Integer Maxima in Power Envelopes of Golay Codewords

Michael W. Cammarano and Meredith L. Walker

April 6, 1999

Abstract

This paper examines the distribution of integer peaks amoung Golay cosets in $\mathbf{Z}_2$ and $\mathbf{Z}_4$. It will prove that the envelope power of at least one element of every Golay coset of $\mathbf{Z}_4$ of length 2^m (for m-even) will have a maximum at exactly 2^{m+1}. Similarly, it will be proven that one element of every Golay coset of $\mathbf{Z}_2$ of length 2^m (for m-odd) will have a maximum at exactly 2^{m+1}. Observations and partial arguments will be made about why Golay cosets of $\mathbf{Z}_2$ of length 2^m (for m-even) contain no elements with such a peak.

*The authors thank Hewlett-Packard for their generous support during the summer of 1997, and to Dr. James Davis, University of Richmond, for his extensive support and assistance.

1 Introduction

1.1 Background on Phase Signal Keying

This paper will examine several problems relating to power envelopes of various codewords in binary and quaternary phase shift keying (BPSK and QPSK, respectively). The value of a given position (which can be $\{1, -1\}$ in binary and $\{1, i, -1, -i\}$ in quaternary) in a codeword is encoded as a phase shift in the oscillating wave with the frequency uniquely associated with that position, using the formula below:

$$d_n e^{i2\pi ft}$$

where d_n is the value of the nth position in the codeword D, t is the time (ranging from 0 to 1), and f is the frequency associated with position n.

Therefore, the complex signal for the codeword, $S(t)$, will be composed of the sum of the individual waves for each position:

$$S(t) = \sum_{n=1}^{N} d_n e^{i2\pi(f_c+f_n)t}$$

where f_c is the basic carrier frequency for the transmitted signal, and f_n is the frequency offset used to encode position n.

And so the envelope power, $P(t)$, will be defined as:

$$\begin{aligned} P(t) &= S(t)S^*(t) \\ &= \sum_{n=1}^{N} d_n e^{i2\pi(f_c+f_n)t} + \sum_{m=1}^{N} d_m^* e^{-i2\pi(f_c+f_m)t} \\ &= \sum_{n,m} d_n d_m^* e^{i2\pi(f_n-f_m)t} \end{aligned}$$

Observe that the carrier frequency f_c cancelled out. Therefore, the envelope power will be an upper bound on the power of any signal, regardless of its frequency (see *Fig. 1.1*). This allows us to use the envelope power to find the global maximum for the signal.

Fig. 1.1 Graph showing the envelope power(dark line) and a sample signal(light line) for the codeword $+++-++-+$. The carrier frequency f_c is 10 for the signal graphed in this example. Note that the codeword acheives a max power of exactly 16.

At this point we will substitute $f_n = nf_s$ and $f_m = mf_s$ as our mapping of frequencies to positions. It is important to note that other mappings are possible as well, except they may not maintain orthogonality.

$$\begin{aligned}
&= \sum_{n,m} d_n d_m^* e^{i2\pi(n-m)f_s t} \\
&= N + \sum_{n \neq m} d_n d_m^* e^{i2\pi(n-m)f_s t} \\
&= N + \sum_{u>0} \left(\sum_{\{n|1 \leq n \leq N-u\}} d_n d_{n+u}^* \right) e^{i2\pi u f_s t} + \sum_{u<0} \left(\sum_{\{n|-u+1 \leq n \leq N\}} d_n d_{n+u}^* \right) e^{i2\pi u f_s t}
\end{aligned}$$

The innermost sum in the expression is referred to as the aperiodic auto correlation, $C_D(u)$ (where D is $d_1 d_2 d_3 \ldots d_N$):

$$C_D(u) = \sum_{\{n|1 \leq n \leq N-u\}} d_n d_{n+u}^*$$

Thus, our final result in this section is:

$$P(t) = N + 2Re\left(\sum_{u>0} C_D(u) e^{i2\pi u f_s t} \right)$$

For engineering purposes, it is preferable to limit the maximum value of $P(t)$. Situations where peaks from many different component frequencies align at a particular value of t, causing a high signal power at that point, are undesirable. We would like to be able to choose codewords that result in power functions that always stay within some predetermined bounds. Note that in the worst case, where all peaks align, the power would have a value of N^2. For an example of this, consider $P_D(0)$ for D where $d_1 = d_2 = d_3 = \cdots = d_N = 1$. Consult [Davis/Jedwab] for additional information.

1.2 Significance of Golay Pairs to the Max Power

If D and E are codewords such that $C_D(u) + C_E(u) = 0$ for all $u > 0$, then D and E comprise a Golay pair [Golay]. Observe that:

$$P_D(t) = N + 2Re\left(\sum_{u>0} C_D(u) e^{i2\pi u f_s t} \right)$$

$$P_E(t) = N + 2Re\left(\sum_{u>0} C_E(u) e^{i2\pi u f_s t} \right)$$

$$\begin{aligned}
P_D(t) + P_E(t) &= 2N + 2Re\left(\sum_{u>0} (C_D(u) + C_E(u)) e^{i2\pi u f_s t} \right) \\
&= 2N \qquad \text{(since } C_D(u) + C_E(u) = 0\text{)}
\end{aligned}$$

Thus, any codeword D that is a member of a Golay pair will have $P_D(t) \leq 2N$, a dramatically lower power bound than the worst case N^2. Our investigation will focus upon properties of Golay pairs, and the details of their power properties.

