Self-Dual Codes and the (22,8,4) Balanced Incomplete Block Design

R. T. Bilous
Department of Computer Science, Concordia University
Montreal, Quebec, Canada H3G 1M8
umbilou1@cs.concordia.ca

G. H. J. van Rees [*]
Department of Computer Science, University of Manitoba
Winnipeg, Manitoba, Canada R3T 2N2
vanrees@cs.umanitoba.ca

SHORT RUNNING HEAD: *Codes and the* $(22, 8, 4)$ *BIBD*

Abstract

We enumerate a list of 594 inequivalent binary $(33, 16)$ doubly-even self-orthogonal codes that have no all-zero coordinates along with their automorphism groups. It is proven that if a $(22, 8, 4)$ Balanced Incomplete Block Design were to exist then the 22 rows of its incident matrix will be contained in at least one of the 594 codes. Without using computers, we eliminate this possibility for 116 of these codes.

Keywords:
enumeration, algorithm, binary code, self-orthogonal, equivalence, automorphism group, balanced incomplete block design, incident matrix, point code, necessary conditions

Communicating Author:
G. H. J. van Rees
Dept. of Computer Science
University of Manitoba
Winnipeg, Manitoba
Canada R3T 2N2

[*]Research supported in part by NSERC Grant OGP0003558

1 Introduction

A (v, b, r, k, λ)-*balanced incomplete block design* (BIBD) is a family of b sets, called blocks, each consisting of k elements taken from a set of v elements such that each element occurs in exactly r blocks and every pair of elements occurs together in exactly λ blocks. Since b and r can be calculated from v, k and λ, we use (v, k, λ) as the *parameters* for the design. There are four well-known necessary conditions for the existence of a BIBD.

Theorem 1.1 In a (v, b, r, k, λ) BIBD, the following holds:
1. $rv = bk$
2. $\lambda(v-1) = r(k-1)$
3. $b \geq v$
4. If $v = b$, and
 a. if v is even then $k - \lambda$ is a perfect square
 b. if v is odd then $z^2 = (k-\lambda)x^2 + (-1)^{v-1)/2}\lambda y^2$ has a solution in integers with x, y, z not all equal to 0.

The proof of this and other facts about block designs can be found in Beth, Jungnickel and Lenz [1] or *The CRC Handbook of Combinatorial Designs* [7]. Unfortunately, these necessary conditions are not sufficient as was proven be Lam et al. [12]. They showed that the (111,11,1)-BIBD did not exist although it meets all four necessary conditions.

In this paper, we are interested in the $(22, 8, 4)$ BIBD. It also obeys the four necessary conditions of Theorem 1.1 but it is not known whether it exists or not. This is an old problem going back as least as far as the tables of BIBDs that Fisher and Yates produced in 1934 [8]. There have been many approaches to finding this design or showing its non-existence: [10], [11], [13], [9], [21], [16], [17] and [18]. Our approach incorporates the information we know from design theory and the information we know from coding theory.

First we give some of the basic facts about BIBDs from design theory. Let B_0 be a particular block in the set of blocks, $\mathcal{B}$, of a particular (22,8,4)-BIBD. Let a_i be the number of blocks in $\mathcal{B}$ that intersect B_0 in i elements, then we can do some simple counting to get:

$$\sum_{i=0}^{8} a_i = b - 1 = 32 \tag{1}$$

$$\sum_{i=0}^{8} i a_i = k(r_1) = 88 \tag{2}$$

$$\sum_{i=0}^{8} \binom{i}{2} a_i = \binom{k}{2}(\lambda - 1) = 84. \tag{3}$$

There are only nine non-negative integer solutions to these equations. Hamada and Kobayashi [10] showed that only four of these solutions were possibly feasible. Using extensive CPU time, McKay and Radziszowski [16] reduced these solutions to the following two solutions which we record as a Theorem 1.2.

Theorem 1.2 The only two possible types of block intersection patterns in a (22,8,4)-BIBD are the following:

TYPE	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
1	0	0	12	16	4	0	0	0	0
2	0	1	9	19	3	0	0	0	0

Now let us define some needed terms from coding theory. Undefined coding theory terms can be found in *The Handbook of Coding Theory* [19] or in MacWilliams and Sloane [14]. Let $V_n(2)$ denote the vector space of all binary n–vectors. An (n, k) *binary linear code*, C, is a k dimensional subspace of $V_n(2)$. We only consider binary linear codes in this paper, and thus, whenever we use the term code we will be referring to this class of codes only. The integers n and k are the *length* and *dimension* of C, respectively. The n–vectors in C are called *codewords.* The *weight* of a codeword c is the number of ones in c. An *even* code only has codewords whose weights are a multiple of 2. A *doubly-even* code only has codewords whose weights are a multiple of 4. A *singly-even* code is an even code that is not a doubly-even code. Codewords will also be called doubly-even or singly-even depending on whether their weight is $\equiv 0$ or 2 mod4. The *minimum distance* of a code, C, is the smallest weight of any non-zero codeword in C. An (n, k, d) *code* is an (n, k) code with minimum distance d.

