More on the uniqueness of the Golay codes

Vera Pless*

University of Illinois at Chicago, Department of Mathematics, Statistics, and Computer Science (M/C 249), Box 4348, Chicago, IL 60680, USA

Received 24 October 1991
Revised 15 January 1992

Abstract

Pless, V., More on the uniqueness of the Golay codes, Discrete Mathematics 106/107 (1992) 391-398.

If $\bar{C}$ is a set of 3^6 ternary vectors of length 12, distance $\geqslant 6$, containing 0, then we show that the supports of the weight 6 vectors in $\bar{C}$ hold an $S(5, 6, 12)$. Further we show that $\bar{C}$ must be a linear, self-dual [12, 6, 6] code, hence the Golay code.

Also any set C of 3^6 ternary vectors of length 11, distance $\geqslant 5$, containing 0, is linear and hence the Golay [11, 6, 6,] code. The supports of the vectors of weight 5 in C hold an $S(4, 5, 11)$.

Similarities and differences with the binary case are discussed.

Several people [1-2, 6] have shown that any set of 2^{12} binary vectors of length 24, distance $\geqslant 8$, containing 0, must be the unique (up to equivalence) [24, 12, 8] Golay code. These proofs start by showing that this set of vectors must actually be a linear code. As the minimum weight of this code is 8, its uniqueness follows from the uniqueness of a binary [24, 12, 8] linear code [2-5]. The same relations hold for a set of 2^{12} binary vectors of length 23, distance $\geqslant 7$, containing 0, and the unique [23, 12, 7] Golay code. Key components of these relationships are the Steiner system $S(5, 8, 24)$ held by the vectors of weight 8 in the Golay [24, 12, 8] code, and the $S(4, 7, 23)$ held by the vectors of weight 7 in the Golay [23, 12, 7] code, the only perfect multiple error-correcting binary code. There are analogous structures for the other perfect multiple error-correcting code, the ternary Golay [11, 6, 5] code. Using techniques from linear programming, Delsarte and Goethals [1] show that an extended perfect 2-code of length 12 must be linear and hence equivalent to the [12, 6, 6] Golay code [3]. They also show that a perfect

Correspondence to: V. Pless, University of Illinois at Chicago, Department of Mathematics, Statistics, and Computer Science (M/C 249), Box 4348, Chicago, IL 60680, USA.

* This work was supported in part by NSA Grant MDA 904-91-H-0003.

2-code of length 11 is linear and so equivalent to the perfect [11, 6, 6] Golay code [3]. The main purpose of this paper is to give an elementary, self-contained proof of the fact that any set of 3^{12} vectors of length 12, distance ≥ 6, containing 0, constitutes the Golay [12, 6, 6] code. We relate this to a similar proof that any set of 3^{12} vectors of length 11, distance ≥ 5, containing 0 is equivalent to the Golay [11, 6, 6] code. We also describe some of the similarities and differences between the binary and ternary cases. In order to do this we start by describing the binary case.

The following outline of the proof of the binary theorem was told to me by Neumaier at the Oberwolfach meeting on 'Codes and Designs' [2].

Theorem 1. *Any set $\bar{C}$ of 2^{12} vectors of length* 24, *distance* ≥ 8, *containing* 0, *constitute a* [24, 12, 8] *linear, self-dual, doubly-even* (*all weights are divisible by* 4) *code.*

Proof (*Outline*). Let C be $\bar{C}$ punctured on any position. Then C is a length 23 code (not necessarily linear) of distance ≥ 7 with 2^{12} vectors. It follows easily that C is a perfect code. Hence the vectors of weight 7 in C hold an $S(4, 7, 23)$. From this one can show that the vectors of weight 8 in $\bar{C}$ hold an $S(5, 8, 24)$.

The next step consists of showing that all distances in $\bar{C}$ are $\equiv 0 \pmod 4$. This uses a clever argument involving the way any vector in $\bar{C}$ can meet the 'tetrads' in a 'sextet' [2, 4].

