogonal and the dot product of a row with itself is n. Multiplying any row or column by -1 changes a Hadamard matrix into another Hadamard matrix. Thus it is possible to normalize any Hadamard matrix by multiplying rows and columns by -1 to change the first row and column to all $+1$'s; this is called the normalized Hadamard matrix. Normalized Hadamard matrices of orders 1, 2, 4 are shown below, with $-$ substituted for -1.

$$H_1 = (1) \qquad H_2 = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}$$

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{pmatrix}$$

These Hadamard matrices are of a special class called Sylvester matrices. A Sylvester matrix is any Hadamard matrix such that

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

is a Hadamard matrix of order $2n$.

Lemma 3 *If* $n = 2^m$ *and* $u_1, ..., u_n$ *are all the distinct binary m-tuples, the matrix* $H = (h_{ij})$ *where* $h_{ij} = (-1)^{u_i \cdot u_j}$ *is a Sylvester matrix of order n.*

Proof: We proceed by induction on m. When $m = 1$, the matrix H is

$$H = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}$$

or the Sylvester matrix H_{2^1} or H_2. Assume that the statement is true for all binary m-tuples. Now consider the matrix generated from the binary $(m+1)$-tuples. The set of $(m+1)$-tuples is the union of the sets of 0 concatenated with each m-tuple and 1 similarly concatenated. Thus the dot product of any $(m+1)$-tuple is the sum of the dot products of the original m-tuples and the dot product of the concatenated elements. The dot product of the $(m+1)$-tuples will be the same as the dot product of the m-tuples provided that one of the concatenated elements is a 0. Only when both concatenated elements are 1 will be dot products be changed, and then they will all be one greater than the original dot products of the m-tuples, changing the sign of each element of the matrix H that corresponds to these $(m+1)$-tuples. These sign changes all occur in the lower-right quarter of the matrix $H_{2^{m+1}}$. Thus the matrix is

$$H_{2^{m+1}} = H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

or the Sylvester matrix of order $2n$. □

Given a real vector $X = (x_1, ...x_n)$ and a Hadamard matrix of order n, the Hadamard transform of X is

$$\hat{X} = XH.$$

Let F^m be the set of binary m-tuples. The entries $(-1)^{u \cdot v}$, for $u, v \in F^m$, form a Hadamard matrix of order $n = 2^m$. If f is a Boolean function defined on F^m, its Hadamard transform $\hat{f}$ is

$$\hat{f}(u) = \sum_{v \in F^m} (-1)^{u \cdot v} f(v), u \in F^m.$$

It is convenient to have a method of writing a real vector obtained from the binary vector by replacing all 1's with -1's and all 0's with $+1$'s. The component of this real vector F in the position corresponding to u is $F(u) = (-1)^{f(u)}$. The Hadamard transform of this vector F is

$$\begin{aligned} \hat{F}(u) &= \sum_{v \in F^m} (-1)^{u \cdot v} F(v), u \in F^m \\ &= \sum_{v \in F^m} (-1)^{f(v) + u \cdot v} \end{aligned}$$

The distribution of the weights of codewords in cosets of $\mathcal{R}(1, m)$ is structured. For instance, all codewords in the zero coset of $\mathcal{R}(1, 4)$ are weight 8 since this

coset is really just the Reed-Muller code itself. Other cosets have structured weight distributions as well. As an example, the coset of $\mathcal{R}(1,4)$ with coset representative $v_1v_2 + v_2v_3 + v_3v_4$ contains codewords of weight 6 and weight 10 only, evenly divided between the two weights.

Theorem 4 *The weight distribution of the coset of* $\mathcal{R}(1,m)$ *that contains* $\mathbf{f}$ *is*

$$\frac{1}{2}(2^m \pm \hat{F}(u)).$$

Proof: Consider the binary vector $\mathbf{f} + \sum_{i=1}^{m} u_i\mathbf{v}_i, u_i \in \{0,1\}$. The vth element of this vector is

$$f(v) + u_1v_1 + u_2v_2 + ... + u_mv_m = f(v) + \sum_{i=1}^{m} u_iv_i = f(v) + u \cdot v.$$

If $f(v) + u \cdot v = 0$, then $(-1)^{f(v)+u\cdot v} = 1$; if $f(v) + u \cdot v = 1$, then $(-1)^{f(v)+u\cdot v} = -1$. The sum

$$\sum_{v \in F^m} (-1)^{f(v)+u\cdot v}$$

is the Hadamard transform $\hat{F}(u)$ and is equal to the number of 0's $(f(v) + u \cdot v = 0)$ minus the number of 1's $(f(v) + u \cdot v = 1)$ in the vector $\mathbf{f} + \sum_{i=1}^{m} u_i\mathbf{v}_i$. The distance between two codewords is the number of positions in which the codewords differ, or equally the number of 1's in the sum of the two codewords. Thus

$$\texttt{dist}\left\{\mathbf{f}, \sum_{i=1}^{m} u_i\mathbf{v}_i\right\}$$

is the same as the number of 1's in their sum. Since there are 2^m elements in these vectors, to find the number of 0's minus the number of 1's we must subtract twice the distance between the two summed vectors from 2^m. Therefore

$$\hat{F}(u) = 2^m - 2\,\texttt{dist}\left\{\mathbf{f}, \sum_{i=1}^{m} u_i\mathbf{v}_i\right\}$$

or

$$\texttt{dist}\left\{\mathbf{f}, \sum_{i=1}^{m} u_i\mathbf{v}_i\right\} = \frac{1}{2}(2^m - \hat{F}(u)).$$

For the complement of the codeword $\mathbf{f} + \sum_{i=1}^{m} u_i\mathbf{v}_i$, $\mathbf{f} + \mathbf{1} + \sum_{i=1}^{m} u_i\mathbf{v}_i$, $\hat{F}(u)$ is the number of 1's minus the number of 0's. Thus

$$\hat{F}(u) = 2\,\texttt{dist}\left\{\mathbf{f}, \mathbf{1} + \sum_{i=1}^{m} u_i\mathbf{v}_i\right\} - 2^m$$

or

$$\texttt{dist}\left\{\mathbf{f}, \mathbf{1} + \sum_{i=1}^{m} u_i \mathbf{v}_i\right\} = \frac{1}{2}(2^m + \hat{F}(u)).$$

Since $\mathcal{R}(1,m)$ can be written as $u_0\mathbf{1} + \sum_{i=1}^{m} u_i\mathbf{v}_i, u_i \in \{0,1\}$, the minimum distance between the vector $\mathbf{f}$ and any codeword in $\mathcal{R}(1,m)$ is $\frac{1}{2}(2^m \pm \hat{F}(u)), u \in F^m$. $\square$