Two codes C_1 and C_2 are *equivalent* if and only if there exists a coordinate permutation of C_1 that takes C_1 into C_2. If C_1 and C_2 are not equivalent then C_1 and C_2 are said to be inequivalent. The *equivalence class* of a code C is the set of all codes that are equivalent to C. An automorphism of a code C is a coordinate permutation that takes C into itself. The set of all automorphisms of C, which is a group, is called the *automorphism group* of C.

Let $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$ be any two n–vectors in $V_n(2)$. The *dot product* of u and v, written $u \bullet v$, is defined as $(\sum_{i=1}^{n} u_i v_i)$ mod 2. Two vectors u and v are called *orthogonal* if $u \bullet v = 0$. The *intersection* of two vectors is the set of coordinate positions in which they both contain ones. If the intersection is non-null then the vectors are said to *intersect.* The *orthogonal complement* of a (n, k) code C, written $C^{\perp}$, is the set of all n–vectors that are orthogonal to every codeword in C. $D + g$, a *translate of* D, is the set of vectors of the form $d + g$ where d is an element of D. It is well known that $C^{\perp}$ is an $(n, k - n)$ code. If $C^{\perp} \subseteq C$ then C is called a *self-orthogonal code.* If $C^{\perp} = C$ then C is called a *self-dual* code. A *self-orthogonal code* is a self-dual code if and only if $n = 2k$.

In Section 2 we will prove that the point code of a (22,8,4)-BIBD, if it exists, must be a subcode of a doubly-even, self-orthogonal (33,16) binary code with no all-zero coordinates. We will enumerate these codes by computer and theoretically check the enumeration. Then, in Section 3, we eliminate many of these codes containing particular configurations of weight 4 codewords. Finally, in Section 4 we state how many of these codes could possibly contain 22 rows that are the incidence matrix of a (22,8,4)-BIBD.

2 Point Code of a $(22, 8, 4)$-BIBD

Label the elements of a design 1 to v and the blocks 1 to b. The *incidence matrix* of a $(22, 33, 12, 8, 4)$-BIBD is a binary 22 by 33 matrix whose (i, j) entry is 1 if element i occurs in block j and is 0 otherwise. The *point code* of a $(22, 8, 4)$-BIBD is the binary, linear code generated by the rows of the incidence matrix. The point code of our design is quite special. In Hall et al. [9] the following was proved.

Theorem 2.1 If a $(22, 8, 4)$-BIBD exists, its point code would be a doubly-even, self-orthogonal code with length 33 and dimension at most 16.

Since our code is generated from an incidence matrix which has 1's in each column we know that the code has 1's in each coordinate position and we can state:

Corollary 2.2 If a $(22, 8, 4)$-BIBD exists, its point code would be a doubly-even, self-orthogonal code with length 33 and dimension at most 16 with no all-zero coordinates.

It is most inconvenient that we do not know the dimension of the point code of our design. However we know that our point code can be embedded in a self-dual code of dimension 16 using the following theorem. The proof is similar to the one in MacWilliams, Sloane and Thompson [15] for the n congruent to 0 modulo 8 case. For utterly complete details of this theorem, see Bilous [3]. We need this theorem for later purposes, to verify the correctness of a classification of codes.

Theorem 2.3 Let C be a doubly-even self-orthogonal (n, s) code with n congruent to $\pm 1 \bmod 8$. Then the number of doubly-even, self-orthogonal (n, k) codes that contain C is:

$$\left(\frac{2^{n-2s-1}-1}{2^{k-s}-1} - 2^{\frac{n-1}{2}-k}(2^{\frac{n-1}{2}-s}-1)\right)\prod_{i=1}^{k-s-1}\frac{2^{n-2(k-i)-1}-1}{2^i-1}$$

Proof Let $A(n, k)$ be the number of (n, k) self-orthogonal codes with $n \equiv \pm 1 \bmod 8$ that contain a particular doubly-even self-orthogonal (n, s) code, C. Let $B(n, k)$ be the number of (n, k) doubly-even, self-orthogonal codes with $n \equiv \pm 1 \bmod 8$ that contain a particular doubly-even self-orthogonal (n, s) code, C. So $A(n, k) - B(n, k)$ is the number of (n, k) singly-even, self-orthogonal codes with $n \equiv \pm 1 \bmod 8$ that contain a particular doubly-even self-orthogonal (n, s) code, C. Let S be the set of such codes. Since we can not determine $B(n, k)$ directly, we determine it by subtracting $A(n, k) - B(n, k)$ from $A(n, k)$. $A(n, k)$ was determined in Pless and Sloane [20] to be:

$$\frac{2^{n-2s-1}-1}{2^{k-s}-1}\prod_{i=1}^{k-s-1}\frac{2^{n-2(k-i)-1}-1}{2^i-1} \tag{4}$$

Now we have to count the number of (n, k) singly-even, self-orthogonal codes with $n \equiv \pm 1 \bmod 8$ that contain a particular doubly-even self-orthogonal (n, s) code, C. Let H denote the set of codewords in $C^\perp$ with weight $\equiv 2 \bmod 4$. Let T denote the set of codes $D \in S$ for which there exists a $v \in H$ such that $C \cup (C + v) \subseteq D$. Clearly $S = T$ and we can calculate $|S|$ by calculating $|T|$.

