Derivatives of Complete Weight Enumerators and New Balance Principle of Binary Self-Dual Codes

Vassil Yorgov
Department of Mathematics and Computer Science
Fayetteville State University
1200 Murchison Rd
Fayetteville, NC 28311

July 5, 2022

Abstract

Let $K = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. It is known that the complete weight enumerator $W$ of a binary self-dual code of length $n$ is an eigenvector corresponding to an eigenvalue 1 of the Kronecker power $K[n]$. For every integer $t$, $0 \leq t \leq n$, we define the $t$-th derivative $W_{<t>}$ of $W$ in such a way that $W_{<t>}$ is in the eigenspace of 1 of the matrix $K[n-t]$. For large values of $t$, $W_{<t>}$ contains less information about the code but has smaller length while $W_{<0>} = W$ completely determines the code. We compute the derivative of order $n-5$ for the extended Golay code of length 24, the extended quadratic residue code of length 48, and the putative [72,24,12] code and show that they are in the eigenspace of 1 of the matrix $K[5]$. We use the derivatives to prove a new balance equation which involves the number of code vectors of given weight having 1 in a selected coordinate position. As an example, we use the balance equation to eliminate some candidates for weight enumerators of binary self-dual codes of length eight.

1 Introduction

In this work, we use the standard notation of error correcting codes. An appropriate reference is the book [4]. Let $C$ be a binary linear self-dual code of length $n$. Thus $C$ is a linear subspace of dimension $n/2$ of the vector space $F^n$, where $F$ is the binary field, and $C$ is equal to its orthogonal code with respect to the usual dot product. The exact weight enumerator of $C$ is a row vector $W$ of length $2^n$ with integer entries labeled with the vectors from $F^n$ listed in lexicographic order. The entry $W[v]$ labeled with a vector $v$ is defined with

$$W[v] = \begin{cases} 1 & \text{if } v \in C \\ 0 & \text{if } v \notin C. \end{cases}$$
Thus $W$ belongs to the vector space $Q^{2^n}$ where $Q$ is the rational field. Clearly the exact weight enumerator $W$ determines completely the code $C$.

Let $K = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $K^2 = K \otimes K$, $K^3 = K^2 \otimes K$, and let $K^{[n]} = K^{[n-1]} \otimes K$, be the $n$-th Kronecker power of $K$. A summary of the properties of Kronecker products of matrices is given in [10]. Let $R$ be the real number field. The matrix $K$ has eigenvalues $1$ and $-1$. The vectors $(1, \sqrt{2} - 1)$ and $(1, -\sqrt{2} - 1)$ are eigenvectors of $K$ corresponding to $1$ and $-1$. Therefore, $K$ is simple, meaning that there exist a basis of $R^2$ consisting of eigenvectors of $K$. The rows of the matrix

\[ B = \begin{bmatrix} 1 & \sqrt{2} - 1 \\ 1 & -\sqrt{2} - 1 \end{bmatrix} \]

form such basis of $R^2$. It follows that the matrix $K^{[n]}$ is also simple and has eigenvalues $1$ and $-1$, [5] page 413. The rows of the Kronecker power $B^{[n]}$ form a basis of $R^{2^n}$. We label the rows of $B^{[n]}$ with the vectors from $F^n$ listed in lexicographic order.

**Lemma 1** The rows of $B^{[n]}$ with even weight labels form a basis of the eigenspace of $1$ of $K^{[n]}$.

**Proof.** We have $BK = DB$ where

\[ D = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \]

Using the properties of Kronecker power, we obtain $(BK)^{[n]} = (DB)^{[n]}$ and $B^{[n]}K^{[n]} = D^{[n]}B^{[n]}$. Since the diagonal matrix $D^{[n]}$ has $1$ on the rows labeled with even weight vectors and $-1$ on the rows labeled with odd weight vectors, the lemma follows from the last equality.

The next lemma is a particular case of a result proved in [8].