Since all the distances in $\bar{C}$ are divisible by 4, any two vectors in $\bar{C}$ are orthogonal to each other. It follows readily from this, and the number of vectors in $\bar{C}$, that $\bar{C}$ is a self-dual, doubly-even, linear code. □

To get the full proof that $\bar{C}$ is equivalent to the Golay code, we must show that any two self-dual, doubly-even [24, 12, 8] linear codes are equivalent. This is the more difficult part of the proof and everyone has her favorite proof. My preference is the proof via the classification of self-dual, doubly-even codes of length 24 [5]. This proof is not so difficult if one knows the technique of the classifications; finding the number of different, inequivalent codes until one has the known number of self-dual, double-even length 24 codes. There are nine inequivalent codes in total and the ones with $d = 4$ can be found by 'glueing' weight 4 component codes together. The Golay code is the unique code with $d = 8$.

Our purpose in describing this is to determine whether portions of this proof can be modified for ternary codes. The next lemma is hopeful.

Lemma 1. *If x and y are ternary vectors, then*

$$\mathrm{wt}(x + y) \text{ (or } \mathrm{wt}(x - y)) \equiv \mathrm{wt}(x) + \mathrm{wt}(y) \pmod 3$$

iff x and y are orthogonal to each other. Hence if C is a set of ternary vectors containing the zero vector and the distance between any two vectors in C is *divisible by* 3, *all vectors in* C *are self-orthogonal and any two vectors are orthogonal to each other.*

Proof. If any two ternary vectors are orthogonal to each other, then their common components are unions of triples of the same or opposite values or pairs of like and opposite values. If we consider $\mathrm{wt}(x+y) \pmod 3$, the triples contribute nothing and the like and opposite values in a pair cancel each other. □

A complication in the ternary case as contrasted to the binary case is the possibility of multiplication by scalars, albeit just by $-1 \equiv 2 \pmod 3$. We often use the symbol 2 instead of -1. The next lemma helps in dealing with this complication.

Lemma 2. *Let* C *be an* $(11, 3^6, 5)$ *ternary code* (*not necessarily linear*) *containing* 0. *Then given any* 4 *coordinate positions, there is a vector of weight* 5 *in* C *with nonzero values in those positions and with a specified value* (*either* 1 *or* 2) *in a specified one of those positions.*

Proof. A simple counting argument shows that C is perfect so that any vector of weight 4 is either distance 1 or 2 to a vector of weight 5 in C or distance 2 to a vector of weight 6 in C.

Without loss of generality we can suppose that the four coordinate positions are the first four positions and that we want to find a vector of weight 5 in C with nonzero values in those four positions and a one in the first position. There are 8 vectors of weight 4 with nonzero values in the first four positions and a one in the first position.

Call this set of vectors S. We first show that not all of these vectors can be distance 2 from a weight 6 vector in C.

Consider the following configuration which we must have (up to equivalence) if we attempt to place our weight 4 vectors into weight 6 vectors whose mutual distance is at least 5. (We can have other configurations but we would run out of room earlier.)

1	2	3	4	5	6	7	8	9	10	11
1	1	1	1	1	1					
1	1	1	2			1	1			
1	1	2	1			2		1		
1	2	1	1				2	2		
1	1	2	2	2					1	
1	2	1	2		2				2	
1	2	2	1							1

By the seventh vector it is clear that one of our weight 4 vectors (with a 1 on the first position) must be either distance 1 or 2 to a weight 5 vector in C. So we assume that $(1, 1, 1, 1, 0, \ldots, 0)$ is distance 2 to $x = (2, 1, 1, 1, 1, 0, \ldots, 0)$.

Then none of the seven other weight 4 vectors in S can be distance 2 from a weight 5 vector in C with a 2 in its first position as any such vector has distance less than 5 from x. Hence either the other vectors in S are distance 2 from a vector of weight 6 in C or distance 1 from a weight 5 vector in C with a 1 in its first position. If we try to place the other 7 vectors in S into weight 6 vectors which are mutually distant 5 or more apart and also distant 5 or more from x we must have one of the following two configurations (up to equivalence). For the first configuration ignore the numbers in parentheses. The second configuration is obtained from the first by using the numbers in parentheses in place of their adjacent numbers and other numbers in parentheses including the last line.