1.2.4 Bent Functions

A Boolean function $f(v_1, ..., v_m)$ is bent if the Hadamard transform coefficients are all $\hat{F}(u) = \pm 2^{m/2}$.
Example. Let $m = 2$ and $f(v_1, v_2) = v_1 v_2$, where the kth position of $\mathbf{f}$ is 1 if and only if the kth positions of v_1 and v_2 are both 1. The truth table for f is

$$\begin{array}{rcl} v_1 & = & 0\,0\,1\,1 \\ v_2 & = & 0\,1\,0\,1 \\ f & = & 0\,0\,0\,1 \end{array}$$

and the Hadamard transform coefficients, $\hat{F}(u) = \sum_{v \in F^m} (-1)^{f(v)+u\cdot v}$, are

$$\begin{array}{rcrcr} \hat{F}(0\,0) & = & 1+1+1-1 & = & 2 \\ \hat{F}(0\,1) & = & 1-1+1+1 & = & 2 \\ \hat{F}(1\,0) & = & 1+1-1+1 & = & 2 \\ \hat{F}(1\,1) & = & 1-1-1-1 & = & -2 \end{array}$$

Since each Hadamard transform coefficient is $\hat{F}(u) = \pm 2^{m/2} = \pm 2$, the function $f(v_1, v_2) = v_1 v_2$ is bent.

Theorem 5 *Let $h(u_1, ...u_m, v_1, ..., v_n) = f(u_1, ..., u_m) + g(v_1, ..., v_n)$. The function h is bent if $f(u_1, ..., u_m)$ is bent and $g(v_1, ..., v_n)$ is bent.*

Proof: Let $u \in F^m$ and $v \in F^n$ such that $w = (u, v)$ and $w \in F^{m+n}$. The Hadamard transform for h is

$$\hat{H}(w) = \sum_{t \in F^{m+n}} (-1)^{h(t)+w\cdot t}$$

where $t = (r, s)$, $r \in F^m$ and $s \in F^n$. The function $h(t)$ can be written as $h(r, s)$ or as the sum of two functions, $h(r, s) = f(r) + g(s)$; similarly, $w \cdot t = (u, v) \cdot (r, s) = u \cdot r + v \cdot s$. The sum is then

$$\hat{H}(w) = \sum_{r \in F^m} \left(\sum_{s \in F^n} (-1)^{f(r)+g(s)+u\cdot r+v\cdot s} \right)$$

$$
\begin{aligned}
&= \sum_{r\in F^m}\left(\sum_{s\in F^n}(-1)^{f(r)+u\cdot r}(-1)^{g(s)+v\cdot s}\right)\\
&= \left(\sum_{r\in F^m}(-1)^{f(r)+u\cdot r}\right)\left(\sum_{s\in F^n}(-1)^{g(s)+v\cdot s}\right)\\
&= \hat{F}(u)\hat{G}(v)
\end{aligned}
$$

and all the Hadamard transform coefficients for h are $\hat{H}(w) = \pm 2^{(m+n)/2}$. □

Corollary 6 *The function* $f(v_1, ..., v_m) = v_1v_2 + v_3v_4 + ... + v_{m-1}v_m$ *is bent for any even* $m \geq 2$.

Proof: The assertion follows clearly from Theorem 4 and the fact that v_1v_2 is bent. □

1.2.5 Cosets of First Order Reed-Muller

The first order Reed-Muller code, $\mathcal{R}(1, m)$, is a group under component-wise addition modulo 2. Cosets of $\mathcal{R}(1, m)$ are generated by adding a length $n = 2^m$ codeword to each codeword in $\mathcal{R}(1, m)$ component-wise modulo 2. Thus each coset can be written as

$$\mathbf{w} + \left(u_0\mathbf{1} + \sum_{i=1}^{m} u_i\mathbf{v}_i\right), u_i \in \{0, 1\}$$

We have already shown that the weight distribution of any coset of $\mathcal{R}(1, m)$ is determined by the Hadamard transform of a contained codeword $\mathbf{f}$. We shall now show that if $f(v)$ and $g(v)$ are affinely equivalent, that is $g(v) = f(Av+B)$ for some $m \times m$ binary matrix A and some binary m-tuple B, then the cosets of $\mathcal{R}(1, m)$ that contain $\mathbf{f}$ and $\mathbf{g}$ have the same weight distribution.

Theorem 7 *Let the Boolean functions* f *and* g *be related by* $g(v) = f(Av + B)$, *where* $v \in F^m$, A *is a binary invertible* $m \times m$ *matrix, and* B *is a binary* m*-tuple. The cosets of R(1,m) containing* $\mathbf{f}$ *and* $\mathbf{g}$ *have the same weight distribution.*

Proof: We prove that the sets $\{\pm\hat{G}(u) : u \in F^m\}$ and $\{\pm\hat{F}(u) : u \in F^m\}$ are equal since the weight distributions of the two cosets is determined by the Hadamard transforms of the functions. Since $g(v) = f(Av + B)$,

$$
\begin{aligned}
\hat{G}(u) &= \sum_{v\in F^m}(-1)^{u\cdot v}G(v)\\
&= \sum_{v\in F^m}(-1)^{u\cdot v}F(Av + B).
\end{aligned}
$$

Setting $w = Av + B$, we find that $v = A^{-1}w + A^{-1}B$. Substituting this value for v in the summation yields

$$\begin{aligned}
\hat{G}(u) &= \sum_{w \in F^m} (-1)^{u\cdot(A^{-1}w)+u\cdot(A^{-1}B)} F(w+B+B) \\
&= \sum_{w \in F^m} (-1)^{u\cdot(A^{-1}w)} (-1)^{u\cdot(A^{-1}B)} F(w) \\
&= \pm \sum_{w \in F^m} (-1)^{u'\cdot w} F(w),\ u' = (u^t A^{-1})^t \\
&= \pm \hat{F}(u')
\end{aligned}$$

Since the sets of Hadamard transforms are equal, the cosets containing **f** and **g** have equal weight distributions. □

The Nordstrom-Robinson code is a set of eight cosets of $\mathcal{R}(1,4)$ contained in $\mathcal{R}(2,4)$. Similar to the $\mathcal{R}(1,4)$ code, the $\mathcal{N}_{16}$ code is length $n = 2^4$. It contains a total of 256 codewords in its eight cosets, but unlike $\mathcal{R}(1,4)$, it is not a linear code over binary since it is possible to add two codewords from different cosets and have a codeword not contained in any coset as the sum. Since the sum of any two codewords in $\mathcal{N}_{16}$ is a bent codeword, the minimum distance in the Nordstrom-Robinson code is 6. For proof of this, see [MacWilliams/Sloane, 426]. Note that $\mathcal{R}(1,4) \subset \mathcal{N}_{16} \subset \mathcal{R}(2,4)$.