**Lemma 2** [8] The complete weight enumerator $W$ of the binary self-dual code $C$ belongs to the eigenspace of $1$ of the matrix $K^{[n]}$. Moreover, any nontrivial $(0,1)$ vector from the eigenspace of $1$ of the matrix $K^{[n]}$ determines a self-dual binary code.

Since $2^n$ increases very rapidly with $n$, this lemma is not practical when the code length $n$ increases. In the next section we define derivatives of $W$ which contain less information about the code $C$ but have smaller size.

## 2 Derivatives of the Complete Weight Enumerator

Let $\rho = \sqrt{2} - 1$ and $\mu = -\sqrt{2} - 1$. The quadratic extension $Q(\rho)$ has automorphism group of order two generated by the automorphism $\Phi : Q(\rho) \to Q(\rho)$ defined with $\Phi(\rho) = \mu$. 

Definition 3 For every integer $t$, $0 \leq t \leq n$, the $t$-th derivative of $W$ is the row vector $W_{<t>}$ of length $2^{n-t}$ having an entry with label $v \in F^{n-t}$ determined by

$$W_{<t>}[v] = \sum_{u \in F^t} \rho^{wt(u)} W[uv]$$

where $wt(u)$ is the Hamming weight of $u$ and $uv$ is the concatenation of $u$ and $v$.

For example, if $u = (1, 1, 0, 1)$ and $v = (1, 0)$, then $uv = (1, 1, 0, 1, 1, 0)$. It follows that every derivative $W_{<t>}$ has nonnegative entries from the quadratic extension $Q(\rho)$. Particularly, $W_{<n>}$ is determined by the weight distribution of $C$.

Lemma 4

$$W_{<n>} = \sum_{u \in F^n} \rho^{wt(u)} W[u] = \sum_{k=0}^{n} A_k \rho^k$$

where $A_k$ is the number of weight $k$ vectors in $C$.

Thus $W_{<n>} \in Q(\rho)$ and contains less information about $C$ than the weight distribution of $C$. On the other end, $W_{<0>} = W$ determines the code $C$ completely.

Lemma 5 For every integer $t$, $0 \leq t \leq n-1$ and for every $v \in F^{n-t-1}$, we have $W_{<t+1>}[v] = W_{<t>}[0v] + \rho W_{<t>}[1v]$.

Proof. The proof is straightforward:

$$W_{<t+1>}[v] = \sum_{u' \in F^{t+1}} \rho^{wt(u')} W[u'v]$$

$$= \sum_{u \in F^t} \rho^{wt(u)} W[u(0)v] + \sum_{u \in F^t} \rho^{wt(u(1))} W[u(1)v]$$

$$= \sum_{u \in F^t} \rho^{wt(u)} W[u(0)v] + \rho \sum_{u \in F^t} \rho^{wt(u)} W[u(1)v]$$

$$= W_{<t>}[0v] + \rho W_{<t>}[1v].$$

Less formally, $W_{<t+1>} = W_{<t>}[0] + \rho W_{<t>}[1]$ where $W_{<t>}[0]$ is the first half and $W_{<t>}[1]$ is the second half of $W_{<t>}$. The next lemma shows that every entry of the second half of $W_{<t>}$ depends only on a corresponding entry from the first half of $W_{<t>}$.

Lemma 6 For every integer $t$, $0 \leq t \leq n-1$ and for every $v \in F^{n-t-1}$, we have $W_{<t>}[1v] = (-1)^{wt(v)} \rho \Phi(W_{<t>}[0v])$ where $\Phi$ is the complementary vector of $v$ and $\Phi$ is the automorphism of $Q(\rho)$ defined above.
Proof. As the all one vector is in the code $C$, for any $u \in F^t$ we have $W[u(1)\overline{v}] = W[u(0)v]$ where $\overline{v}$ and $v$ are the complementary vectors of $u$ and $v$. By Definition 3,