1.3 Background on Reed-Muller Codes

Soon it will be shown how Golay pairs can be constructed using Reed-Muller codes. Some basic background on Reed-Muller codes as we will use them follows. We will

be discussing Reed-Muller codes of length 2^m. Our basis vectors will be numbered as follows:

x_1	consists of the sequence 2^{m-1} 0's followed by 2^{m-1} 1's
x_2	consists of the sequence 2^{m-2} 0's followed by 2^{m-2} 1's repeated twice.
$\vdots$	
x_{m-n}	consists of the sequence 2^{m-n} 0's followed by 2^{m-n} 1's repeated n times.
$\vdots$	
x_m	consists of alternating 0's and 1's.

Linear combinations of these basis vectors will form first order Reed-Muller(RM) codes. The second order RM basis vectors include the first order vectors x_i, as well as all intersections of first order vectors $x_i x_j$. Linear combinations of these will form the second order RM codes. We will use r to represent the order of the RM codes.

The notation $RM(1, m)$ represents the code comprised of all linear combinations of the first-oder basis vectors. Similarly, $RM(2, m)$ represents the code comprised of all linear combinations of second order basis vectors. Note that the weight of any codeword in $RM(1, m)$ will be 2^{m-1} and that of any codewrod in $RM(2, m)$ will be 2^{m-2}.

For more information of Reed-Muller codes, consult [Macwilliams/Sloane].

1.4 Construction From Reed-Muller Templates

Previous work with Golay pairs had demonstrated that they could be constructed in binary using a simple template involving Reed-Muller codes.

Form a codeword g of length 2^m as follows:

$$\mathrm{g} = AB + BC + \cdots + XY + YZ + x$$

Where every 1st order Reed-Muller basis vector is represented
by exactly one of the vectors $\{A, B, C, \ldots, Z\}$ and $x \in RM(1, m)$
Note that $AB + \cdots + YZ$ is equivalent to $x_{\pi(1)}x_{\pi(2)} + \cdots + x_{\pi(m-1)}x_{\pi(m)}$.

Any g of this form can be made into a member D of a Golay pair by assigning $d_n = (-1)^{\mathrm{g}_n}$ to map the values $\{0, 1\}$ from the Reed-Muller codeword onto the values $\{1, -1\}$ used in the BPSK. It has been proven that this construction method for g will always produce a member of a Golay pair, and it is conjectured that this construction method produces *all* Golay codewords.

Essentially, these Golay pairs will all be elements in the coset of $RM(1, m)$ with coset representative $AB + BC + \cdots + YZ$. A similar construction can be applied to find a member of a quaternary Golay pair, which will be any element g of the coset of*quaternary* $RM(1, m)$[1] with coset representative $2(AB + BC + \cdots + YZ)$, using the mapping $d_n = i^{\mathrm{g}_n}$.

1.5 Weight Equivalence

In a template that involves ALL of the basis vectors $x_1 \ldots x_m$ (such as $AB + BC + \cdots + YZ$ seen above), any resulting codeword will have the same weight, regardless

[1]Throughout this paper, quaternary Reed-Muller refers to a code constructed from the same basis vectors as binary RM, but taking linear combinations in $\mathbf{Z}_4$.

of the mapping chosen. This can be argued by noting that Reed-Muller codes can be constructed using a binary counter [Macwilliams/Sloane]. For every possible $c \in F_2^m$, there will be exactly one position n such that c_1 is the binary value of the n^{th} basis vector A, c_2 is the value of the n^{th} basis vector B, c_3 is the value of the n^{th} basis vector C, and so forth through all basis vectors of $RM(1,m)$. Any position represented by $c \in F_2^m$ in one mapping will have a corresponding position with the same c (and hence the same value) in any other mapping, although clearly it need not be in the same position. Thus, different mappings between the basis vectors and the vectors $A \ldots Z$ in the template will all result in equal weight codewords.

Example: For $m = 3$:

	$A = x_1, B = x_2, C = x_3$	$A = x_2, B = x_1, C = x_3$
A	000**0**1111	00110**0**11
B	001**1**0011	00001**1**11
C	010**1**0101	01010**1**01
$AB + BC$	000**1**0001	00000**1**10

1.6 Distribution of Max Power Values Within Golay Cosets

Previous investigations into the maximum power within any 1st order Reed-Muller coset, whether Golay or not, revealed intriguing patterns. The computer results in Appendix A are sorted listings of the length 16 coset leaders and the maximum power contained in any element of that coset for all $RM(1,m)$ cosets within $RM(2,m)$. In the binary case, notice that the twelve cosets with the lowest maximum power values are the only cosets that satisfy the Golay construction formula given above, and all of their powers are < 32 as expected, but never take on the integer value 32. However, there are a large number of cosets with elements containing exact peaks of 64, and of course the single coset containing the all-1 case (and simple variants thereof) which has a peak of exactly 256. Compare these results with those in the quaternary output, in which *all* twelve Golay cosets contain peaks of exactly 32, 40 cosets contain peaks of exactly 64, 11 cosets contain peaks of exactly 128, and still there is one coset containing peaks of exactly 256.

Our primary objective has been to learn more about the emergence of integer peaks – understanding what codewords can produce them in both binary and quaternary codes of various lengths, and what causes the distribution of these integer peaks among cosets and within the elements of a coset. To approach this task, it was necessary to gain an understanding of what conditions enable integer peaks to appear.