1	2	3	4	5	6	7	8	9	10	11
2	1	1	1	1						
1	1	1	2		1	1				
1	1	2	1		2		1			
1	2	1	1			2	2			
1	1	2	2	(2)				1	1(0)	
1	2	1	2					2	(1)	1(0)
1	2	2	1						2	2
(1)	(2)	(2)	(2)							(1)

In the first configuration there is no way for 1222 to be near enough to either a weight 5 or weight 6 vector in C. In the second configuration 1222 is contained in a weight 5 vector. This demonstrates the lemma. □

Theorem 2. *Let C be an* $(11, 3^6, 5)$ *ternary code* (*not necessarily linear*) *containing* 0. *Then if x is a weight* 5 *vector in C, $-x$ is also in C. Hence the vectors of weight* 5 *in C hold an* $S(4, 5, 11)$.

Proof. We can suppose $x = (1, 1, 1, 1, 1, 0, \ldots, 0)$. Consider the vector $2x = -x$. By Lemma 2, there is some weight 5 vector y in C with a 2 on its first position and nonzero components in positions 2, 3 and 4. Up to equivalence there are the following three possibilities for y since $d(x, y) \geq 5$.

(1) $y = 2x$,

(2) $y = (2, 2, 2, 1, 0, 1, 0, \ldots)$,

(3) $y = (2, 2, 2, 2, 0, 1, 0, \ldots)$.

We show that (2) and (3) are not possible. Consider (2). By Lemma 2 there is a weight 5 vector z in C with nonzero coordinates on its first 4 positions and a 2 on its fourth position. Hence $z \neq y$. In order to be distance 5 from x, z must have at least three 2's in the first four positions. But then $d(y, z) < 5$, a contradiction.

In situation (3) we have the following configuration (up to equivalence) by using Lemma 2 again to construct vectors in C which have a 2 on their first position and nonzero coordinates on positions 2, 3, 5; 2, 4, 5; 3, 4, 5 respectively.

1	2	3	4	5	6	7	8	9	10	11
1	1	1	1	1						
2	2	2	2		1					
2	2	1		2		1				
2	1		2	2			1			
2		2	1	2				1		

There is now no way to find a weight 5 vector which is distance 5 from these vectors, has a 2 on position 5 and nonzero components in positions 2, 3 and 4. As such a vector must exist in C by Lemma 2, we see that $-x$ is in C.

The design property follows from Lemma 2 and the fact that if x and y are weight 5 vectors with 4 nonzero components in common, either $d(x, y) < 5$ or $d(x, -y) < 5$. □

This is enough to prove our main theorem.

Theorem 3. *Let $\bar{C}$ be a set of 3^6 ternary vectors of length* 12 *with distance* ≥ 6, *containing* 0. *Then the vectors of weight* 6 *in $\bar{C}$ hold an $S(5, 6, 12)$. Further, $\bar{C}$ is the linear Golay* [12, 6, 6] *code.*

Proof. Let C be $\bar{C}$ punctured on some position. Then C is an $(11, 3^6, 5)$ code and so by Theorem 2 the vectors of weight 5 in C hold an $S(4, 5, 11)$.

Further by this theorem if x is a weight 5 vector in C, then $-x$ is also in C. It is immediate from this that if y is a weight 6 vector in $\bar{C}$, then $-y$ is also in $\bar{C}$.