For each $v \in H$, let $x(v)$ denote the number of singly-even self-orthogonal (n, k) codes with $n \equiv \pm 1 \bmod 8$ that contain $C \cup (C + v)$. For each $D \in T$, let $y(D)$ denote the number of codewords $v \in H$ such that $C \cup (C + v) \subseteq D$. Then

$$\sum_{D\in T} y(D) = \sum_{v\in H} x(v). \tag{5}$$

Consider the right hand side of the equation (5). Since C is doubly-even and $\mathrm{wt}(v) \equiv 2 \bmod 4$, we know that $v \notin C$ and so $C \cup (C + v)$ is singly-even. Therefore, we know that the number of doubly-even codes containing $C \cup (C+v)$ is 0. Therefore the number of singly-even self-orthogonal codes that contain $C \cup (C+v)$ is equal to the number of self-orthogonal codes that contain $C \cup (C + v)$. Let f denote this number. By Pless and Sloane [20], we know that f is the same for any $v \in H$ and so $\sum_{v\in H} x(v) = f|H|$, where f is the value in equation (4).

Consider the left hand side of the equation (5). Clearly, the number of codewords in H for which $C \cup (C + v) \subseteq D$, where $D \in T$, is equal to the number of vectors in D with weight $\equiv 2 \bmod 4$. Since D is singly-even, half of these vectors must be even i.e. 2^{k-1}. Therefore $\sum_{D\in T} y(D) = |T|2^{k-1}$. Substituting this equation into equation (5) gives us:

$$|T| = f|H|/2^{k-1}. \tag{6}$$

We now have to calculate $|H|$, the number of codewords in $C^\perp$ with weight $\equiv 2 \bmod 4$. Let D be a (n, k) doubly-even self-orthogonal code containing a particular (n, s) doubly-even self-orthogonal code with $n \equiv 1 \bmod 8$. Then we can write:

$$C^\perp = D \cup (D + g) \cup (D + f_1) \cup \ldots \cup (D + f_j).$$

where $D^\perp = D \cup (D + g)$ and $j = 2^{n-s}/2^{(n-1)/2} - 2 = 2^{((n+1)/2)-2} - 2$. We will count $|H|$, the number of codewords of weight $\equiv 2 \bmod 4$ in $C^\perp$, by counting the number of such codewords in each translate of D.

First consider $D^\perp = D \cup (D + g)$. Since n is odd, we know that the all 1's vector is not in D and thus exactly half the codewords in $D^\perp$ have even weight. Since D contains only even weight codewords ($\equiv 0 \bmod 4$) then $D+g$ must contain only odd weight codewords. So $D^\perp$ contains no singly-even codewords.

Consider the remaining translates of D. Since the all 1's vector is not in D it is also not in C. So exactly half the codewords in $C^{\perp}$ have even weight. Since exactly half the codewords in $D^{\perp}$ have even weight, exactly half the codewords in $(D+f_1)\cup\ldots\cup(D+f_j)$ have even weight. Clearly, the parity of the codewords in $D+f_i$ is equal to the parity of f_i. So exactly half the f_i's have even weight and half odd weight. Now the even f_i's are not in $D^{\perp}$ so they have dot product of $\equiv 2$ mod 4 with some codeword in D, so the codewords in $D+f_i$ must be half doubly-even and half singly-even. Therefore the total number of singly-even codewords in $|H|$ is:

$$\begin{aligned}((j/2)(|D|)/2) &= ((2^{\frac{n+1}{2}-s}-2)/2)(2^{\frac{n-1}{2}}/2)\\ &= 2^{n-s-2}-2^{\frac{n-1}{2}-1}.\end{aligned}$$

Substitute for $|H|$ and f in equation 6 to get $|T|$. Then subtract this value from (4) to get the final answer. □

If a $(22, 8, 4)$-BIBD exists then by Corollary 2.2 there is a doubly-even, self-orthogonal (33,k)-code without any all-zero coordinate with dimension at most 16. Then by Theorem 2.3, we know that this can be contained in a doubly-even, self-orthogonal (33,16)-code without any all-zero coordinate. Let us record this.

Theorem 2.4 If a $(22, 8, 4)$-BIBD exists, then there exists a doubly-even, self-orthogonal (33,16)-code with no all-zero coordinate that contains the point code of this design.

Although Theorem 2.3 gives us the number of doubly-even, self-orthogonal (33,16)-code without any all-zero coordinate, no one has enumerated them. However, Bilous has enumerated all the inequivalent self-orthogonal (34,17) codes with minimum distance at least 4 along with their automorphism groups in Bilous [6]. He used the techniques we developed in [5]. This is also described in Bilous's Thesis [3]. These codes are listed at the following web site: [2]. This is a good starting point for our enumeration.

Theorem 2.5 The number of inequivalent binary, self-dual (34,17)-codes is 24,147 of which 3,295 have distance 2, 19,914 have distance 4 and 938 have distance 6.

Let C be a self-orthogonal $(33, 16)$ code. Since C can not contain the all 1's vector, C can be *lengthened* to a self-dual $(34, 17)$ code, D, by inserting an all 0 coordinate before the j^{th} coordinate in C and then adding the all 1's vector to the basis of the code. The converse of this operation, called *cross sectioning*, can also be done by removing all codewords in D with a 1 in coordinate j and then deleting coordinate j to get D_j Using Lagrange's theorem, it is easy to show that a self-dual code must have exactly half of its codewords with a 1 in a specific coordinate and half with a 0 in that coordinate (in a non all-zero coordinate).