1.7 A Valuable Observation

For our purposes we will find it convenient to observe from the power expansion that:

$$\begin{aligned} e^{ix} &= 1 + ix + \tfrac{(ix)^2}{2!} + \tfrac{(ix)^3}{3!} + \cdots \\ &= (1 - \tfrac{x^2}{2!} + \tfrac{x^4}{4!} - \cdots) + i(x - \tfrac{x^3}{3!} + \tfrac{x^5}{5!} - \cdots) \\ &= \cos x - i \sin x \end{aligned}$$

This description in terms of familiar trigonometric functions will simplify much of the work to follow. Henceforth, we will use:

$$S(t) = \sum_{n=1}^{N} d(n) \cos(2\pi n t) + i \sum_{n=1}^{N} d(n) \sin(2\pi n t)$$

2 Our Initial Speculations

2.1 Limitations on the Formation of Integer Peaks

We begin by making a speculation about where integer peaks can occur. We hypothesize that integer peaks in the sum of all the frequencies will only occur at values of t where exact peaks in the component frequencies align with each other. We have been unsuccessful at proving this claim, but it has intuitive appeal and is supported by the evidence we have been able to gather with available computing resources. Overall, we are confident that this claim, or some generalization of it, will hold, but can only offer the empirical results to support it.

Consider the ways in which sin and cos waves overlap, given the possible frequency values (*Table 2.1*). The values from the table can be substituted for the sin and cos functions used to calculate $P(t)$, yielding greatly simplified formulas for computing power at certain values of t. For example, noting that at $t = 0$, all cosine functions (regardless of frequency) assume the values 1, and all sine functions assume the value 0. So, at $t = 0$:

$$S(t) = \sum_{n=1}^{N} d_n = d_1 + d_2 + \cdots + d_{N-1} + d_N$$

Similarly, at $t = \frac{1}{2}$:

$$S(t) = -d_1 + d_2 - d_3 + d_4 - \cdots - d_{N-1} + d_N \qquad \text{(since } N = 2^m\text{, } N \text{ is obviously even)}$$

And at $t = \frac{1}{4}$:

$$S(t) = (d_1 - d_3 + d_5 - d_7 + \cdots + d_{N-3} - d_{N-1})i + (-d_2 + d_4 - d_6 + d_8 - \cdots - d_{N-2} + d_N)$$

Recall from section 1.1 that $P(t) = SS^*$.

It is clear from the tables that in both binary and quaternary, $P(t)$ *must* have an integer value where t is a multiple of $\frac{1}{4}$. Also, it is evident that it is possible to obtain integer maxima on $P(t)$ when t is a multiple of $\frac{1}{8}$ (for example, if 8 $\frac{\sqrt{2}}{2}$ terms are added, while the ± 1 terms cancel, then $(8\frac{\sqrt{2}}{2})^2$ will give exactly 32).

It appears, however, that at values of t equal to $\frac{n}{2^m}$ where $2^m > 8$ causing sin and cos values other than ± 1, $\pm\frac{\sqrt{2}}{2}$, and 0 to appear, integer peaks can only occur when those other values cancel with each other; therefore the integers result only from combinations of ± 1, $\pm\frac{\sqrt{2}}{2}$. At positions not of the form $\frac{n}{2^m}$, integer peaks cannot form at all, since there will be no way for the complicated irrational values of the sin and cos functions to cancel with each other leaving an integer result (examine the column of *Table 1* showing the values at $t = 0.111$ for an example of this).

All of this is purely conjecture, but when the power functions of actual codewords are examined, we find that ALL integer peaks occur at positions where t is a multiple of $\frac{1}{8}$ for codes of all lengths examined (m=2,3,4, and portions of the codes m=5 and m=6). We expect that this result will hold true for all values of m.

SIN

	$t=$								
f	0	$\frac{1}{8}$	$\frac{2}{8}$	$\frac{3}{8}$	$\frac{4}{8}$	$\frac{5}{8}$	$\frac{6}{8}$	$\frac{7}{8}$	0.111
1	0	$\frac{\sqrt{2}}{2}$	1	$\frac{\sqrt{2}}{2}$	0	$-\frac{\sqrt{2}}{2}$	-1	$-\frac{\sqrt{2}}{2}$	0.642
2	0	1	0	-1	0	1	0	-1	0.984
3	0	$\frac{\sqrt{2}}{2}$	-1	$\frac{\sqrt{2}}{2}$	0	$-\frac{\sqrt{2}}{2}$	1	$-\frac{\sqrt{2}}{2}$	0.867
4	0	0	0	0	0	0	0	0	0.344
5	0	$-\frac{\sqrt{2}}{2}$	1	$-\frac{\sqrt{2}}{2}$	0	$\frac{\sqrt{2}}{2}$	-1	$\frac{\sqrt{2}}{2}$	-0.338
6	0	-1	0	1	0	-1	0	1	-0.864
7	0	$-\frac{\sqrt{2}}{2}$	-1	$-\frac{\sqrt{2}}{2}$	0	$\frac{\sqrt{2}}{2}$	1	$\frac{\sqrt{2}}{2}$	-0.986
8	0	0	0	0	0	0	0	0	-0.647
9	0	$\frac{\sqrt{2}}{2}$	1	$\frac{\sqrt{2}}{2}$	0	$-\frac{\sqrt{2}}{2}$	-1	$-\frac{\sqrt{2}}{2}$	-0.006
10	0	1	0	-1	0	1	0	-1	0.637
11	0	$\frac{\sqrt{2}}{2}$	-1	$\frac{\sqrt{2}}{2}$	0	$-\frac{\sqrt{2}}{2}$	1	$-\frac{\sqrt{2}}{2}$	0.984
12	0	0	0	0	0	0	0	0	0.870
13	0	$-\frac{\sqrt{2}}{2}$	1	$-\frac{\sqrt{2}}{2}$	0	$\frac{\sqrt{2}}{2}$	-1	$\frac{\sqrt{2}}{2}$	0.351
14	0	-1	0	1	0	-1	0	1	-0.333
15	0	$-\frac{\sqrt{2}}{2}$	-1	$-\frac{\sqrt{2}}{2}$	0	$\frac{\sqrt{2}}{2}$	1	$\frac{\sqrt{2}}{2}$	-0.861
16	0	0	0	0	0	0	0	0	-0.987