It is now possible to show that the vectors of weight 6 in $\bar{C}$ hold an $S(5, 6, 12)$. Consider 5 positions out of these 12 and puncture $\bar{C}$, obtaining C, on one of these positions. As the vectors of weight 5 in C hold an $S(4, 5, 11)$ some vector y of weight 5 in C contains the 4 nonpunctured positions. Hence $\bar{y}$ in $\bar{C}$ must be of weight 6 and it covers the 5 positions we began with. We still must show that $\bar{y}$ and $-\bar{y}$ are the unique vectors in $\bar{C}$ whose support contains the given 5 positions. If not, another vector, say z, in $\bar{C}$ of weight 6 has nonzero coordinates in these 5 positions. Then either $d(\bar{y}, z) < 6$ or $d(\bar{y}, -z) < 6$. The conclusion follows as we know that $-z$ must also be in $\bar{C}$ so that the existence of this z gives a contradiction.

The next step is to show that all distances in $\bar{C}$ are divisible by 3. The only distances we have to eliminate are 7, 8, 10 and 11. Suppose x and y are vectors in

$\bar{C}$ with $d(x, y)=7$. If we add $-x$ to all vectors in $\bar{C}$ we obtain another set of vectors with the same properties as $\bar{C}$ and a vector of weight 7 in it. So we suppose x is a vector of weight 7 in $\bar{C}$. Then there is a vector y in $\bar{C}$ of weight 6 with nonzero coordinates on at least 5 of the nonzero positions in x. But $-y$ is also in $\bar{C}$ and we must have either $d(x, y)<6$ or $d(x, -y)<6$ eliminating such an x.

If there are two vectors in $\bar{C}$ of distance 8, as before we can suppose that $\bar{C}$ contains a vector x of weight 8. We again let y be a vector in $\bar{C}$ of weight 6 with nonzero coordinates in at least 5 of the positions where x has nonzero coordinates. Then either $d(x, y)<6$, $d(x, -y)<6$, $d(x, y)=7$ or $d(x, -y)=7$. As none of these are possible, there are no vectors of distance 8 in $\bar{C}$.

Suppose now that there is a vector x of weight 10 in $\bar{C}$. Then there cannot be a vector y of weight 6 whose support is contained in the support of x or else we would get from either y or $-y$ a vector whose distance to x is either less than 6 or equal to 7 or 8. Hence a vector of weight 6 in $\bar{C}$ whose support covers 5 of the nonzero positions in x must have a nonzero position outside x. As any 2 weight 6 vectors, y and z, $y \neq z$, must have either no, 2, 3 or 4 nonzero positions in common (since these vectors hold an $S(5, 6, 12)$) and there are only 2 positions outside the positions in x, it is not possible to find vectors of weight 6 in $\bar{C}$ to cover all the 5-tuples contained in the support of x. A similar situation holds if $\bar{C}$ contains a vector of weight 11.

We have just demonstrated that all vectors in $\bar{C}$ have weights divisible by 3. Let $\bar{C}'$ be the ternary code generated by $\bar{C}$ so that $\dim \bar{C}' \geqslant 6$. By Lemma 1, $\bar{C}'$ is self-orthogonal implying that $\dim \bar{C}' \leqslant 6$. Hence $\dim \bar{C}' = 6$ which means that $\bar{C}' = \bar{C}$. There is a similar argument in [1].

In contrast to the binary case, it is now quite simple to show that any two ternary $[12, 6, 6]$ self-dual codes are equivalent by considering a generator matrix G of the form (I, A). It is not hard to show that G can be chosen as follows (up to equivalence) where I is the 6×6 identity matrix:

$$G = \left(I \;\middle|\; \begin{matrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{matrix} \right). \qquad \square$$

Theorem 4. *Any set C of 3^6 ternary vectors of length* 11, *distance* $\geqslant 5$, *containing* 0, *constitutes the Golay* [11, 6, 5] *code.*

Proof. Any $(11, 3^6, 5)$ ternary code C is perfect, i.e., spheres of radius 2 about codewords are disjoint and cover the space. From this, as 0 is in C, we can determine the entire weight distribution of C. We describe how this can be done. Note that a weight 3 vector can only be in a sphere about a weight 5 vector in C. Hence $\binom{5}{3} A_5 = 2^3\binom{11}{3}$ so that $A_5 = 132$. We can determine that $A_6 = 132$ also by noting that vectors of weight 4 are in spheres about vectors of either weight 5 or weight 6 in C. The disposition of vectors of weight 5 shows that $A_7 = 0$ and so on. It turns out that the only weights occurring in C are $0, 5, 6, 8, 9$ and 11, hence weights that are either 0 or $2 \pmod 3$. Further $A_0 + A_6 + A_9 = 1 + 132 + 110 = 243 = 3^5$.