So let us start with D and cross section D to get $D_j = C$. The codewords in C will be doubly-even, only if the 2^{16} codewords in D that have a 0 in coordinate j are doubly-even. So we define a *doubly-even coordinate* in a self-dual $(2n, n)$ code, D to be a coordinate, j, such that the 2^n codewords that have a 0 in coordinate j all have weight a multiple of 4. Since the all 1's codeword of length 34 is in D, D is not doubly-even. Then, by Lagrange's theorem, we know that half of the codewords must have doubly-even weight. So it is not necessarily true that all codewords that have a value of 0 in coordinate j have doubly-even weight. However, if j is a doubly-even coordinate, the 2^{16} codewords with a 0 in coordinate j are all the doubly-even codewords and the rest of the codewords in D have a 1 in column j.

Could it be that D has two or more doubly-even coordinates? Let us suppose so. Let j and k be two doubly-even coordinates in D. Then the doubly-even words have a 0 in columns k and j, while the other codewords have a 1 in both coordinate j and k. In other words, coordinate j and k are identical. Hence D_j has a coordinate that is all 0. But $D_j = C$ could not have been generated by the rows of an incidence matrix, because then there would have been an all 0's column in the incidence matrix which is a contradiction. So we are interested only in self-dual $(34, 17)$ codes which have exactly one self-dual coordinate. The next lemma tells us when this fails to happen.

Lemma 2.6 The only self-dual codes that have more than 1 doubly-even coordinate are the weight 2 codes.

Proof If a self-dual code, D, has two or more double-even coordinates, then those coordinates are identical. Consider a word of weight 2 with 1's in coordinate j and k, say w. Since coordinate j and k are identical, then w is orthogonal to all codewords in C , so w is in $D^{\perp}$ and hence in D. Alternatively, if a code D has weight 2, let c be a word of weight 2. Let the 1's in c occur in coordinate j and k. Because the other codewords must be orthogonal to c, the other codewords must have two 0's or two 1's in coordinate j and k. □

It is easy to check that two equivalent self-dual $(34, 17, \geq 4)$ codes with exactly one doubly-even coordinate apiece can be cross-sectioned at those coordinates to produce equivalent self-orthogonal $(33, 16, \geq 4)$ codes and vice versa. So we need only consider a list of inequivalent self-dual $(34, 17, \geq 4)$ codes with exactly one doubly-even coordinate when we are trying to produce a list of inequivalent self-orthogonal $(33, 16, \geq 4)$ codes generated by the incidence matrix of a $(22, 8, 4)-$ BIBD.

Since there is only one doubly-even coordinate in the codes of interest, it must be fixed by the code's automorphism group. The code formed by cross-sectioning at the doubly-even coordinate must obviously have the same automorphism group except that the fixed coordinate is deleted. These facts allow us to have the following efficient algorithm to produce a list of codes (along with their automorphism groups) we are interested in from the list of codes that we have.

Algorithm 2.7 :

- Input: A list L_D of pairs (C_D, Π_D) where D is a self-dual $(34, 17, \geq 4)$ code and Π_D is the automorphism group of D. The list has the property that all such equivalence classes of codes are represented exactly once in the list.
- Output: A list L_C of pairs (C_C, Π_C) where C is a doubly-even self-orthogonal $(33, 16, \geq 4)$ code with no all-zero coordinate and Π_C is the automorphism group of C. The list has the property that all such equivalence classes of codes are represented exactly once in the list.

```
begin
  Clear the list $L_C$
  for each $(C_D, \Pi_D)$ in $L_D$ do
    if $C_D$ has a doubly-even coordinate then
          Set $C_C$ = cross-section of $C_D$
          Set $\Pi_C = \Pi_D$ with doubly-even coordinate deleted
              and subsequent coordinates decremented by 1
    end if
    insert $(C_C, \Pi_C)$ into $L_C$.
  end for
end
```

This algorithm was implemented and the result is in the following theorem.

Theorem 2.8 The number of inequivalent doubly-even self-orthogonal $(33, 16, \geq 4)$ codes with no all-zero coordinate is 594.

These codes can be found at the following web site [2]. We conclude this section by showing how the sizes of the automorphism groups of the these codes can be used to confirm that 594 is the correct number.

First we find the total number of self-orthogonal, doubly-even $(33,16)$ codes with no all-zero coordinate by computing:

$$\sum_{C\in L_C}\frac{33!}{\mathrm{Aut}(C)}$$

where $\mathrm{Aut}(C)$ is the size of the automorphism group of C. See [19].

Now we will compute the same number theoretically. If we put s=0 and $k=\frac{n-1}{2}$, in Theorem 2.3 we get the following theorem.

Theorem 2.9 Let $n\equiv\pm1 \bmod 8$, then the number of $(n,(n-1)/2)$ doubly-even self-orthogonal codes codes is:

$$2\prod_{i=1}^{\frac{n+1}{2}-2}(2^i+1).$$

Of course, we are not interested in codes which have an all-zero coordinate.