COS

	$t=$								
f	0	$\frac{1}{8}$	$\frac{2}{8}$	$\frac{3}{8}$	$\frac{4}{8}$	$\frac{5}{8}$	$\frac{6}{8}$	$\frac{7}{8}$	0.111
1	1	$\frac{\sqrt{2}}{2}$	0	$-\frac{\sqrt{2}}{2}$	-1	$-\frac{\sqrt{2}}{2}$	$-$	$\frac{\sqrt{2}}{2}$	0.766
2	1	0	-1	0	1	0	-1	0	0.175
3	1	$-\frac{\sqrt{2}}{2}$	0	$\frac{\sqrt{2}}{2}$	-1	$\frac{\sqrt{2}}{2}$	0	$-\frac{\sqrt{2}}{2}$	-0.498
4	1	-1	1	-1	1	-1	1	-1	-0.938
5	1	$-\frac{\sqrt{2}}{2}$	0	$\frac{\sqrt{2}}{2}$	-1	$\frac{\sqrt{2}}{2}$	0	$-\frac{\sqrt{2}}{2}$	-0.941
6	1	0	-1	0	1	0	-1	0	-0.503
7	1	$\frac{\sqrt{2}}{2}$	0	$-\frac{\sqrt{2}}{2}$	-1	$-\frac{\sqrt{2}}{2}$	0	$\frac{\sqrt{2}}{2}$	0.169
8	1	1	1	1	1	1	1	1	0.762
9	1	$\frac{\sqrt{2}}{2}$	0	$-\frac{\sqrt{2}}{2}$	-1	$-\frac{\sqrt{2}}{2}$	0	$\frac{\sqrt{2}}{2}$	0.999
10	1	0	-1	0	1	0	-1	0	0.771
11	1	$-\frac{\sqrt{2}}{2}$	0	$\frac{\sqrt{2}}{2}$	-1	$\frac{\sqrt{2}}{2}$	0	$-\frac{\sqrt{2}}{2}$	0.181
12	1	-1	1	-1	1	-1	1	-1	-0.493
13	1	$-\frac{\sqrt{2}}{2}$	0	$\frac{\sqrt{2}}{2}$	-1	$\frac{\sqrt{2}}{2}$	0	$-\frac{\sqrt{2}}{2}$	-0.937
14	1	0	-1	0	1	0	-1	0	-0.943
15	1	$\frac{\sqrt{2}}{2}$	0	$-\frac{\sqrt{2}}{2}$	-1	$-\frac{\sqrt{2}}{2}$	0	$\frac{\sqrt{2}}{2}$	-0.509
16	1	1	1	1	1	1	1	1	0.163

Table 2.1

3 The Quaternary m-even Case

This argument will show that there is at least one element of every quaternary Golay coset that has a peak of exactly $2N$ $(= 2^{m+1})$. The specific codeword we will use to demonstrate is $2(AB+BC+\cdots+XY+YZ)+A+Z$. Our approach takes advantage of several simplifications: the simplicity of computing the power at $t = 0$ and the ability to break down the quaternary problem into several binary problems. Recall that at $t = 0$, $P = SS^*$, where

$$S = \sum_{n=1}^{N} (i)^{(2L+A+Z)_n}$$

Note: As before, L represents the Golay coset leader $AB + BC + \cdots + XY + YZ$ (binary).

To simplify the quaternary into several binary problems, we observe that $2L + A + Z$ will contain 3's in the positions where 1's from L and a 1 from either A or Z (not both) align. This reduces to the *binary* problem of finding $L \cap (A + Z)$. In a similar, but more complicated, example:

The codeword $2L + A + Z$ will contain 2's either where
  0's from L and 1's from A and Z align
    yielding $w(AZ) - w((AZ) \cap L)$ 2's
OR
  where 1's from L align with 0's from A and Z
    yielding $w(L) - w((AZ) \cap L) - w((A + Z) \cap L)$ 2's.

Thus, there are a total of $w(AZ) + w(L) - w((A + Z) \cap L) - 2w((AZ) \cap L)$ 2's in the final codeword. Notice that these weight calculations are performed in binary.

We claim that the following conditions will hold for all even values of m:

$w(L) = 2^{m-1} - 2^{\frac{m}{2}-1}$

$w(AZ) = 2^{m-2}$

$w(A + Z) = 2^{m-1}$

$w((AZ) \cap (L)) = 2^{m-3} + 2^{\frac{m}{2}-2}$

$w((A + Z) \cap (L)) = 2^{m-2} - 2^{\frac{m}{2}-1}$

The weights of AZ and $A + Z$ are evident given the properties of Reed-Muller codes.

We will use induction to prove the other conditions for $A = x_1, B = x_2, \ldots$. Reed Muller codewords of length 2^m can be constructed by concatenating RM codewords of length 2^{m-1} by using the lemmas below. In our notation, the subscript n outside of the square brackets indicates that every x_i (where $i \in \{0, \ldots, n\}$) in the brackets is a basis vector of $RM(1, n)$. Example: $[x_1]_2 = 0011$. Concatenation is represented by a | symbol. Example: $[x_1 \mid x_1]_2 = 00110011$.