1.2.6 Golay Codewords

Let $f(v_1, ..., v_m) = v_{\alpha_1}v_{\alpha_2} + v_{\alpha_2}v_{\alpha_3} + \cdots + v_{\alpha_{m-1}}v_{\alpha_m}$ such that the v_{α_i}'s are distinct and elements of the generator matrix of $\mathcal{R}(1,m)$, m is even. Any codeword that has such a function $f(v)$ generating its reduced polynomial is a Golay codeword.

Theorem 8 *Any function $f(v)$ such that* **f** *is a Golay codeword is bent.*

Proof: Let $f(v_1, ..., v_m) = v_{\alpha_1}v_{\alpha_2} + v_{\alpha_2}v_{\alpha_3} + \cdots + v_{\alpha_{m-1}}v_{\alpha_m}$. Let A be a binary, invertible $m \times m$ matrix, m is even, with the form

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & \cdots & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
1 & 0 & 1 & 0 & 1 & 0 & \cdots & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 1
\end{pmatrix}$$

Let $v = (v_1, \ldots, v_m)$ be a row vector. Then vA maps each v_i to itself if i is even, or to the sum of all terms with odd i greater than or equal to the i of the term being mapped if i is odd. Consider $f(vA)$. It is the sum $(v_{\alpha_1} + v_{\alpha_3} + \cdots + v_{\alpha_{m-1}})(v_{\alpha_2}) + (v_{\alpha_2})(v_{\alpha_3} + v_{\alpha_5} + \cdots + v_{\alpha_{m-1}}) + (v_{\alpha_3} + v_{\alpha_5} + \cdots + v_{\alpha_{m-1}})(v_{\alpha_4}) + (v_{\alpha_4})(v_{\alpha_5} + v_{\alpha_7} + \cdots + v_{\alpha_{m-1}}) + \cdots + (v_{\alpha_{m-3}} + v_{\alpha_{m-1}})(v_{\alpha_{m-2}}) + (v_{\alpha_{m-2}})(v_{\alpha_{m-1}}) + (v_{\alpha_{m-1}})(v_{\alpha_m})$. Note that the first term, originally $v_{\alpha_1}v_{\alpha_2}$, is v_{α_2} multiplied by all the v_{α_i}, i is odd. The second term is v_{α_2} multiplied by all v_{α_i}, i is odd and strictly greater than 1. Since these are binary vectors, adding a vector to itself produces the all 0 vector. Therefore the sum of the first two terms reduces to $v_{\alpha_1}v_{\alpha_2}$ after cancellation. We can clearly continue to cancel terms from each pair of products. In the third and fourth terms cancellation leaves only $v_{\alpha_3}v_{\alpha_4}$, and so on for each pair of terms. Therefore $f(v)$ is affinely equivalent to the bent codeword $v_1v_2 + v_3v_4 + \cdots + v_{m-1}v_m$ and bent by Theorem 6. □

We shall be using as coset representatives for the $\mathcal{N}_{16}$ code six Golay codewords, the all zero codeword, and the codeword containing all possible quadratic terms in $\mathcal{R}(1, 4)$. The polynomials for the Golay representatives are

$$\begin{array}{ll} v_1v_2 + v_2v_3 + v_3v_4 & v_2v_1 + v_1v_4 + v_4v_3 \\ v_4v_1 + v_1v_3 + v_3v_2 & v_1v_4 + v_4v_2 + v_2v_3 \\ v_1v_3 + v_3v_4 + v_4v_2 & v_3v_1 + v_1v_2 + v_2v_4 \end{array}$$

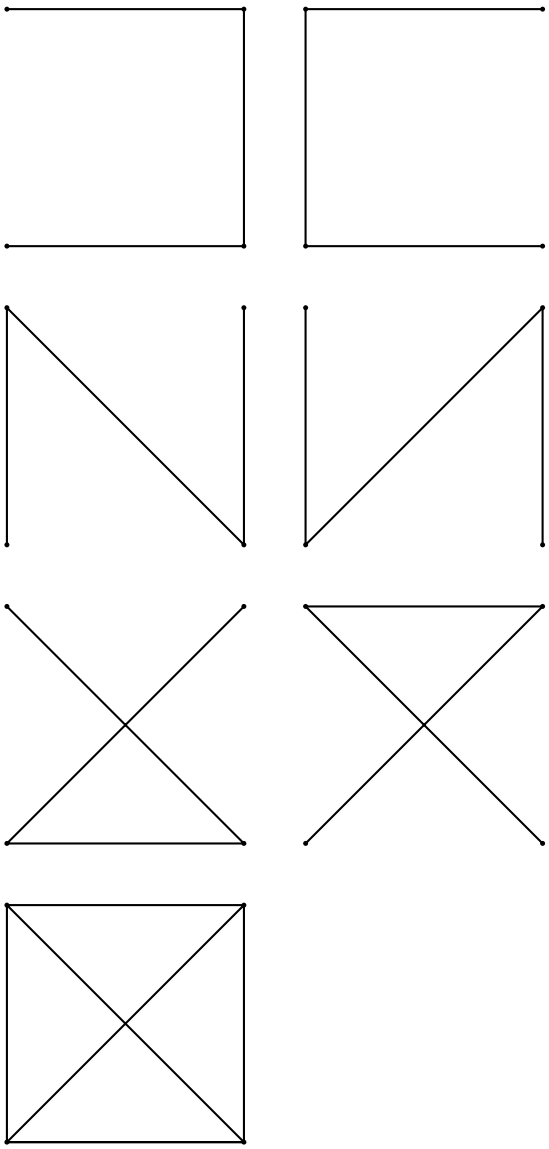
and the polynomial with all quadratic terms is $v_1v_2 + v_1v_3 + v_1v_4 + v_2v_3 + v_2v_4 + v_3v_4$.

1.2.7 Some Useful Notation

Codewords with only quadratic terms can be represented by a graph in which each edge represents a quadratic term that is the product of the two vertices it connects. The vertices are numbered $1, 2, \ldots, m$, starting with the uppermost point to the left proceeding clockwise, and represent the terms $v_1, v_2, \ldots, v_m$. Thus the quadratic term v_1v_2 is represented by the line segment from point 1 to point 2, and the vector v_iv_j is always mapped to the segment connecting points labeled i and j. In $\mathcal{R}(2, 4)$, the codeword $v_1v_3 + v_2v_3 + v_2v_4 + v_3v_4$ can be represented by:

The codeword $v_1v_2 + v_1v_4 + v_2v_3 + v_3v_5 + v_3v_6 + v_4v_5 + v_5v_6$ in $\mathcal{R}(2,6)$ can be represented by the following graph.

We shall be using as the coset representatives of the $\mathcal{N}_{16}$ code the following set of codewords. Six of these eight coset representatives are Golay codewords, the other two being the codewords containing every quadratic term possible from $\mathcal{R}(2,4)$ and the zero codeword which has as its coset $\mathcal{R}(1,4)$. The seven representatives that have graphs - the zero coset representative has an empty graph as it contains no quadratic terms - are drawn below.