$$W_{<t>}[1\overline{v}] = \sum_{u \in F^t} \rho^{wt(u)} W[u(1)\overline{v}]$$

$$= \sum_{u \in F^t} \rho^{wt(u)} W[u(0)v]$$

$$= \sum_{u \in F^t} \rho^{t-wt(u)} W[u(0)v]$$

$$= \rho^{t} \sum_{u \in F^t} \rho^{-wt(u)} W[u(0)v]$$

We check that $\rho^{-1} = -\mu$. Because $C$ contains only even weight vectors, $W[u(0)v] = 0$ when $wt(u)$ and $wt(v)$ have different parities. Therefore

$$W_{<t>}[1\overline{v}] = \rho^{t} \sum_{u \in F^t} (-\mu)^{wt(u)} W[u(0)v]$$

$$= \rho^{t} (-\mu)^{wt(v)} \sum_{u \in F^t} \mu^{wt(u)} W[u(0)v]$$

$$= \rho^{t} (-\mu)^{wt(v)} \Phi \left( \sum_{u \in F^t} \mu^{wt(u)} W[u(0)v] \right)$$

$$= (-1)^{wt(v)} \rho^{t} \Phi (W_{<t>}[0\overline{v}])$$

Theorem 7 For every integer $t$, $0 \leq t \leq n$, the $t$-th derivative $W_{<t>}$ belongs to the eigenspace of 1 of $K[n-t]$.

Proof. The statement of the theorem is true for $W_{<0>} = W$ from Lemma 2. Thus $WK[n] = W$. Since $W = (W[0]W[1])$ (recall that this is the concatenation of $W[0]$ and $W[1]$) and

$$K[n] = K \otimes K^{n-1} = \frac{1}{\sqrt{2}} \begin{bmatrix} K^{n-1} & \overline{K}^{n-1} \\ K^{n-1} & -K^{n-1} \end{bmatrix}$$

we have

$$\frac{1}{\sqrt{2}} (W[0] + W[1])K^{n-1} = W[0]$$

$$\frac{1}{\sqrt{2}} (W[0] - W[1])K^{n-1} = W[1].$$

By adding and then subtracting these equations, we obtain

$$W[0]K^{n-1} = \frac{1}{\sqrt{2}} (W[0] + W[1])$$

$$W[1]K^{n-1} = \frac{1}{\sqrt{2}} (W[0] - W[1]).$$
Now it is easy to check that
\[
\left(W[0] + \left(\sqrt{2} - 1\right)W[1]\right)K^{[n-1]} = \frac{1}{\sqrt{2}} (W[0] + W[1]) + \frac{\sqrt{2} - 1}{\sqrt{2}} (W[0] - W[1])
\]
\[
= W[0] + \frac{2 - \sqrt{2}}{\sqrt{2}} W[1]
\]
\[
= W[0] + \left(\sqrt{2} - 1\right) W[1].
\]
Hence, \(W_{<1>} = W_{<0>}[0] + \rho W_{<0>}[1] = W[0] + (\sqrt{2} - 1) W[1]\) is in the eigenspace of 1 of \(K^{[n-1]}\).
From this, we prove similarly that \(W_{<2>} = W_{<1>}[0] + \rho W_{<1>}[1]\) is in the eigenspace of 1 of \(K^{[n-2]}\).
Using Lemma 5, we complete the proof by induction on \(t\). ■

3 A Balance Principle for Self-Dual Codes

**Theorem 8** Let \(t\) be a selected coordinate position of \(C\), let \(\delta \in F = \{0, 1\}\), and let \(A_{k, \delta}\) be the cardinality of the set
\[
\{ v \in C \mid wt(v) = k \text{ and } v[t] = \delta \}.
\]
Then \(\sum_{k=0}^{n} A_{k, 1} \rho^{k-1} = \sum_{k=0}^{n} A_{k, 0} \rho^{k+1}\) and \(\sum_{k=0}^{n} A_{k, 1} \rho^{k-1} = \frac{1 + \rho}{1 + \rho^2} W_{<n>}\). Particularly, \(\sum_{k=0}^{n} A_{k, 1} \rho^{k-1}\) does not depend on the selection of \(t\).

