

No Extendable Biplane of Order Nine*

BHASKAR BAGCHI

*Statistics and Mathematics Division,
Indian Statistical Institute,
203 Barrackpore Trunk Road, Calcutta 700 035, India*

Communicated by Marshall Hall, Jr.

Received December 10, 1986

We prove the nonexistence of 3-(57, 12, 2) designs. This is achieved by a detailed analysis of the ternary code of a putative 3-design with these parameters. In view of a theorem of Mesner, our result is equivalent to nonexistence of triangle-free strongly regular graphs of order 324 and valency 57. © 1988 Academic Press, Inc.

1. INTRODUCTION

In [6] Mesner observed that for each $\lambda \geq 1$ it is parametrically feasible that a (symmetric) 2-design with parameters

$$v = (\lambda + 2)(\lambda^2 + 4\lambda + 2), \quad k = \lambda^2 + 3\lambda + 1, \quad \lambda_2 = \lambda \quad (1.1)$$

may be extendable to a 3-design with parameters

$$v = (\lambda + 1)(\lambda^2 + 5\lambda + 5), \quad k = (\lambda + 1)(\lambda + 2), \quad \lambda_3 = \lambda. \quad (1.2)$$

In the above, as also later, given a t -design δ , $\lambda_i = \lambda_i(\delta)$, $0 \leq i \leq t$, denotes the number of blocks of δ containing a point-set of size i .

Mesner also proved in [6] that the existence of a 3-design (1.2) is equivalent to the existence of a strongly regular graph with parameters

$$((\lambda + 1)^2(\lambda + 4)^2, (\lambda + 1)(\lambda^2 + 5\lambda + 5), 0, (\lambda + 1)(\lambda + 2)) \quad (1.3)$$

Namely, given a strongly regular graph (1.3), fix a vertex x and look at the incidence system whose points are the vertices adjacent to x , blocks are the vertices (other than x) nonadjacent to x , and incidence is defined by adjacency in the graph. This system is a 3-design (1.2) (see Theorem (5.5) in [2, p. 41]). Conversely, given a design (1.2), this construction can be uniquely reversed to get the graph (1.3).

* Technical Report No. 18/86 of the Indian Statistical Institute.

In [1], Cameron proved that if a 3 - (v, k, λ_3) design δ is an extension of a symmetric 2 -design, then one of the following possibilities holds: (i) $v = 496$, $k = 40$, $\lambda_3 = 3$, (ii) δ is a Hadamard 3 -design, i.e., $v = 4t$, $k = 2t$, $\lambda_3 = t - 1$ for some $t \geq 2$ (this is coexistent with Hadamard matrices of order $4t$), or (iii) δ has the parameters as in (1.2) for some $\lambda \geq 1$. (Cameron also mentions the possibility of a 3 - $(112, 12, 1)$ design—but this is now ruled out by the computer-aided result in [5].) A recent study of the series (1.2) was done by Sane, Shrikhande, and Singhi in [8].

When $\lambda = 1$, (1.1) is the (unique) projective plane of order four which is well known to have three different but isomorphic extensions yielding the first of the three Witt designs; it admits the sporadic simple group M_{22} . The corresponding graph (1.3) is the Higman-Sims graph admitting the sporadic simple group HS as an automorphism group.

In this paper we investigate the case $\lambda = 2$ and prove that the 3 -design (1.2) does not exist in this case. When $\lambda = 2$, (1.1) is a biplane of order nine. Four distinct biplanes of order nine are known at present (see [3]), and—according to the authors of [2]—one of these was examined by Hall and Baumert and found to be non-extendable. By our result, no biplane of order nine (known or unknown) can be extended to a 3 -design. In view of Mesner's theorem quoted above, this also implies nonexistence of a $(324, 57, 0, 12)$ strongly regular graph. Also, together with Cameron's theorem, it implies that the only extendable biplane is the one of order three (which is also a Hadamard 2 -design).

Since each contraction of a design (1.2) is symmetric, it follows that any two distinct blocks of (1.2) meet in 0 or $\lambda + 1$ points. Further the block size k is a multiple of $\lambda + 1$. Hence, for any prime p dividing $\lambda + 1$, the p -ary code C of the design (i.e., the code over the field of order p generated by the columns of its $v \times \lambda_0(0, 1)$ incidence matrix) is self-orthogonal: $C \subseteq C^\perp$. Hence the dimension of C is at most $v/2$. In the following, we look at the ternary code C of a putative 3 - $(57, 12, 2)$ design. By the above, C is self-orthogonal and hence $\dim(C) \leq 28$. In Section 2, we make use of certain structural properties of the design proved in [8] to conclude that $\dim C = 28$, i.e., C is maximal self-orthogonal. This, together with further arguments in Section 3, places strong restrictions on the weight enumerator of C^\perp . In Section 4 we use McWilliam's identity (see [2] or [4]) to prove that these restrictions determine the Hamming weight enumerator of C . Indeed, it turns out that all the non-trivial coefficients of this weight enumerator are fractions, a contradiction which establishes the non-existence of the design. A computer has been resorted to only in the final section in order to solve a system of 16 linear equations in as many unknowns; this took only 3 seconds of total processing time.