Since we will be concerned with whether or not the codeword produced by the sum of two bent codewords is bent, we introduce a method for determining if the sum of two bent functions is a bent function. First determine the reduced polynomial for both functions. Graph both functions as detailed previously. To add the graphs, draw the graph that contains all the edges of both graphs, but delete all the edges that both graphs share. If g_i is an edge of either graph G_1 or G_2, the graphs of the original bent functions, then the sum is the set $G_\Sigma = \{g_i : g_i \in G_1 \bigcup G_2 - G_1 \bigcap G_2\}$. To check if G_Σ is bent, it is possible to compute $\hat{G}_\Sigma(u)$, but it is simpler to construct

and use an adjacency matrix. This adjacency matrix is

$$A = \begin{cases} a_{ij} = 1 & \text{if the } i\text{th and } j\text{th point are connected by an edge in } G_\Sigma \\ a_{ij} = 0 & \text{if the } i\text{th and } j\text{th point are not connected by an edge or if } i = j \end{cases}$$

The adjacency matrix A has 0's along its main diagonal and is symmetric. Row reduce A modulo 2; if A is of full rank, then G_Σ is bent. If A is of less than full rank, G_Σ is not bent. For proof of this, see [MacWilliams/Sloane, 441].

Theorem 9 *The maximum number of Golay coset representatives a code may contain and still have all pairwise sums of codewords be bent is* $\binom{m}{2}$.

Proof: Consider the graph of a Golay codeword. Since each vertex is connected to either 1 or 2 other vertices, all the rows of the adjacency matrix must have weight 1 or 2. No vertex is connected to itself so there are a maximum of $\binom{m-1}{1}+\binom{m-1}{2} = \binom{m}{2}$ ways to write a row of the adjacency matrix of a Golay codeword. If two codewords have adjacency matrices such that there is a row A_i that is the same in both matrices, then the adjacency matrix of the sum of these codewords will have a row of all zeros, and thus will not be of full rank. Therefore the maximum number of Golay codewords that can be contained in a code such that the sum of any two codewords is bent is $\binom{m}{2}$. □

1.2.8 Kerdock Codes

The Nordstrom-Robinson code is the smallest of the Kerdock codes. These codes exist for even $m \geq 4$ and have the following properties:
Similar to $\mathcal{R}(1, m)$, $\mathcal{K}(m)$ has length $n = 2^m$.
The $\mathcal{R}(1, m)$ code has 2^{m+1} codewords and $\mathcal{K}(m)$ is merely 2^{m-1} cosets of $\mathcal{R}(1, m)$ within $\mathcal{R}(2, m)$, so $\mathcal{K}(m)$ has 2^{2m} codewords.
The minimum distance between codewords is $2^{m-1} - 2^{m/2-1}$.
In general it is true that $\mathcal{R}(1, m) \subset \mathcal{K}(m) \subset \mathcal{R}(2, m)$ with the Nordstrom-Robinson code being the Kerdock code for $m = 4$.

The Kerdock code as defined is not a linear code. It is possible to add two codewords of $\mathcal{K}(m)$ and find their sum to be a codeword not contained in the code. It is possible to generate a code that is equivalent to $\mathcal{K}(m)$ and linear, but over $\mathbb{Z}_4$ instead of $\mathbb{Z}_2$. To do this we look at cyclic codes and their polynomial representation. Let $f(x)$ divide $x^n - 1$ over $\mathbb{Z}_2$. The set of polynomials $\{g(x)f(x) : deg(g) < n - deg(f)\}$ defines a cyclic code over $\mathbb{Z}_2$.
Example. Let $n = 7$; $f(x) = x^3 + x + 1$ divides $x^7 - 1$ over $\mathbf{Z}_2$. The cyclic code is then $\{g(x)(x^3 + x + 1) : deg(g) < 4\}$. Since all the polynomials of the form $g(x)f(x)$ can be written as linear combinations of the polynomials $1 \times f(x)$, $x \times f(x)$, $x^2 \times f(x)$, and $x^3 \times f(x)$, the generator matrix for this code will be 4×7. This

generator matrix is written with the coefficients of the polynomials as the entries, with the first column corresponding to the constant term or x^0, the second column corresponding to x^1, and so on with the last column corresponding to x^6. This particular matrix is

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

Cyclic codes are linear. They also have the property that $x_1x_2\cdots x_n \in \mathcal{C}$ implies $x_nx_1\cdots x_{n-1} \in \mathcal{C}$, where x_i is the ith term of any codeword. To construct a code equivalent to $\mathcal{K}(m)$, find a polynomial $f(x)$ that divides x^n-1. Define two additional polynomials, $d(x)$ and $e(x)$, where $d(x)$ is the polynomial found by deleting all the even-powered terms of $f(x)$ and keeping only the odd-powered terms. The polynomial $e(x)$ is found by deleting the odd-powered terms and retaining only the terms of even power. Now our new cyclic code over $\mathbb{Z}_4$ can be generated by the polynomial $g(x^2) = (d(x))^2 - (e(x))^2 \, (mod\ 4)$. The final polynomial, $g(x)$, can be found from $g(x^2)$ and generates a cyclic code over $\mathbb{Z}_4$ just as $f(x)$ generated a cyclic code over $\mathbb{Z}_2$.

Example. Since $f(x) = x^3 + x + 1$, $d(x) = x^3 + x$ and $e(x) = 1$. We must find the polynomial $g(x)$ to construct the code, so the first step is to find $g(x^2)$. Doing the arithmetic modulo 4, we find $g(x^2) = x^6 + 2x^4 + x^2 - 1 \equiv x^6 + 2x^4 + x^2 + 3$. Thus $g(x) = x^3 + 2x^2 + x + 3$. The generator matrix for the new cyclic code is

$$\begin{pmatrix} 3 & 1 & 2 & 1 & 0 & 0 & 0 \\ 0 & 3 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 3 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 3 & 1 & 2 & 1 \end{pmatrix}$$

Since this is a cyclic code over $\mathbb{Z}_4$, the codewords generated can have each row appear multiple times in its reduced polynomial form - up to 3 times - before cancellation. Thus there are $4^4 = 256$ codewords in this cyclic code. Adding a parity check bit to each row enlarges the matrix to 4×8. We now have an almost cyclic code with the generator matrix

$$\begin{pmatrix} 3 & 1 & 2 & 1 & 0 & 0 & 0 & 1 \\ 0 & 3 & 1 & 2 & 1 & 0 & 0 & 1 \\ 0 & 0 & 3 & 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 3 & 1 & 2 & 1 & 1 \end{pmatrix}$$

This code is length $n = 8$ with 256 codewords. This code is equivalent to the $\mathcal{K}(4)$ or the Nordstrom-Robinson code, but we must map it back into binary to see this. This mapping is accomplish by the use of an explicit gray map that preserves distance - Lee distance in quaternary and Hamming distance in binary - between the two

codes. The mapping is

$$0 \mapsto 00 \;\; 1 \mapsto 01$$

$$2 \mapsto 11 \;\; 3 \mapsto 10$$

The new code is length $n = 16$ with 256 codewords, exactly like the Nordstrom-Robinson code. To fully see that these codes are identical, we can exchange columns to make the derived Kerdock code match the Nordstrom-Robinson code in all respects. By adding a parity check bit to the generator matrix over $\mathbb{Z}_4$, gray-mapping the full code - not just the generator matrix - into $\mathbb{Z}_2$, and reordering the columns, it is possible to generate the $\mathcal{K}(m)$ code from a cyclic code over $\mathbb{Z}_4$.