**Proof.** Let \(t = n\). From Theorem 6, \(W_{<n-1>} = (W_{<n-1>}[0]W_{<n-1>}[1])\) is in the eigenspace of 1 of \(K\), which is generated by vector \((1, \rho)\). Therefore, \(W_{<n-1>}[1] = \rho W_{<n-1>}[0]\). Since
\[
W_{<n-1>}[1] = \sum_{u \in F^{n-1}} \rho^{wt(u)} W[u](1) = \sum_{k=0}^{n} A_{k, 1} \rho^{k-1}
\]
\[
W_{<n-1>}[0] = \sum_{u \in F^{n-1}} \rho^{wt(u)} W[u](0) = \sum_{k=0}^{n} A_{k, 0} \rho^{k}
\]
we obtain the first equality of the Theorem. From Lemma 5, \(W_{<n>} = W_{<n-1>}[0] + \rho W_{<n-1>}[1]\). Thus \(W_{<n>} = W_{<n-1>}[0] + \rho^2 W_{<n-1>}[0]\). Using Lemma 4, we obtain \(\sum_{k=0}^{n} A_{k} \rho^k = (1 + \rho^2) W_{<n-1>}[0]\) and \(W_{<n-1>}[0] = \frac{1}{1 + \rho^2} \sum_{k=0}^{n} A_{k} \rho^k\).
Then \(W_{<n-1>}[1] = \frac{\rho}{1 + \rho^2} \sum_{k=0}^{n} A_{k} \rho^k\). Since \(\frac{1}{1 + \rho^2} = \frac{1 + \rho}{1 + \rho^2}\), we obtain the second equality of the Theorem.
If \(t \neq n\), we apply a permutation to the coordinates of \(C\) which sends \(t\) to \(n\). Since equivalent codes have the same weight distribution, the statement of the Theorem holds for \(t \neq n\). ■
4 Examples

4.1 Binary Self-Dual Codes of Length 8

There are two binary self-dual codes of length 8 [7]. They have weight enumerators

\[ W_a = (1, 0, 0, 0, 14, 0, 0, 0, 1) \]

\[ W_b = (1, 0, 4, 0, 6, 0, 4, 0, 1). \]

Here the entry \( A_k \) in position \( 1+k \) is equal to the number of code vectors of weight \( k, k = 0, 1, \ldots, 8. \)

Each of these weight enumerators satisfies the equation \( XM = 2^4 X \) where \( M \) is the transpose of the Krawtchouk matrix \( K_8 \). The entry of \( K_n \) in row \( i \) and column \( j \) is

\[
\sum_{m=0}^{i} (-1)^m \binom{j}{m} \binom{n-j}{i-m}.
\]

Using computer algebra system Magma [2], we determine all solutions of this equation with nonnegative integer entries. They are:

\[
(1, 0, 0, 0, 14, 0, 0, 0, 1), (1, 0, 1, 0, 12, 0, 1, 0, 1),
(1, 0, 20, 10, 0, 20, 1), (1, 0, 30, 8, 0, 30, 1),
(1, 0, 4, 0, 6, 0, 40, 1), (1, 0, 5, 0, 4, 0, 5, 0, 1),
(1, 0, 6, 0, 20, 6, 0, 1), (1, 0, 7, 0, 0, 0, 7, 0, 1).
\]

Let \( A_{k,0} = y \) for a self-dual binary code realizing some of these solutions. Then we can express the possible nonzero values of \( A_{k,0} \) and \( A_{k,1} \) with \( y \). We have

| \( k \) | 0 | 2 | 4 | 6 | 8 |
|-------|---|---|---|---|---|
| \( A_{k,0} \) | 1 | \( \frac{1}{4} A_4 \) | \( A_2 - y \) | 0 |
| \( A_{k,1} \) | 0 | \( A_2 - y \) | \( \frac{1}{4} A_4 \) | 1 |

For each of the eight possible weight enumerators we solve for \( y \) the balance equation from Theorem 7. The found values of \( y \) are 0, \( \frac{3}{4} \), \( \frac{3}{2} \), 3, \( \frac{15}{4} \), \( \frac{9}{2} \), \( \frac{21}{4} \). Since \( y \) must be a nonnegative integer, all possible weight enumerators except for \( W_a \) and \( W_b \).