There is a rich tradition of application of coding theory to designs. See the paper [4] by Hall for a representative sample. But it appears that the

hitherto successful applications have been to symmetric 2-designs (the fruitful interplay between the Witt designs and the Golay codes excepted) and to construction of t -designs from codes via the Assmus-Matson theorem. While we have not striven for generality in this paper, we hope that the techniques used (namely the restriction homomorphisms in Section 2 and the equations in Section 3) may have wider applicability in designs.

2. DIMENSION

2.1. Notation and Terminology. We shall regard a ternary code C , with X as its set of co-ordinate positions, as a vector subspace of the F_3 -vector space F_3^X of all F_3 -valued functions on X . Here $F_3 = \{0, 1, -1\}$ with field operations modulo 3. $n = |X|$ is the length of the code. For $w \in C$, the support of w is the set $S = \{x \in X: w(x) \neq 0\}$. Thus $S = S^+ \cup S^-$, where $S^\pm = \{x \in X: w(x) = \pm 1\}$. S^+ (S^-) will be called the positive (negative) support of w . The weight $|w|$ of w is by definition the size $|S|$ of S . If $s^\pm = |S^\pm|$, we shall say that the word w is of type (s^+, s^-) . Notice that the type of $-w$ is (s^-, s^+) . Thus, while investigating the existence of a word w of type (a, b) (say), we can assume without loss of generality that $a \geq b$ and hence $a \geq \frac{1}{2}|w|$. For any subset B of X , the word $X_B \in F_3^X$ (the indicator of B) is defined by $X_B(x) = 1$ if $x \in B$, $= 0$ if $x \in X \setminus B$. In particular, the indicator of X itself will be denoted by 1 (the "all-one" vector). Note that different occurrences of the symbol 1 may have different meanings depending on the code to which it belongs (this is especially so during the proof of Proposition 2.7 below). But in each case the meaning should be clear from the context.

If \mathcal{B} is a family of subsets of X , then the subcode of F_3^X generated by $\{X_B: B \in \mathcal{B}\}$ will be called the *ternary code of the incidence system* (X, \mathcal{B}) .

If Y is a subset of X , the vector space homomorphism $h: F_3^X \rightarrow F_3^Y$, defined by $h(w) =$ the restriction of w to Y , will be called a *restriction homomorphism*. If C is a subcode of F_3^X , the restriction of h to C will be called a *restriction homomorphism on C* , and the image $h(C)$ will be called the *restriction of C to Y* . Note that if C is the ternary code of an incidence system (X, \mathcal{B}) , then the restriction of C to Y is the ternary code of the incidence system (Y, \mathcal{B}) , where \mathcal{B} consists of the nonempty intersections $\beta \cap Y$, $\beta \in \mathcal{B}$.

2.2. LEMMA. *If C is the ternary code of a $2-(v, k, \lambda_2)$ design then the minimum weight of C^\perp is at least $\frac{1}{2}\{2(v-1)/(k-1)+1\}$.*

Proof. Let $S = S^+ \cup S^-$ be the support of a nonzero word of C^\perp . Without loss of generality $|S^+| \geq |S^-|$. Fix $x \in S^+$. Let e_x be the number

of blocks through x which meet S in $i+1$ points. Clearly $e_0=0$. Also, since each of the e_i blocks through x meeting S in a doubleton meets S in a unique point, we have $e_1 \leq \lambda_2 |S| \leq (\lambda_2/2)|S|$. Now a two-way counting gives

$$\begin{aligned} \lambda_2(|S|-1) &= \sum_{i \geq 1} i e_i \geq e_1 + 2 \sum_{i \geq 2} e_i \\ &= e_1 + 2(\lambda_1 - e_1) \\ &= 2\lambda_1 - e_1 \geq 2\lambda_1 - (\lambda_2/2)|S|. \end{aligned}$$

Hence

$$|S| \geq \frac{2}{3} \left(\frac{2\lambda_1}{\lambda_2} + 1 \right) = \frac{2}{3} \left(\frac{2(v-1)}{k-1} + 1 \right).$$

2.3. LEMMA. *Let C be the ternary code of a $1-(v, k, \lambda_1)$ design. Then (i) if $k \equiv 0 \pmod{3}$ then $1 \in C^\perp$, and (ii) if $\lambda_1 \not\equiv 0 \pmod{3}$ then $1 \in C$.*

Proof. Part (i) is trivial. Part (ii) holds since the sum of the indicators of all the blocks (which is a word of C) is $\lambda_1 \cdot 1$.

2.4. LEMMA. *The ternary code of the (trivial) $3-(12, 3, 1)$ design is of dimension 11.*

Proof. Clearly this code is 1^\perp .