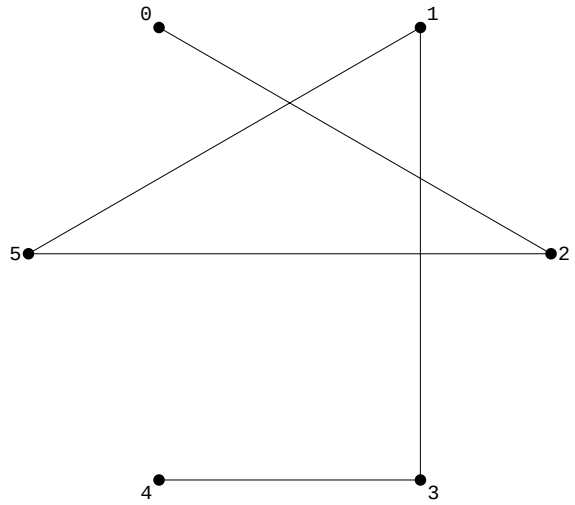
2 Observations

2.1 Preliminary Observations

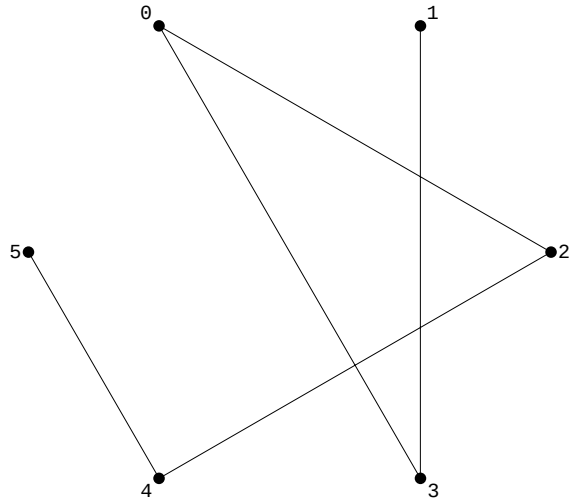
By observing the Nordstrom-Robinson code, a few properties were immediately apparent. All the Golay codewords which were present in the form of the code with which we were working had a complement codeword which was a reflection, or a rotation, of that codeword. Thus we attempted to look for symmetries in Golay codewords in $\mathcal{R}(2, 6)$. The results revealed different properties than those encountered in $\mathcal{R}(2, 4)$.

Our first observation was that the sum of a Golay codeword and its reflection across any axis of its graph was not bent. A computer program, which ran over all Golay codewords of length $n = 2^6$, confirmed these results.

It became clear after a few attempts that rotation of graphs offered a more practical way of creating sets of codewords whose sums were bent. In order to simplify the work with rotations, a new notation was introduced. Every Golay codeword could be represented by a string of six digits in $\mathbb{Z}_6$. For example, the codeword $v_1v_3 + v_3v_6 + v_6v_2 + v_2v_4 + v_4v_5$ could be simply represented by the string 136245. The graph that represents this codeword is



Rotating the graph of this codeword by one shift counterclockwise gives



which is equivalent to adding 1 to each position in the string of digits modulo 6, yielding the string 136245. Note that while the graphs are labeled beginning with 0 to facilitate rotation, the generator matrix of $\mathcal{R}(r, m)$ has no row v_0. The row v_1 corresponds to the vertex labeled 0 in every graph.

The sum of any codeword with its rotation is easily obtained following the notation described in the Background, and the adjacency matrix was used to find out whether that sum was bent or not. In this example, the sum of these two codewords can be represented graphically by:

The adjacency matrix for this codeword is

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

and, since this matrix has full rank, the sum of the codeword $v_1v_3 + v_3v_6 + v_6v_2 + v_2v_4 + v_4v_5$, and its first rotation is bent.

2.2 Golay Codewords of length 2^6

The total number of Golay codewords in $\mathcal{R}(2,6)$ is $\frac{6!}{2} = 360$, but many of these codewords are equivalent under rotation. If two codewords are defined as equivalent if and only if one codeword's graph can be rotated to produce the other codeword's graph, then there are 64 distinct codewords in $\mathcal{R}(2,6)$. Those 64 codewords are divided into 5 sets whose elements share the same properties toward their rotations.

(i) Among the 64 distinct Golay codewords, 18 have the property that when summed with any of their rotations, none of the resulting codewords were bent.

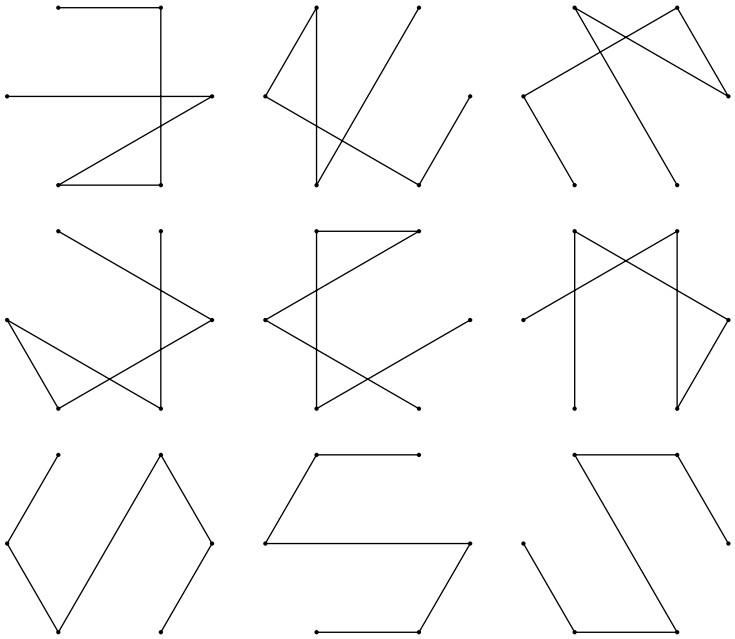
(ii) There are 12 codewords whose sum with their first clockwise rotation is bent. Their sum with their first counter-clockwise rotation is bent too, but since the sum of any of these codewords with its second rotation in either direction is not bent, one can only chose a set of two vectors at a time whose sum is bent. Any set of three vectors includes two vectors where one is equal to the other vector rotated twice clockwise, and thus the sum of these two vectors is not bent.