Definition: Let L_m represent the Golay coset leader $x_1x_2+x_2x_3+\cdots+x_{m-1}x_m$ of length $N=2^m$. Let **0** and **1** represent the all-0 codeword and the all-1 codeword, respectively. Let α be a binary value (0 or 1) and α' its complement.

The following lemmas outline how Reed Muller vectors of length 2^m are formed by concatenating two length 2^{m-1} Reed Muller vectors.

A second order Reed-Muller vector x_1x_{a+1} of length 2^m is formed by concatenating the all-0 vector and the RM basis vector x_a of length 2^{m-1}.

The RM basis vector x_{a+1} of length 2^m is formed by concatenating the RM basis vactor x_a of length 2^{m-1} with itself.

All of these lemmas for concatenation are both additive and multiplicative. For example, $[x_a + x_b \mid x_a+x_b]_{m-1} = [x_{a+1}+x_{b+1}]_m$ (using the lemma that $[x_a \mid x_a]_{m-1} = [x_{a+1}]_m$ and the additive properties of the binary vectors). It can be easily shown that lemmas 5 and 6 below are true because of the bitwise nature of the operations involved.

Concatenation Lemmas:

1. $[\mathbf{1} \mid \mathbf{1}]_{m-1} = [\mathbf{1}]_m$
2. $[\mathbf{0} \mid \mathbf{1}]_{m-1} = [x_1]_m$
3. $[\mathbf{0} \mid x_a]_{m-1} = [x_1x_{a+1}]_m$
4. $[x_a \mid x_a]_{m-1} = [x_{a+1}]_m$
5. $[x_a \mid x_b]_{m-1} = [y]_m$ and $[x_c \mid x_d]_{m-1} = [z]_m$
   $\Rightarrow [x_a + x_c \mid x_b + x_d]_{m-1} = [y+z]_m$
6. $[x_a \mid x_b]_{m-1} = [y]_m$ and $[x_c \mid x_d]_{m-1} = [z]_m$
   $\Rightarrow [x_ax_c \mid x_bx_d]_{m-1} = [yz]_m$

Theorem 3.1: The codeword of form $[L_m + \alpha x_1]_m$ has weight $2^{m-1} - 2^{\frac{m}{2}-1}$.

Proof: By induction. The result for m=2 is trivial ($w([x_1x_2]_2) = w(0001) = w([x_1x_2 + x_1]_2) = w(0010) = 1 = 2^{2-1} - 2^{\frac{2}{2}-1}$).

Using the lemmas above, the codeword decomposes as follows:

$$
\begin{aligned}
&[x_1x_2 + x_2x_3 + \cdots + x_{m-1}x_m + \alpha x_1]_m \\
&= [x_1x_2 + \cdots + x_{m-2}x_{m-1} \mid x_1x_2 + \cdots + x_{m-2}x_{m-1} + x_1 + \alpha\mathbf{1}]_{m-1} \\
&= [x_1x_2 + \cdots + x_{m-3}x_{m-2} \mid x_1x_2 + \cdots + x_{m-3}x_{m-2} + x_1 \mid \\
&\quad x_1x_2 + \cdots + x_{m-3}x_{m-2} + \alpha\mathbf{1} \mid x_1x_2 + \cdots + x_{m-3}x_{m-2} + x_1 + \alpha'\mathbf{1}]_{m-2} \\
&= [L_{m-2} \mid L_{m-2} + x_1 \mid L_{m-2} + \alpha\mathbf{1} \mid L_{m-2} + x_1 + \alpha'\mathbf{1}]_{m-2}
\end{aligned}
$$

Regardless of the value of α, three of the component vectors will be of the form $[L_{m-2}+\alpha x_1]_{m-2}$ and thus will have weight $2^{m-3} - 2^{\frac{m}{2}-2}$ by the induction. The remaining component is the complement of a vector of the form $[L_{m-2} + \alpha x_1]_{m-2}$ (since it has the **1**vector added to it) and thus will have weight $2^{m-2} - (2^{m-3} - 2^{\frac{m}{2}-2})$.

$$
\begin{aligned}
w([L_m + \alpha x_1]_m) &= 3(w([L_{m-2} + \alpha x_1]_{m-2})) + 2^{m-2} - w([L_{m-2} + \alpha x_1]_{m-2}) \\
&= 3(2^{m-3} - 2^{\frac{m}{2}-2}) + 2^{m-2} - (2^{m-3} - 2^{\frac{m}{2}-2})
\end{aligned}
$$

$$\mathbf{Thus}\ \boldsymbol{w([L_m + \alpha x_1]_m) = 2^{m-1} - 2^{\frac{m}{2}-1}}$$

Q.E.D.

The codeword $[L_m + x_m]_m$ is formed by a permutation of the mapping of the codeword $[L_m + \alpha x_1]_m$ and therefore must have equivalent weight (consult section 1.5).

Theorem 3.2: The codeword of form $[L_m + x_1 + x_m]_m$ has weight $2^{m-1} + 2^{\frac{m}{2}-1}$.