Theorem 2.10 Let $n\equiv 1 \bmod 8$. Then the number of $(n,(n-1)/2)$ doubly-even self-orthogonal codes that do not have a coordinate of zeros is:

$$(2^{\frac{n-1}{2}}-2(n-1))\prod_{i=1}^{\frac{n-1}{2}-2}(2^i+1)$$

.

Proof We count these codes by subtracting the number of $(n,(n-1)/2)$ doubly-even, self-orthogonal codes with some coordinates of zeros from the number of all $(n,(n-1)/2)$ doubly-even, self-orthogonal codes. The latter number we have from Theorem 2.10. Now any self-orthogonal $(n,(n-1)/2)$ code with some coordinates of zeros can only have 1 coordinate of zeros as otherwise its dimension would be too small. If that coordinate of zeros is deleted the resulting code will be self-dual of length $n-1$. Conversely, if we start with a $(n-1,(n-1)/2)$ doubly-even, self-dual code, we can insert a coordinate of zeroes in any of n positions to get a $(n,(n-1)/2)$ doubly-even, self-orthogonal codes with a coordinate of zeros. We can count the number of $(n-1,(n-1)/2)$ doubly-even, self-dual codes by replacing n with $n-1$ in Theorem 2.9. If we then multiply this number by n, we get the number of $(n,(n-1)/2)$ doubly-even, self-orthogonal codes with one co-ordinate of zeros. So our count is:

$$2\prod_{i=1}^{\frac{n+1}{2}-2}(2^i+1)-2n\prod_{i=1}^{\frac{n-1}{2}-2}(2^i+1).$$

Simplifying gives the result. □

Now the theoretical result gives that the number of $(33,16)$ doubly-even self-orthogonal codes that do not have a coordinate of zeros is $(2^{16}-2^6)(3)(5)(7)\dots(2^{14}+1)$ which is the same number the computer gives so that we can be sure that there are 594 doubly-even, self-orthogonal codes with minimum distance greater than 4. These are the codes that must be investigated to see if there are 33 codewords of weight 12 that form the incidence matrix of a (22,33,12,8,4)-BIBD. These 594 codes are listed at Bilous [2]. We call this list of 594 codes, L.

3 Eliminating Codes

If a (22,8,4)-BIBD exists then at least one of the 594 codes in L must contain 22 codewords of weight 12 that are 22 rows of the incidence matrix of this design. We now show that many of these 594 codes do not contain any such set of 22 codewords. The first of the matrices eliminated occurred before our list was computed. Van Rees [21] proved that if the point code of a (22,33,12,8,4)-BIBD has dimension 16 then it must be indecomposable. However, this eliminates only 14 of the 594 codes on L, so we use a different approach. We concentrate on weight 4 codewords.

Lemma 3.1 In a doubly-even, self-orthogonal $(33, 16, \geq 4)$ code without any all-zero coordinates, no weight 12 codeword that is part of a set of 22 codewords making up an incidence matrix for (22,8,4)-BIBD can intersect a weight 4 codeword.

Proof Consider a weight 4 codeword in our code. Call it s. Let us consider the 4 coordinates in the code (and in the incidence matrix) that contain these 4 ones of s. Let us put these 4 columns on the extreme left as in Figure 1. Let x_i be the number of rows of the incidence matrix that have a weight i in the 4 left-most columns. The weights must be even as the weight 12 rows and weight 4 row are still rows of a self-orthogonal code. We can write down the following two equations. The first counts the rows in the incidence matrix and the second counts the number of ones in the 4 left-most columns.

$$x_0 + x_1 + x_4 = 22$$
$$2x_2 + 4x_4 = 32$$

Note that $x_4 \leq 4$ is due to Theorem 1.2.

The remaining solutions in non-negative integers are:

x_0	x_2	x_4
6	16	0
7	14	1
8	12	2
9	10	3
10	8	4

Suppose $x_0 \geq 8$, then there are 8 rows in the 4 left-most columns of the incidence matrix that are all-zeroes. Call this submatrix D_L. Then there are 12 ones per row in the right-most 29 columns of these 8 rows. Call this submatrix D_R. The average weight per column in D_R is $3\frac{9}{29}$. If we wish to minimize the number of pairs of ones in D_R, the weights of the columns in D_R should be 3 or 4 only, i.e. 9 columns of weight 4 and 20 columns of weight 3. This gives a minimum of $9\binom{4}{2} + 20\binom{3}{2} = 114$ pairs. But in these 8 rows of the incidence matrix of the design, the pair count should be exactly $4\binom{8}{2} = 112$. The pair count is too large so $x_0 \leq 7$.