(iii) There are 20 codewords such that the sums with both their second and fourth rotations are bent. Therefore any two elements of this set, when summed, will yield a bent codeword as the sum. The sets which includes the first, third, and fifth rotation of each of these vectors also has the property that the sum of any of its two elements are bent.

(iv) Among the Golay codewords in $\mathcal{R}(2,6)$, 14 codewords have the property that their sum with their first and second rotation is bent. Since the sum of any of these codewords with their third rotation is never bent, we could create sets of a maximum of 3 codewords such that the sum of any two elements in the set was bent.

(v) Among the 14 codewords in the previous set, 6 have the additional property that they are equal to their third rotation. In fact, there are only 3 rotations of these codewords that exist, since a rotation by 3 always gives back the original codeword. All the codewords that are equal to their third rotation are present in this set.

In order to maximize the number of elements in a set such that the sum of any two elements in the set is bent, we selected members of some of the previous sets so that the sum of their respective rotations remained bent. The maximum number of codewords obtained this way was 9. The first six codewords come from the third set, and the last three come from the fifth set. The graphical representation of one of these groups of 9 is:



There are six such sets of nine codewords such that the sum of any two codewords is bent. All of these sets have six codewords from the third set, and 3 from the fifth set.

An exhaustive search was run on all the Golay codewords in $\mathcal{R}(2,6)$, but none had the property that their sum with all the codewords in any of the six sets was bent.

2.3 Mapping

By knowing a set of codewords such that the sum of any two of them is bent, we could create a new set with the same number of codewords such that a given Golay codeword is included in it. By finding the mapping of coordinates that changes one of the codewords in the set into a different codeword outside the set, then applying the same mapping to all the other codewords, a new set is created in which the sum of any two elements is bent.

Theorem 10 *Let $f(u)$ and $g(u)$ be Golay codewords such that their sum, $h(u)$, is bent. Let M be a mapping of the coordinates $v_1, v_2, \ldots, v_m$ such that $M(k(u)) = K(uA)$, where A is a matrix of 0's and 1's such that $A_{ij} = 1$ if v_j is mapped to v_i. $M(f(u)) + M(g(u))$ is bent.*

Proof: Since $f(u)$ and $g(u)$ are both Golay, they only contain quadratic terms, and their sum, $h(u)$, only contains quadratic terms. We can thus write

$$f(u) = uQu^t \quad g(u) = uPu^T \quad h(u) = uRu^T$$

Where Q,P,and R are $m \times m$ matrices such that $Q_{ij} = 1$ if the term $u_i u_j$ is present in the polynomial form of the codeword. The equation $f(u) + g(u) = h(u)$ can be written as:

$$uQu^T + uPu^T = uRu^T.$$

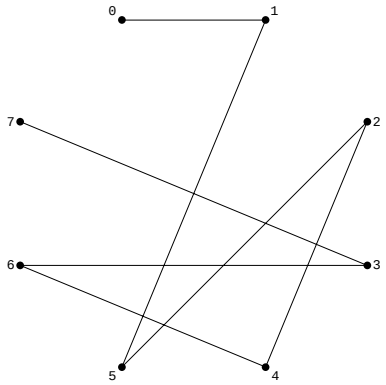
In this notation,

$$\begin{aligned} M(f(u)) + M(g(u)) &= f(uA) + g(uA) \\ &= (uA)Q(uA)^T + (uA)P(uA)^T \\ &= vQv^T + vPv^T, v = uA \\ &= vRv^T \\ &= h(v) \\ &= h(uA) \end{aligned}$$

By Theorem 6, $h(uA)$ is bent. $\square$

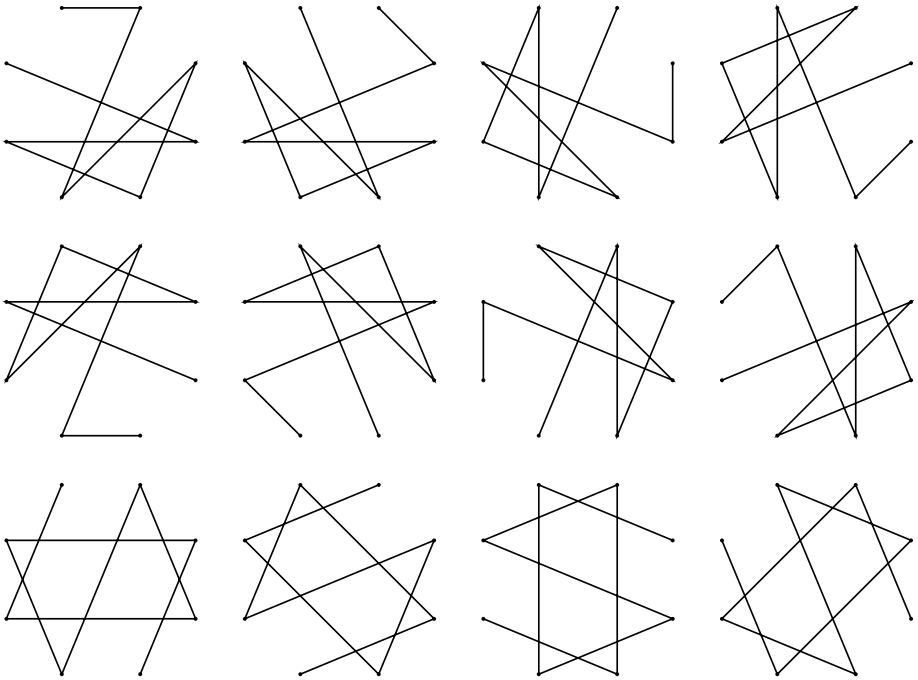
2.4 Golay codewords of length 2^8

We attempted to extrapolate the properties of $\mathcal{R}(2,6)$ to $\mathcal{R}(2,8)$, but the properties of $\mathcal{R}(2,8)$ were different. While in $\mathcal{R}(2,6)$ all codewords that were equal to their halfway rotation had the property that their sum with their other rotations was bent, such a property did not hold in $\mathcal{R}(2,8)$. However, there were some interesting results. A set of codewords existed such that the sum of any codeword in that set with any of its eight rotations was always bent. An example of such a codeword is 12635748 whose graphic representation is:



By searching all the other possible Golay codewords in $\mathcal{R}(2,8)$, we found that there existed some codewords whose sum with all the possible rotations of this codeword were bent. By carefully choosing these codewords so that their sum was at least bent with some of their rotations, we could construct a set of 12 codewords

such that the sum of any two of them is bent. Notice that the first 8 graphs are simply the 8 possible rotations of 12635748, while the next 4 are the codeword 17426835 and its first three rotations.