Let D consist of the vectors in C with weights divisible by 3. If x in D has weight 6, then we can show that $-x$ is in D (see [1] also) by considering which spheres in C could contain the 6 weight 5 vectors formed from nonzero components of $-x$. An analogous argument shows that if y in D has weight 9, $-y$ is also in D.

Lemma 4.1 in [1] states that for arbitrary ternary vectors a and b,

$$d(a, b) = \mathrm{wt}(a) + \mathrm{wt}(b) + (a, b) \pmod 3.$$

If a is in C and b is in D,

$$\begin{aligned} d(a, b) &= \mathrm{wt}(a) + (a, b) \pmod 3, \\ d(a, -b) &= \mathrm{wt}(a) + (a, -b) \pmod 3 \\ &= \mathrm{wt}(a) - (a, b) \pmod 3. \end{aligned}$$

As $d(a, b) = d(a, -b)$, (a, b) must be 0. Hence all vectors in D are orthogonal to all vectors in C. So the linear code generated by D has a dual code of dimension at least 6. As D contains 3^5 vectors, D is linear of dimension 5 and C is its dual code, linear, and of dimension 6. □

As C contains vectors of weight 11 we could suppose that up to equivalence C contains the all one vector. Then we could try to prove Theorem 4 from Theorem 3 by extending C, that is if $c = (c_1, c_2, \ldots, c_{11})$ is in C, we would adjoin a coordinate c_0 so that $\sum_{i=0}^{11} c_i = 0 \pmod 3$. It is easy to show that the extended coordinate would be 0 for vectors in D and $\neq 0$ for vectors not in D, but it is difficult to show that vectors of distance 5 apart are extended to vectors of distance 6 apart.

When I wrote my paper on the 'Uniqueness of the Golay codes' I did not realize that there was such a short proof of the uniqueness of the extended ternary Golay code so I showed it was unique by classifying all self-dual ternary [12, 6] codes. This was the first classification of self-dual codes over any field and many more followed, mainly for binary and ternary codes. The referee of the 'Uniqueness' paper [3] liked this style of proof and suggested that it would be a good idea to prove that a binary [24, 12, 8] self-dual code is unique by classifying all [24, 12] binary self-dual codes. At that time this approach seemed very difficult to me. Now it is quite reasonable.

Another proof that at first sight seems easier for the binary case than the ternary case is the proof that the associated Steiner system is unique based on the uniqueness of its code. It is not difficult to show that the binary code C generated by the blocks of an $S(5, 8, 24)$ is self-orthogonal. It is more work, but can be done, to show that C has minimum weight 8 and dimension 12. What about the ternary case?

If one places ones on the supports of the blocks in an $S(5, 6, 12)$ and generates a ternary code, this code will not be self-orthogonal. Is there a canonical way to place 2's on these supports?

References

[1] P. Delsarte and J.M. Goethals, Unrestricted codes with the Golay parameters are unique, Discrete Math. 12 (1975) 211–224.

[2] A. Neumeier, private communication, 1990.

[3] V. Pless, On the uniqueness of the Golay codes, J. Combin. Theory 5 (1968) 215–228.

[4] V. Pless, Introduction to the Theory of Error Correcting Codes (Wiley, New York, 2nd Ed., 1989).

[5] V. Pless and N.J.A. Sloane, On the classification and enumeration of self-dual codes, J. Combin. Theory, Ser. A 18 (1975) 313–335.

[6] S.L. Snover, The uniqueness of the Nordstrom–Robinson and the Golay binary codes, Ph.D. Thesis, Dept. of Mathematics, Michigan State Univ., 1973.