Proof: By induction. Evident for m=2. The first codeword decomposes as follows:

$$\begin{aligned}
&[x_1x_2 + x_2x_3 + \cdots + x_{m-1}x_m + x_1 + x_m]_m \\
&= [x_1x_2 + \cdots + x_{m-3}x_{m-2} + x_{m-1} \ \mid \ x_1x_2 + \cdots + x_{m-3}x_{m-2} + x_1 + x_{m-1} + \mathbf{1}]_{m-1} \\
&= [x_1x_2 + \cdots + x_{m-3}x_{m-2} + x_{m-2} \ \mid \ x_1x_2 + \cdots + x_{m-3}x_{m-2} + x_{m-2} + x_1 \ \mid \\
&\quad x_1x_2 + \cdots + x_{m-3}x_{m-2} + x_{m-2} + \mathbf{1} \ \mid \ x_1x_2 + \cdots + x_{m-3}x_{m-2} + x_1 + x_{m-2}]_{m-2} \\
&= [L_{m-2} + x_{m-2} \ \mid \ L_{m-2} + x_{m-2} + x_1 \ \mid \ L_{m-2} + x_{m-2} + \mathbf{1} \ \mid \ L_{m-2} + x_1 + x_{m-2}]_{m-2}
\end{aligned}$$

The two components of form $[L_{m-2} + x_1 + x_{m-2}]_{m-2}$ both have weight $2^{m-3} + 2^{\frac{m}{2}-2}$ (by induction). The component of form $[L_{m-2} + x_{m-2}]_{m-2}$ has weight $2^{m-3} - 2^{\frac{m}{2}-2}$. And the remaining component is the complement of $[L_{m-2} + x_{m-2}]_{m-2}$, and thus will have weight $2^{m-2} - (2^{m-3} + 2^{\frac{m}{2}-2})$.

$$\begin{aligned}
w([L_m + x_1 + x_m]_m) &= 2(w([L_{m-2} + x_1 + x_{m-2}]_{m-2})) + w([L_{m-2} + x_{m-2}]_{m-2}) \\
&\quad + 2^{m-2} - w([L_{m-2} + x_{m-2}]_{m-2}) \\
&= 2(2^{m-3} + 2^{\frac{m}{2}-2}) + 2^{m-3} - 2^{\frac{m}{2}-2} + 2^{m-2} - (2^{m-3} + 2^{\frac{m}{2}-2})
\end{aligned}$$

Thus $w([L_m + x_1 + x_m]_m) = 2^{m-1} + 2^{\frac{m}{2}-1}$ **Q.E.D.**

Theorem 3.3: The codeword of form $[L_m + x_1x_m]_m$ has weight $2^{m-1} - 2^{\frac{m}{2}}$

Proof: This codeword decomposes as follows:

$$\begin{aligned}
&[x_1x_2 + x_2x_3 + \cdots + x_{m-1}x_m + x_1x_m]_m \\
&= [x_1x_2 + \cdots + x_{m-2}x_{m-1} \ \mid \ x_1x_2 + \cdots + x_{m-2}x_{m-1} + x_1 + x_{m-1}]_{m-1} \\
&= [x_1x_2 + \cdots + x_{m-3}x_{m-2} \ \mid \ x_1x_2 + \cdots + x_{m-3}x_{m-2} + x_1 \ \mid \\
&\quad x_1x_2 + \cdots + x_{m-3}x_{m-2} + x_{m-2} \ \mid \ x_1x_2 + \cdots + x_{m-3}x_{m-2} + x_1 + x_{m-2} + \mathbf{1}]_{m-2} \\
&= [L_{m-2} \ \mid \ L_{m-2} + x_{m-2} \ \mid \ L_{m-2} + x_{m-2} \ \mid \ L_{m-2} + x_1 + x_{m-2} + \mathbf{1}]_{m-2}
\end{aligned}$$

Here, no induction is involved – the component vectors are in forms for which the weights have previously been proven. Summing the appropriate weight values for the components results in:

$$\begin{aligned}
w([L_m + x_1x_m]_m) &= w([L_{m-2}]_{m-2}) + w([L_{m-2} + x_1]_{m-2}) + w([L_{m-2} + x_{m-2}]_{m-2}) \\
&\quad + 2^{m-2} - w([L_{m-2} + x_1 + x_{m-2}]_{m-2}) \\
&= 3(2^{m-3} - 2^{\frac{m}{2}-2}) + 2^{m-2} - (2^{m-3} + 2^{\frac{m}{2}-2})
\end{aligned}$$

Thus $w([L_m + x_1x_m]_m) = 2^{m-1} - 2^{\frac{m}{2}}$ **Q.E.D.**

This proves that the given weight formulas are true for $A = x_1, B = x_2, \ldots$. Based on the weight equivalence property previously discussed, *any* mapping of the basis vectors $v_1, \ldots, v_m$ onto the vectors $A, \ldots, Z$ will result in an equivalent weight codeword of the form $AB + BC + \cdots + YZ$.