2.5 The Kerdock Codes

Recall from the background that the Kerdock code of length 16, $\mathcal{K}(4)$, is equivalent to the Nordstrom-Robinson code, $\mathcal{N}_{16}$. In order for the Kerdock code of that length to include a maximum number of Golay codewords as coset representatives, one has to do a mapping on the columns of the original Kerdock generator matrix. The mapping simply permutes the position of the columns.

One property of $\mathcal{K}(m)$ is that is always includes a coset whose representative is the zero codeword. Since the zero codeword is not a bent function, this coset has a different weight distribution than the other cosets. In fact, this coset has the same properties as $\mathcal{R}(1, m)$, and, upon certain mappings on the columns, the coset can be transformed into $\mathcal{R}(1, 4)$ as we have constructed it. Given that both $\mathcal{R}(1, m)$ and the zero coset are linear, a column mapping which produces as part of the new code the generator matrix of $\mathcal{R}(1, m)$ will produce the entire code $\mathcal{R}(1, m)$. Since $\mathcal{R}(1, m) \subset \mathcal{K}(m)$, we can restrict our search of column permutations to the set of permutations that contain $\mathcal{R}(1, m)$, or even simpler that contain the generator matrix for $\mathcal{R}(1, m)$. The zero coset is the only coset of $\mathcal{R}(1, m)$ whose codewords are not bent, and thus all the codewords of this coset of $\mathcal{K}(m)$ can be found quickly.

We examined the code $\mathcal{K}(6)$ and attempted to find the maximum number of Golay coset representatives ($\binom{6}{2} = 15$) by determining the exact column permutation. Unfortunately there are $2^7 = 128$ codewords in the zero coset of $\mathcal{K}(6)$ and so many codewords makes for an unreasonably large number of column permutations that might be successful. To understand how $\mathcal{K}(6)$ might be mapped back into the desired form by column permutation, we examined $\mathcal{K}(4)$.

The generator matrix for $\mathcal{K}(4)$ over $\mathbb{Z}_4$ is

$$\begin{pmatrix} 3 & 1 & 2 & 1 & 0 & 0 & 0 & 1 \\ 0 & 3 & 1 & 2 & 1 & 0 & 0 & 1 \\ 0 & 0 & 3 & 1 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 3 & 1 & 2 & 1 & 1 \end{pmatrix}$$

All the codewords of the zero coset of $\mathcal{K}(4)$ are weight 8 as this coset is really just $\mathcal{R}(1,4)$. We generated all the linear combinations of the quaternary matrix and looked for all the codewords of weight 8. Because of the gray mapping we used, it is possible to determine the weight of a codeword in binary by looking at its quaternary pre-image. The weight of a codeword is twice the number of 2's plus the number of 1's and 3's. Although there must not exist more than 32 codewords of weight 8, there are many more than 32 possible ways to generate a weight 8 codeword from 8 digits over $\mathbb{Z}_4$. Surprisingly, all the codewords of weight 8 were divided into two evenly sized groups: one group of codewords consisting solely of 1's and 3's, and one group consisting solely of codewords of 0's and 2's. Thus if a codeword contained a 1 or a 3, it could not contain a 0 or a 2, and conversely. Since we must find the generator matrix of $\mathcal{R}(1,4)$ within these 32 codewords, we decided to work backwards from the generator matrix to the list of quaternary codes. As shown before, the generator matrix for $\mathcal{R}(1,4)$ is

$$\begin{array}{c} \mathbf{1} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

The first row, **1**, is simply the row of all 2's in quaternary. This row is present regardless of the mapping and thus we ignore it. The last row consisting of even alternating 0's and 1's is the row of all 1's in quaternary; for the same reason we ignore it. The other three rows consist of blocks of 0's and 1's in binary, a minimum of two 0's or 1's in each block. Thus in quaternary these rows will be represented by rows of 0's and 2's when the binary code is 00 or 11, respectively. We have reduced our search to looking for 3 rows out of 16 (the number of rows consisting only of 0's and 2's) with the property that, after a permutation of columns, the three rows will

look like

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 \end{pmatrix}$$

which when mapped back into binary will be the three necessary rows to complete the generator matrix of $\mathcal{R}(1,4)$. We found that switching the second with the third column and the fourth with the sixth column of the quaternary generator matrix of $\mathcal{K}(4)$ produced, when mapped into binary, the correct $\mathcal{R}(1,4)$ code. Thus we sought to adapt our method to $\mathcal{K}(6)$. In $\mathcal{K}(6)$, the zero coset has 128 codewords, so the first step is to reduce this number to a more reasonable size that we can search for the necessary codewords to complete the generator matrix of $\mathcal{R}(1,6)$. As before, the row of all 1's and the row of all 2's in the quaternary code were both present, so only 5 more rows were needed to complete the generator matrix of $\mathcal{R}(1,6)$. The rest of the rows would consist only of 0's and 2's, so we only had to search half of the code of the correct rows. We also noticed that half of the rows of 0's and 2's were the complement of the other half, that is adding the two rows together would produce the all 2 row. We found a set of 32 codewords such that no codeword and its complement were present in the set, and restricted our search to that set. At this point two assumptions were made. The first is the assumption that using the complements of a code will not produce any new, distinct codes with different column permutations. This assumption is based on the linearity of the code over $\mathbb{Z}_4$. The second assumption was that since it was possible to permute columns of $\mathcal{K}(4)$ over $\mathbb{Z}_4$, it will be possible to do the same in $\mathcal{K}(6)$. Thus no column permutations in binary were examined, and any possible code in which the generator matrix was found by permutations of the columns on the rows of 1's and 3's was neglected.

We noticed that for the zero coset of $\mathcal{K}(4)$, the three missing rows would have the form shown above. Looking at the columns, it is clear that they are all the "binary" (of 0's and 2's) 3-tuples. The same principle holds for $\mathcal{K}(6)$, though we were looking for 5-tuples instead. Instead of switching columns, we sought to reoder them in such a way that all the "binary" 5-tuples were present and in "binary" ascending order. Thus any five rows that contained in their columns all the "binary" 5-tuples contained a reordering of columns such that the generator matrix of $\mathcal{R}(1,6)$ was present once the code was mapped into binary. Even though a code might contain the generator matrix for $\mathcal{R}(1,6)$, it could still fail in other cosets. Thus we had to first find the code and then generate every codeword in it. After we found these codewords, we checked the reduced polynomial form of each to see if the codewords were Golay. Since a Golay codeword cannot have any terms in its reduced polynomial of cubic order or higher, we immediately rejected any code that contained even a single cubic term in a codeword's polynomial. We had a computer program search for sets of 5 rows such that we could find the generator matrix of $\mathcal{R}(1,6)$, reorder the columns as necessary, and then check reduced polynomials. The program never

found more than seven Golay coset representatives which implies that it was either written incorrectly or that our assumptions reduced the search to such a level that finding 15 Golay coset representatives was not possible.