Consider the case where $x_0 = 7$. Then let D_L be the 7×4 submatrix of zeroes. Also there is a row, r of the incidence matrix that intersects s in its 4 ones. Let r have its 12 ones on the extreme left coordinate positions. Let D_M be the 7×8 submatrix adjoined to D_L. These 8 columns are the columns that contain ones in r and zeroes in s. Let D_R be the 7×21 submatrix adjoining D_M on its right as in Figure 2. In D_M, every row must intersect r in 4 columns. So every row in D_M must have exactly 4 ones. So the average weight of a column of D_M is $3\frac{1}{2}$. This means there are 8 ones in every row of D_R and the average weight of a column of D_R is $2\frac{2}{3}$. This gives us a minimum pair count in these 7 rows of $4\binom{4}{2} + 4\binom{3}{2} + 14\binom{3}{2} + 7\binom{2}{2} = 85$. But this contradicts that the pair count should be $4\binom{7}{2} = 84$. So $x_0 < 7$. That means that there is only one solution to our equations. It has $x_4 = 0$. □

When we search the 594 codes on L for 22 codewords of weight 12 that could be an incidence matrix of a (22,8,4)-BIBD, Theorem 3.1 eliminates 10-20 percent of the codewords of weight 12 from consideration. Further, we can look at accumulations of weight 4 words and eliminate certain other codes from our list L. These codes are listed by Bilous [2] and given labels depending on what configurations of weight 4 codewords are contained in the code. See [3] or [4] for details.

Consider the following three codewords:
11110000...0
11001100...0
10101010...0

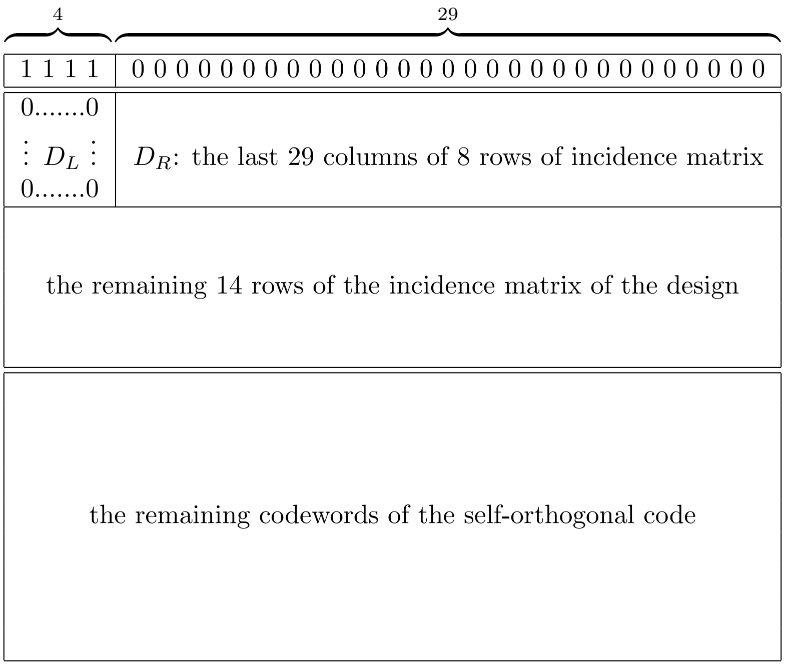
4
29
1 1 1 1
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0.......0
D_L
0.......0
D_R: the last 29 columns of 8 rows of incidence matrix
the remaining 14 rows of the incidence matrix of the design
the remaining codewords of the self-orthogonal code

Figure 1: The code with s and the embedded incidence matrix displayed.

They generate a subcode which Pless calls e_7 but Bilous calls an e_3-block (assuming no further weight 4 codewords intersect the original 3 codewords). In this paper, we will call the three rows an e_3. Of course, these seven coordinate positions can occur anywhere. We eliminate codes containing these 3 rows with the following theorem.

Theorem 3.2 If a doubly-even self-orthogonal (33,16)-code contains an e_3, then it does not contain 22 rows of weight 12 that could be the incidence matrix of a (22,8,4)-BIBD.

Proof Assume that such a code can contain both the 22 rows of an incidence matrix, M of a (22,8,4)-BIBD and an e_3. Let the ones in the e_3 occur in the left-most seven coordinate positions. Consider the weights of the 22 rows of M in the seven left-most coordinate positions. Since the code is self-orthogonal, it is easy to check that the weights of the rows of M in the seven left-most coordinate positions must be 0,3,4 or 7. Further any weight 4 rows must be a copy of one of the 7 weight 4 rows generated by e_3. Using Lemma 3.1, we see that weight 4 or 7 is not possible either. Then if x_i is the number of weight i rows in M, then simple counting gives:

$$\begin{aligned} x_0 + x_3 &= 22 \\ 3x_3 &= 56 \end{aligned}$$

Clearly there is no solution in integers. □

Of the 594 codes on list L, this eliminates the 90 codes which contain an e_3, i.e. the codes labelled by Bilous [2] e_3, e_4 and e_8. Now the weight 4 codewords can clump in other ways. Consider the following i generators of a subcode where the coordinates may occur anywhere:
$1111000000\ldots00$
$1100110000\ldots00$
$1100001100\ldots00$
$\vdots$
$1100000000\ldots11$.