4.2 The Golay Code of Length 24

This well known code is the only binary self-dual code of length 24 with minimum weight 8 [6]. The nonzero entries of the weight distribution of this code are \( A_0 = 1, A_8 = 759, A_{12} = 2576, A_{16} = 759, A_{24} = 1. \) The supports of all code vectors of weight 8, 12, and 16 form 5-designs [1]. Hence we can compute all values \( A_{k,0} \) and \( A_{k,1} \). The result is given in the table

| \( k \) | 0 | 8 | 12 | 16 | 24 |
|-------|---|---|----|----|----|
| \( A_{k,0} \) | 1 | 506 | \( \frac{2227}{2} \) | 759 - 506 | 0 |
| \( A_{k,1} \) | 0 | 759 - 506 | \( \frac{2227}{2} \) | 506 | 1 |

These values satisfy the balance equation of Theorem 7.

Using the three 5-design supported by the code wards of weight 8, 12, and 16, we compute the derivative \( W_{<19>} \) and check that it satisfies the equation \( W_{<19>} K^{[5]} = W_{<19>}. \) Its entries are given below:

-1167936*p + 483776, 1202240* - 497984
4.3 The Extended Quadratic Residue Code of Length 48

This is the only \([48,24,12]\) binary self-dual code [3]. The supports of all code vectors of weight 12, 16, 20, 24, 28, 32, and 36 form 5-designs [1]. This allows us to compute the derivative \(W_{<43>}\) and to check that \(W_{<43>} R^{[5]} = W_{<43>}\). The entries of \(W_{<43>}\) are

\[
1202240*p - 497984, -1180608*p + 489024, \\
1202240*p - 497984, -1180608*p + 489024, \\
-1180608*p + 489024, 1023936*p - 424128, \\
1202240*p - 497984, -1180608*p + 489024, \\
-1180608*p + 489024, 1023936*p - 424128, \\
1023936*p - 424128, -750144*p + 310720, \\
1202240*p - 497984, -1180608*p + 489024, \\
-1180608*p + 489024, 1023936*p - 424128, \\
1023936*p - 424128, -750144*p + 310720, \\
-1180608*p + 489024, 1023936*p - 424128, \\
1023936*p - 424128, -750144*p + 310720, \\
-1180608*p + 489024, 1023936*p - 424128, \\
-1180608*p + 489024, 1023936*p - 424128, \\
1749670572392448*p - 724737280770048, \\
1799773991403520*p - 745490796445696, \\
1799773991403520*p - 745490796445696, \\
-1787591301070848*p + 740444560883712, \\
1799773991403520*p - 745490796445696, \\
-1787591301070848*p + 740444560883712, \\
-1787591301070848*p + 740444560883712, \\
-1787591301070848*p + 740444560883712, \\
-1666630947373056*p + 690341141872640, \\
1799773991403520*p - 745490796445696, \\
-1787591301070848*p + 740444560883712, \\
-1787591301070848*p + 740444560883712, \\
-1787591301070848*p + 740444560883712, \\
1749670572392448*p - 724737280770048, \\
-1787591301070848*p + 740444560883712, \\
-1787591301070848*p + 740444560883712, \\
1749670572392448*p - 724737280770048, \\
1749670572392448*p - 724737280770048, \\
1749670572392448*p - 724737280770048, \\
-1666630947373056*p + 690341141872640, \\
1799773991403520*p - 745490796445696, \\
-1787591301070848*p + 740444560883712, \\
-1787591301070848*p + 740444560883712, \\
1749670572392448*p - 724737280770048, \\
-1787591301070848*p + 740444560883712, \\
-1787591301070848*p + 740444560883712, \\
1749670572392448*p - 724737280770048, \\
-1787591301070848*p + 740444560883712, \\
-1787591301070848*p + 740444560883712, \\
1749670572392448*p - 724737280770048, \\
-1787591301070848*p + 740444560883712, \\
-1787591301070848*p + 740444560883712, \\
1749670572392448*p - 724737280770048, \\
-1787591301070848*p + 740444560883712, \\
-1787591301070848*p + 740444560883712, \\
1749670572392448*p - 724737280770048, \\
-1787591301070848*p + 740444560883712, \\
-1787591301070848*p + 740444560883712, \\
1749670572392448*p - 724737280770048, \\
-1787591301070848*p + 740444560883712, \\
1749670572392448*p - 724737280770048, \\
-1666630947373056*p + 690341141872640, \\
-750144*p + 310720, 7081024*p - 2933056, \\
\]
4.4 The Putative [72,36,16] Binary Self-Dual Code