Appendix A
Six sets of Nine Golay Codewords in $\mathcal{R}(2,6)$

The following sets include nine codewords each, written in the short-hand notation as a string of digits (See Preliminary Observations for more detail). Notice that, in each set, the second and the third codewords are respectively the second and the fourth clockwise rotation of the first codeword. The fifth and the sixth codewords are also the second and the fourth clockwise rotation of the fourth codeword. The eigth and the ninth codewords in each set are the first and second clockwise rotation of the seventh codeword.

$\{013425, 235041, 451203, 125430, 341052, 503214, 024153, 135204, 240315\}$
$\{013425, 235041, 451203, 135420, 351042, 513204, 054123, 105234, 210345\}$
$\{014325, 230541, 452103, 135420, 351042, 513204, 051423, 102534, 213045\}$
$\{031245, 253401, 415023, 143250, 205412, 421034, 042513, 153024, 204135\}$
$\{031245, 253401, 415023, 153240, 215402, 431024, 012543, 123054, 234105\}$
$\{032145, 254301, 410523, 153240, 215402, 431024, 015243, 123054, 231405\}$

Appendix B
sets of twelve Golay Codewords in $\mathcal{R}(2,8)$

The following sets contain 12 Golay codewords in $\mathcal{R}(2,8)$ with the property that the sum of any two codewords is bent. Notice that the seven codewords after the first one are just the first codewords 7 possible rotation, and that codewords 10-12 are the rotations of the ninth codeword.

{01347652, 12450763, 23561074, 34672105, 45703216, 56014327, 67125430, 70236541, 06315724, 17426035, 20537146, 31640257}

{01476352, 12507463, 23610574, 34721605, 45032716, 56143027, 67254130, 70365241, 02137564, 13240675, 24351706, 35462017}

{01524637, 12635740, 23746051, 34057162, 45160273, 56271304, 67302415, 70413526, 06315724, 17426035, 20537146, 31640257}

{01526437, 12637540, 23740651, 34051762, 45162073, 56273104, 67304215, 70415326, 02173564, 13204675, 24315706, 35426017}

{01534726, 12645037, 23756140, 34067251, 45170362, 56201473, 67312504, 70423615, 06173524, 17204635, 20315746, 31426057}

{03145276, 14256307, 25367410, 36470521, 47501632, 50612743, 61723054, 72034165, 02137564, 13240675, 24351706, 35462017}

{03452176, 14563207, 25674310, 36705421, 47016532, 50127643, 61230754, 72341065, 06315724, 17426035, 20537146, 31640257}

{03714562, 14025673, 25136704, 36247015, 47350126, 50461237, 61572340, 72603451, 02351764, 13462075, 24573106, 35604217}

{03762415, 14073526, 25104637, 36215740, 47326051, 50437162, 61540273, 72651304, 06351724, 17462035, 20573146, 31604257}

{03764215, 14075326, 25106437, 36217540, 47320651, 50431762, 61542073, 72653104, 02137564, 13240675, 24351706, 35462017}

{04135267, 15246370, 26357401, 37460512, 40571623, 51602734, 62713045, 73024156, 02573164, 13604275, 24715306, 35026417}

{04137625, 15240736, 26351047, 37462150, 40573261, 51604372, 62715403, 73026514, 02537164, 13640275, 24751306, 35062417}

{04165732, 15276043, 26307154, 37410265, 40521376, 51632407, 62743510, 73054621, 06173524, 17204635, 20315746, 31426057}

{04315267, 15426370, 26537401, 37640512, 40751623, 51062734, 62173045, 73204156, 06715324, 17026435, 20137546, 31240657}

{04317625, 15420736, 26531047, 37642150, 40753261, 51064372, 62175403, 73206514, 06751324, 17062435, 20173546, 31204657}

{04327516, 15430627, 26541730, 37652041, 40763152, 51074263, 62105374, 73216405, 02351764, 13462075, 24573106, 35604217}

{04561372, 15672403, 26703514, 37014625, 40125736, 51236047, 62347150, 73450261, 06537124, 17640235, 20751346, 31062457}

{04571263, 15602374, 26713405, 37024516, 40135627, 51246730, 62357041, 73460152,
02137564, 13240675, 24351706, 35462017}
{04573621, 15604732, 26715043, 37026154, 40137265, 51240376, 62351407, 73462510,
02173564, 13204675, 24315706, 35426017}
{04723156, 15034267, 26145370, 37256401, 40367512, 51470623, 62501734, 73612045,
02715364, 13026475, 24137506, 35240617}
{04751263, 15062374, 26173405, 37204516, 40315627, 51426730, 62537041, 73640152,
06351724, 17462035, 20573146, 31604257}
{04753621, 15064732, 26175043, 37206154, 40317265, 51420376, 62531407, 73642510,
06315724, 17426035, 20537146, 31640257}
{05124673, 16235704, 27346015, 30457126, 41560237, 52671340, 63702451, 74013562,
06751324, 17062435, 20173546, 31204657}
{05126473, 16237504, 27340615, 30451726, 41562037, 52673140, 63704251, 74015362,
02537164, 13640275, 24751306, 35062417}
{05174326, 16205437, 27316540, 30427651, 41530762, 52641073, 63752104, 74063215,
06537124, 17640235, 20751346, 31062457}
{05436712, 16547023, 27650134, 30761245, 41072356, 52103467, 63214570, 74325601,
02573164, 13604275, 24715306, 35026417}
{05743612, 16054723, 27165034, 30276145, 41307256, 52410367, 63521470, 74632501,
06751324, 17062435, 20173546, 31204657}
{07354162, 10465273, 21576304, 32607415, 43710526, 54021637, 65132740, 76243051,
02715364, 13026475, 24137506, 35240617}
{07362451, 10473562, 21504673, 32615704, 43726015, 54037126, 65140237, 76251340,
06715324, 17026435, 20137546, 31240657}
{07364251, 10475362, 21506473, 32617504, 43720615, 54031726, 65142037, 76253140,
02573164, 13604275, 24715306, 35026417}
{07412536, 10523647, 21634750, 32745061, 43056172, 54167203, 65270314, 76301425,
06751324, 17062435, 20173546, 31204657}
{07541236, 10652347, 21763450, 32074561, 43105672, 54216703, 65327014, 76430125,
02573164, 13604275, 24715306, 35026417}

References

[1] J.F. Dillon A survey of Bent Functions I don't know where it came from.

[2] J.A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes. *Submitted,* 1997

[3] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes (2nd edition).* Nrth Holland, Amsterdam, 1986.