From these conditions it neccessarily follows that the quaternary codeword $2L + A + Z$ will contain:

symbol	*number of times symbol appears in $2L + A + Z$ (quaternary)*
1 (i)	$w(A + Z) - w((A + Z) \cap (L))$ $= 2^{m-1} - (2^{m-2} - 2^{\frac{m}{2}-1})$ $= \mathbf{2^{m-2} + 2^{\frac{m}{2}-1}}$
2 (-1)	$w(AZ) + w(L) - w((A + Z) \cap (L)) - 2w((AZ) \cap (L))$ $= 2^{m-2} + (2^{m-1} - 2^{\frac{m}{2}-1}) - (2^{m-2} - 2^{\frac{m}{2}-1}) - 2(2^{m-3} - 2^{\frac{m}{2}-2} + 2^{\frac{m}{2}-1})$ $= \mathbf{2^{m-2} - 2^{\frac{m}{2}-1}}$
3 ($-i$)	$w((A + Z) \cap (L))$ $= \mathbf{2^{m-2} - 2^{\frac{m}{2}-1}}$
0 (1)	$2^m -$(# of '1's + # of '2's + # of '3's) $= \mathbf{2^{m-2} + 2^{\frac{m}{2}-1}}$

Table 2

Example ($m = 4$):

$A = V_1, B = V_2, C = V_3, D = V_4$

$$\begin{array}{ll} \{0,1,0,1,0,1,0,1,1,2,1,2,1,2,1,2\} & (A+D) \\ +\ \{0,0,0,2,0,0,2,0,0,0,0,2,2,2,0,2\} & 2(AB+BC+CD) \\ = \{0,1,0,3,0,1,2,1,1,2,1,0,3,0,1,0\} & \\ \equiv \{1,i,1,i,-i,1,i,-1,i,i,-1,i,1,-i,1,i,1\} & \end{array}$$

Observe that (in *binary*):
$w(A+D) = 2^{4-1} = 8$
$w(AD) = 2^{4-2} = 4$
$w(L) = 2^{4-1} - 2^{\frac{4}{2}-1} = 6$
$w((AD) \cap L) = 2^{4-3} + 2^{\frac{4}{2}-2} = 3$
$w((A+D) \cap L) = 2^{4-2} - 2^{\frac{4}{2}-1} = 2$
So, our claims hold in this example.

The important result of this section is:

Theorem 3.4: The codeword $2L + A + Z$ over $\mathbf{Z}_4$ has peak power exactly equal to 2^{m+1}. Thus, every coset of the form $2L + RM(1, m)$ over $\mathbf{Z}_4$ has a codeword which achieves maximum power.

Proof: Using the number of symbol occurrences from *Table 2* in the formula $S(t) = d_1 + \cdots + d_N$:

$$\begin{aligned} S(t) &= (2^{m-2} + 2^{\frac{m}{2}-1})i + (2^{m-2} - 2^{\frac{m}{2}-1})(-i) + (2^{m-2} + 2^{\frac{m}{2}-1})(-1) + (2^{m-2} + 2^{\frac{m}{2}-1})1 \\ &= 2^{\frac{m}{2}} + (2^{\frac{m}{2}})i \\ P(t) &= SS^* = 2^m \end{aligned}$$

Q.E.D.

4 The m-odd Cases

The coset leader L_m $(AB + BC + \cdots + XY + YZ)$ has a peak of exactly 2^{m-1} at position $t = 0$ when m is odd. Note that the simplified power formula for $t = 0$ is easily computed from the weight of the codeword being considered.

Theorem 4.1: The codeword L_m has weight $2^{m-1} - 2^{(m-1)/2}$.

Proof: Using the concatenation lemmas from the previous section, L_m decomposes as follows:

$$\begin{aligned}
&[x_1x_2 + x_2x_3 + \cdots + x_{m-1}x_m]_m \\
&= [x_1x_2 + \cdots + x_{m-2}x_{m-1} \ \mid \ x_1x_2 + \cdots + x_{m-2}x_{m-1} + x_1]_{m-1} \\
&= [L_{m-1} \ \mid \ L_{m-1} + x_1]_{m-1}
\end{aligned}$$

Now, substituting the weight formulas derived in the previous section, both of those components have weight $2^{m-2} - 2^{\frac{m-1}{2}-1}$ (since m is odd, $m-1$ is even and the formulas from last section are appropriate).

Thus $w([L_m]_m) = 2^{m-1} - 2^{\frac{m-1}{2}}$

Q.E.D.

This leads to the following conclusion:

Theorem 4.2: The coset leader L_m has peak power exactly equal to 2^{m+1} for m odd. Therefore, every coset $L + RM(1, m)$ over $\mathbf{Z}_4$ for m-odd has a codeword which achieves the maximum power.

Proof: Using the simplified power formula for $t = 0$, this essentially means that the number of surplus 1's (those which are not cancelled out by 0's) squared gives the max power desired, because:

$$\begin{aligned}
P(0) &= (w(L) - (2^m - w(L)))^2 \\
&= \left(2^m - 2\left(2^{m-1} - 2^{(m-1)/2}\right)\right)^2 \\
&= \left(2^m - 2^m + 2^{(m+1)/2}\right)^2
\end{aligned}$$

Thus $P(0) = 2^{m+1}$

Q.E.D.

5 Argument that binary Golay cosets do not contain an integer max of 32

The following is an incomplete argument that there cannot be integer peak powers of 32 in any binary Golay coset, based upon our previous argument that integer powers can only occur at a limited number of positions. The power computation is greatly simplified at these positions and we will examine each of them individually.

At t = 0 $S = (d_1 + d_2 + d_3 + \cdots + d_{16})$ $P = SS^*$

Since all the $d_n s$ assume values of ± 1 in binary, S will be an integer.

Similarly, at $t = \frac{1}{2}$ $S = (-d_1 + d_2 - d_3 + \cdots - d_{15} + d_{16})$ $P = SS^*$

Again, all of the $d_n s$ will be ± 1, and S will be an integer. Since there is no integer-valued solution to $SS^* = 32$, there cannot be a peak of 32 at position t = 0 or at $t = \frac{1}{2}$.