The existence of this code is a long standing open question [9]. Its weight enumerator is known:

\[
\begin{align*}
&<0,1>,<16,249849>,<20,18106704>,<24,462962955>,<28,4397342400>,<32,16602715899>, \\
&<36,25756721120>,<40,16602715899>,<44,4397342400>,<48,462962955>,<52,18106704>, \\
&<56,249849>,<72,1>.
\end{align*}
\]

The supports all code vectors of weight 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, and 56 form 5-designs [1]. Using this designs, we compute the derivative \( W_{<67>} \) and check that \( W_{<67>^2} = W_{<67>} \). The entries of \( W_{<67>} \) are

\[
\begin{align*}
&-1787591301070848^*p + 74044560883712, \\
&1749670572392448^*p - 724737280770048, \\
&1749670572392448^*p - 724737280770048, \\
&-166630947373056^*p + 690341141872640, \\
&1749670572392448^*p - 724737280770048, \\
&-166630947373056^*p + 690341141872640, \\
&-166630947373056^*p + 690341141872640, \\
&11704454583615488^*p - 4848143828713472.
\end{align*}
\]
-2713300183161139309314048*p + 1123885734654746797539328,
2745563299524396139413504*p - 1137249555016829104029696,
-2713300183161139309314048*p + 1123885734654746797539328,
-2713300183161139309314048*p + 1123885734654746797539328,
18297763639587213294960640*p - 7579181860614308846632960

The existence of this code remains an open question. If a code exists, there
must be a chain of derivatives $W_{<67>}, \cdots, W_{<0>}$ with $W_{<0>}$ having only 0
and 1 entries. Lemma 6, Lemma 6, and Theorem 6 may be useful tools in a search
for such a chain.

Acknowledgement 9 This copy of computer algebra system Magma [2] used
in this work has been made available through a generous initiative of the Simons
Foundation covering U.S. colleges, universities, nonprofit research entities, and
their students, faculty, and staff.

5 References

References

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, J. Combin. Theory, vol. 6, 122–151, 1969.
[2] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I.
   The user language, J. Symbolic Comput., 24, 235–265, 1997.
[3] S. K. Houghten, C. W. H. Lam, L. H. Thiel, J. A. Parker, The extended
   quadratic residue code is the only (48, 24, 12) self-dual doubly-even code,
   IEEE Trans. Inform. Theory, IT-49, 53–59 2003.
[4] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes,
   Cambridge University Press, Cambridge, 2003.
[5] P. Lancaster and M. Tismenetsky, The Theory of Matrices with Applications,
   Academic Press, New York, NY, USA, 1985.
[6] V. Pless, On the uniqueness of the Golay codes, J. Combin. Theory 5,
   215–228 1968.
[7] V. Pless, A classification of self-orthogonal codes over GF(2),Discrete
   Math., vol. 3, 209-246, 1972.
[8] J. Simonis, MacWilliams identities and coordinate partitions, Linear Algebra
   Appl., 1, 81-91, 1995.
[9] N. J. A. Sloane, Is there a (72, 36) d=16 self-dual code, IEEE Trans. Inform.
   Theory, IT-19, 251, 1973.
[10] H. Zhang and F. Ding, On the Kronecker products and their applications,
    J. of Applied Math., vol. 2013, 1-8.