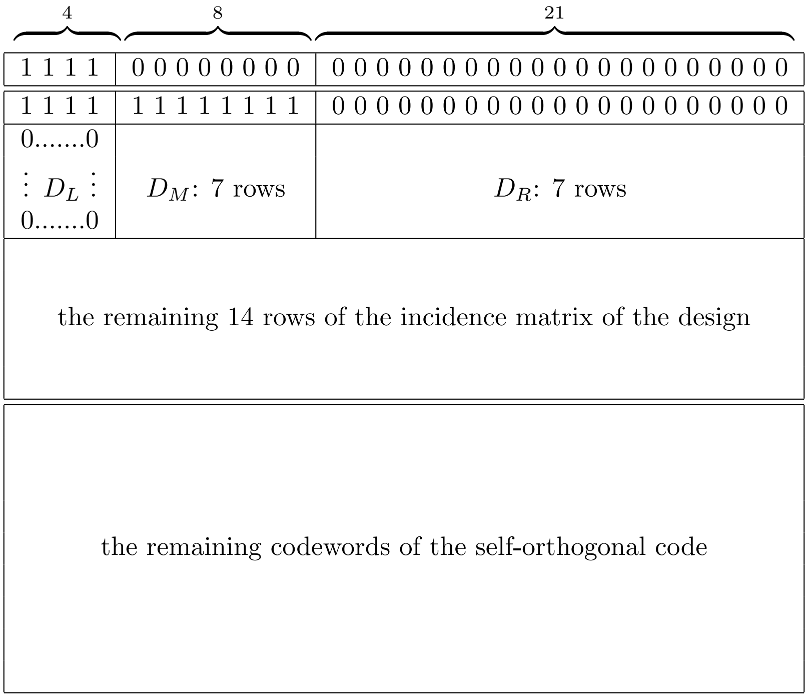

Figure 2: The code with s and r and the embedded incidence matrix displayed.

Pless [20] calls the subcode generated by these rows a D_{2i+2} but Bilous [2] would call this a d_i-block assuming that no other weight 4 codewords intersect these i rows. We will refer to these rows as a d_i. If i is large enough, then the code containing a d_i can not also contain the incidence matrix of a (22-8,4)-BIBD.

Theorem 3.3 If a doubly-even self-orthogonal (33,16)-code contains a d_i where $i \geq 5$, then the code does not contain 22 rows of weight 12 that could be the incidence matrix of a (22,8,4)-BIBD.

Proof Assume that such a code can contain both the 22 rows of an incidence matrix, M of a (22,8,4)-BIBD and a d_i, where $i \geq 5$. The first 5 rows of the d_i, are a d_5 and let the ones in the d_5 occur in the left-most 10 coordinate positions. Call those positions D_L. Group the coordinate positions in pairs as follows: p_i is the pair of coordinate positions $2i-1$ and $2i$. It is clear that the d_5 rows generates a weight 4 codeword with ones in coordinate pairs p_k and p_j for any k, j where $1 \leq k, j \leq 6$. Note that a codeword with 10 or 01 in a p_i must have a 10 or 01 in every p_j to ensure even intersection with every codeword generated by d_6. Also note that codeword with 00 or 11 in a p_i must have a 11 or 00 in every p_j to ensure even intersection with every codeword generated by d_5. Let x_i be the number of rows in M, restricted to the columns of D_L of weight i. Then we have just proved that rows in M restricted to D_L have even weight with each p_i pair containing 00 or 11, or the weight of the row is 6. But if all p_i pairs contain either 00 or 11 and has weight larger than 2, then the row intersects a weight 4 codeword generated by d_5 in 4 positions. But by Lemma 3.1 this is impossible. So the only i for which x_i is non-zero is 0, 2 or 6. We can write down the following equations:

$$\begin{aligned} x_0 + x_2 + x_6 &= 22 \\ 2x_2 + 6x_6 &= 96 \end{aligned}$$

The only solutions in non-negative integers are:

x_0	x_2	x_6	Solution
0	9	13	A
2	6	14	B
4	3	15	C
6	0	16	D

Solution A has 9 rows which have weight 2 in the the 12 left-most coordinate positions, call the submatrix D_L. Call the adjoining 21 columns in these 9 rows D_R. To minimize the pair count in the columns of D_L we must have 6 columns of weight 1 and 6 columns of weight 2. To minimize the pair count in the columns of D_R we must have 6 columns of weight 5 and 15 columns of weight 4. The minimum pair count in these 9 rows of M is $6\binom{1}{2}+6\binom{2}{2}+6\binom{5}{2}+15\binom{4}{2}=156$. But it should be $4\binom{9}{2}=144$.

Solution B implies that there is a row r in M that has zeroes in the 12 left-most coordinate positions. Let the next 12 coordinate positions contain the ones of r. Consider the 6 rows that have weight 6 in the 12 left-most columns. Let D_L be the 6×12 submatrix in the leftmost columns of M and in those 6 row. Let D_M be the 6×12 submatrix adjoined to D_L and let D_R be the submatrix adjoined to D_M on the right. To minimize the pair count in those 6 rows there must be 12 columns of weight 1 in D_L, 12 columns of weight 2 in D_M and 9 columns of weight 4 in D_R. This gives a minimum pair count of $12\binom{1}{2}+12\binom{2}{2}+9\binom{4}{2}=66$. But it should be $4\binom{6}{2}=60$.

In both Solution C and D there are 4 rows that have only 0 entries in the 12 left-most coordinate positions, call this submatrix D_L. Call the remaining 4 by 21 matrix D_R. D_R has 48 1's in it so the minimum pair in the columns occurs when there are 18 columns of weight 3 and 13 columns of weight 2 in D_R. This gives a minimum of $6\binom{3}{2}+15\binom{2}{2}=33$ but it is suppose to be $4\binom{4}{2}=24$.