At $t = \frac{1}{4}$ $P = (d_1 - d_3 + d_5 + \cdots + d_{13} - d_{15})^2 + (-d_2 + d_4 - d_6 + \cdots - d_{14} + d_{16})^2$
At $t = \frac{3}{4}$ $P = (-d_1 + d_3 - d_5 + \cdots - d_{13} + d_{15})^2 + (-d_2 + d_4 - d_6 + \cdots - d_{14} + d_{16})^2$

For the power to equal 32 at these postions, both the sum of the odd terms and the sum of the even terms must go to ± 4. In each of the sums half of the terms are added and half are subtracted. Thus, to assume a value of ± 4, the d_n values for n-odd must be a $6 - 2$ pattern of pluses and minuses. The d_n for n-even must also have a $6 - 2$ pattern. If the same value occurs 6 times among the odd terms and 6 times among the even terms, then there will be a 12-4 pattern overall which will produce a power of $(12-4)^2$ at t = 0(see above), so the power of 32 will not be a peak. Similarly, if the value occuring 6 times among odd terms is different than the one occuring 6 times among the even terms, at $t = \frac{1}{2}$ all the odd terms will be subtracted again yielding $P = (12 - 4)^2 = 64$. Therefore, anytime a codeword has a power of 32 at $t = \frac{1}{4}$ or $t = \frac{3}{4}$ it must necessarily have a higher power of 64 at either $t = 0$ or $t = \frac{1}{2}$, so 32 is not a peak.

At $t = \frac{1}{8}$ $P = (\frac{\sqrt{2}}{2}d_1 - \frac{\sqrt{2}}{2}d_3 - d_4 - \frac{\sqrt{2}}{2}d_5 + \frac{\sqrt{2}}{2}d_7 + d_8 + \cdots + \frac{\sqrt{2}}{2}d_{16})^2$
$+(\frac{\sqrt{2}}{2}d_1 d_2 + \frac{\sqrt{2}}{2}d_3 - \frac{\sqrt{2}}{2}d_5 - d_6 + \frac{\sqrt{2}}{2}d_7 + \frac{\sqrt{2}}{2}d_9 + \cdots - \frac{\sqrt{2}}{2}d_{15})^2$

To make P = 32 the codeword must either be such that both the sums assume values of ± 4 (meaning that all of the terms multiplied by $\frac{\sqrt{2}}{2}$ cancel out) or that one sum assumes the value $8\frac{\sqrt{2}}{2}$ and the other sum assumes the value 0 (requiring that all of the real terms cancel). Demonstrating that this can not occur requires examining a large number of special cases and we were unable to develop a reasonable approach to solving this problem.

Develpment of a generalized method for this problem that does not require case-by-case analysis would be beneficial.

6 Areas for Further Investigation

The preceeding proofs for the m-even quaternary and the m-odd cases prove that there is at least one peak of 2^{m+1} within each of the Golay cosets. It appears that a large portion of the members of the m-even quaternary Golay cosets (160 out of the 256 elements for $m = 4$) and all of the members of the m-odd Golay cosets have peak power of 2^{m+1}(Appendix B). The case for m-odd is especially interesting, because in the cases examined ($m = 3$ and $m = 5$) exactly half of the elements had peaks at $t = 0$. It seems probable that additional rules (and accompnying proofs) can be found to characterize the peak-forming behavior of many or all of the elements in the Golay cosets. Further research into the distribution of peak powers within the Golay cosets for both m-even and m-odd should be conducted. It is worth observing that there are also many interesting peak-formation behaviors among non-Golay cosets as well, and research into this are would also be extremely valuable.

Our conjecture about integer peaks occuring at only positions where t is a multiple of $\frac{1}{8}$ was only tentatively argued. The properties of integer peak formation should be further researched. If possible, properties should be proven.

In the m-even Golay cosets, the binary codewords never achieve a peak power of 2^{m+1}. We began arguing this result in the $m = 4$ case, but general proofs are necessary.

Appendix A
Listings by Coset

This table lists all the cosets of $RM(1,4)$ in $RM(2,4)$ over $\mathbf{Z}_2$, and the highest power found in any element for each of the cosets. It is presented in sorted order based on the max power. Observe that the first 12 cosets (the ones containing only elements with peaks below 32) are the 12 Golay cosets.

This table is similar to that on the previous page, but computed over $\mathbf{Z}_4$. Notice that changing from $\mathbf{Z}_2$ to $\mathbf{Z}_4$ causes the max values to all assume integer values that are powers of 2.

Appendix B
Detailed Listings Within a Coset

This table lists all of the elements of a single Golay coset, as an illustration of the m-odd case in $\mathbf{Z}_2$. All of the elements have peaks of exactly 64. In this coset, exactly half of them occur at position $t = 0$ and half at $t = \frac{1}{2}$ (note: the $t = \frac{1}{2}$ positions are listed as position 16 in this table. That was the notation used by our software originally).

This table is a detailed listing of all the elements of a single Golay coset illustrating the power behavior of the m-even case in $\mathbf{Z}_4$. There are 160 elements with power maxima of exactly 32. All occur at positions where t is a multiple of $\frac{1}{8}$.

(continuation of previous page)

References

[Macwilliams/Sloane] F.J. MacWilliams, N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Mathematical Library, NY. 1986.

[Davis/Jedwab] J.A. Davis, J. Jedwab. "Peak-to-Mean Power Control and Error Correction for OFDM Transmission Using Golay Sequences and Reed-Muller Codes" *Electronic Letters* 13 Feb. 1997, Vol. 33, No. 4, pp 267–268.

[Golay] M.J.E. Golay. "Complementary Series" *IRE Trans. Int. Theory* 1961, 7, pp. 82–7.