□

This eliminates , from list L, 26 codes which contain a d_5. Using the names which Bilous [2] gave them, the codes that are eliminated are 1 d_{10}, 2 d_8's, 2 d_7's, 7 d_6's and 14 d_5's. Note that Theorem 3.3 also eliminates the code labelled e_8 as e_8 contains both an e_3 and a d_5. There are several case when a code on the list contains several e_i's and/or d_i's. If one tries this technique on a code containing a d_4, one gets 3 solutions of which 2 can be ruled out. The remaining solution is very complicated and probably needs a computer to eliminate it.

4 Conclusion

Putting Theorem 3.2 and Theorem 3.3 together eliminates 116 of the codes on list L. We can now state our conclusion.

Theorem 4.1 There are only 378 inequivalent, doubly-even, self-orthogonal (33,16) binary codes that have no all-zero coordinate that might contain the point code of a (22,8,4)-BIBD.

Of course what this means is that the remaining codes can be tackled with computer algorithms. This has already been attempted in Bilous [4]. He has eliminated a further 299 of the codes so we can state.

Theorem 4.2 There are now only 79 inequivalent, doubly-even, self-orthogonal (33,16) binary codes that have no all-zero coordinate that might contain the point code of a (22,8,4)-BIBD.

One of the authors, Bilous has programmed the search in parallel and this is its current state.

Theorem 4.3 There are now only 11 inequivalent, doubly-even, self-orthogonal (33,16) binary codes that have no all-zero coordinate that might contain contain the point code of a (22,8,4)-BIBD.

These are the 11 codes of minimum distance 8.

References

[1] T. Beth, D. Jungnickel and H. Lenz, Design Theory I & II, Encyclopedia of Mathematics and its Apllications 69 & 78, Cambridge University Press, Cambridge, 1999.

[2] R. T. Bilous, http://www.cs.umanitoba.ca/∼/umbilou1/DoublyEvenCodes/codesandgroups (1998)

[3] R. T. Bilous, The Point Code of a $(22, 33, 12, 8, 4)$-Balanced Incomplete Block Design, Ph. D. thesis, University of Manitoba, Winnipeg, 2001.

[4] R. T. Bilous, Searching a $(33, 16)$ doubly-even code for a $(22, 33, 12, 8, 4)$-BIBD, J Combin Math Combin Comput 46 (2003), 53–64.

[5] R. T. Bilous and G. H. J. van Rees, An enumeration of binary self-dual codes of length 32, Des Codes Cryptogr 26 (2002), 61–86.

[6] R. T. Bilous, An enumeration of binary self-dual codes of length 34, J Combin Math Combin Comput, submitted

[7] C. J. Colbourn and J. H. Dinitz (editors), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, 1996.

[8] R. A. Fisher and F. Yates, Statistical Tables for Biological, Agricultural and Medical Research, Longman, London, 1938.

[9] M. Hall Jr., R. Roth, G. H. J. van Rees and S. A. Vanstone, On designs (22,33,12,8,4) J. Combin Theory, Ser A 47 (1988), 157–175.

[10] N. Hamada and Y. Kobayshi, On the block structure of BIB designs with parameters $v = 2, b = 33r = 12, k = 8$ and $\lambda = 4$, J Combin Theory, Ser A 24 (1978), 75–83.

[11] S. Kapralov, Combinatorial $2-(22, 8, 4)$ designs with automorphisms of order 3 fixing one point, Math. Educ. in Math., Proceedings of the XVI Spring Conference of Union of Bulgarian Mathematicians, (1987), 453–458.

[12] C. W. H. Lam, L. Thiel, and S. Swiercz, The nonexistence of finite projective planes of order 10, Canad J Math 41(6) (1989), 1117–1123.

[13] I. Landgev and V. Tonchev, Automorphisms of $2-(22, 8, 4)$ designs, Discete Math 77 (1989), 177–189.

[14] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North-Holland, Amsterdam (1977).

[15] F. J. MacWilliams, N. J. A. Sloane and J. G. Thompson, Good Self Dual Codes Exist, Discrete Math. 3 (1972), 153–162.

[16] B. D. McKay and S. P. Radziszowski, $2-(22, 8, 4)$ designs have no blocks of type 3, J Combin Math Combin Comput 30 (1999), 251–253.

[17] B. D. McKay and S. P. Radziszowski, Towards deciding the existence of $2-(22, 8, 4)$ designs, J Combin Math Combin Comput 22 (1996), 211–222.

[18] P. R. J. Östergård, A 2-(22,8,4) design cannot have a 2-(10,4,4) subdesign, Designs, Codes and Cryptography, **27** (2002), 257–260.

[19] V. S. Pless and W. C. Huffman (editors), Handbook of Coding Theory, Elsevier, Amsterdam, 1998.

[20] 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.

[21] G. H. J. van Rees; $(22, 33, 12, 8, 4)$-BIBD, an Update, In Computational and Constructive Design Theory, Ed. W. D. Wallis; Kluwer (1996), 337–357.