2.5. LEMMA. *The ternary code of a $2-(9, 3, 3)$ design, in which no block is repeated thrice, is of dimension 8.*

Proof. Let C be this code. We shall show that $C=1^\perp$. By Lemma 2.3(i), $C \subseteq 1^\perp$, so it suffices to show $C^\perp \subseteq \langle 1 \rangle$. Let $0 \neq w \in C^\perp$. By Lemma 2.2, $|w| \geq 6$. So, if S^* is the positive support of w , then (replacing w by $-w$ if necessary) we may assume $u = |S^*| \geq 3$. Since each block has size 3 and is orthogonal to w , no block meets S^* in exactly two points. Hence the given design induces a $2-(u, 3, 3)$ design on S^* . The integrality requirement for its existence shows u is odd. Also, by hypothesis the design has no $2-(3, 3, 3)$ subdesign, so that $u \neq 3$. Hence $|S^*| = u \geq 5$, so that $|1-w| \leq 4$. Since 1 and w belong to C^\perp and the minimum weight of C^\perp is at least 6, it follows that $1-w=0$, i.e., $w=1$.

In order to state and prove our next lemma, we recall the following from [8]. A maximal 3-arc in a (symmetric) $2-(45, 12, 3)$ design F is a set of nine points which meets every block of F in zero or three points. Given a maximal 3-arc A in F , there are exactly nine blocks of F disjoint from A . These nine blocks constitute a maximal 3-arc A^* in the dual F^* of F . The

incidence system induced by F on A is a $2-(9, 3, 3)$ design $I(A)$ ((i), (ii), and (iii) of Theorem 3.6 in [8] with $\lambda=2$). Recall that if x and y are two distinct points of F , then the line joining x and y is defined to be the intersection of the blocks through x and y ; the line is called trivial if it has just two points. Since $\lambda_2(F)=3$, all the lines of F are trivial if and only if the same is true of its dual F^* . If this is the case, then for any maximal 3-arc A of F , no block of $I(A)$ is repeated thrice, and the same holds for the design $I^*(A^*)$ induced by F^* on A^* .

2.6. LEMMA. *Let F be a $2-(45, 12, 3)$ design all of whose lines are trivial. Suppose F has a maximal 3-arc. Then the dimension of the ternary code of F is at least 16.*

Proof. Let X be the point set of F and write $X=Y \cup Z$, where Y is a maximal 3-arc and Z is its complement. Let G_1 be the incidence system induced by F on Y and let G_2 be the incidence system with Z as its point-set and the nine blocks of F disjoint from Y as its blocks. Then G_1 is a design satisfying the hypothesis of Lemma 2.5, and G_2 is the dual of such a design. Hence if C_1 and C_2 are the ternary codes of G_1 and G_2 , respectively, then by Lemma 2.5, we have $\dim(C_1) = \dim(C_2) = 8$.

(Note that the dimension of the code of any incidence system equals that of its dual. This is because any matrix and its transpose have the same rank over any field.) Let C_0 be the ternary code of F , and let $h: C_0 \rightarrow C_1$ be the restriction homomorphism. Then we have $\text{image}(h) = C_1$ and kernel $(h) \supseteq C_2$. Hence

$$\dim C_0 = \dim \text{image}(h) + \dim \text{kernel}(h) \geq \dim C_1 + \dim C_2 = 8 + 8 = 16.$$

2.7. PROPOSITION. *The ternary code of a $3-(57, 12, 2)$ design is maximal self-orthogonal.*

Proof. As noted in the Introduction, the ternary code C of a $3-(57, 12, 2)$ design E is self-orthogonal (i.e., $C \subseteq C^\perp$) and hence $\dim C \leq 28$. So it suffices to show that $\dim C \geq 28$.

Let C' be the ternary code of the incidence system induced by E on a fixed block B of E . Since any two blocks of E meet in zero or three points and $\lambda_3(E)=2$, this system is a $3-(12, 3, 1)$ design. Write the point set of E as $B \cup X$, where X is the complement of B . Let F be the incidence system with point-set X whose blocks are the blocks of E disjoint from B . From the proof of Cameron's theorem in [1] one sees that F is a $2-(45, 12, 3)$ design. By Proposition 2.6 and Theorem 3.5(v) of [8], F satisfies the hypothesis of Lemma 2.6 above. Let C_0 be the ternary code of F . Obviously C_0 may be regarded as a subcode of C . Let $h: C \rightarrow C'$ be the restriction homomorphism. Then $\text{image}(h) = C'$ and $\text{kernel}(h) \supseteq C_0$. Hence, $\dim C \geq \dim C' + \dim C_0 \geq 11 + 16 = 27$ by Lemma 2.4 and Lemma 2.6. So

it is enough to see that equality cannot hold in this inequality. Suppose the contrary. Then $C_0 = \text{Kernel}(h)$ and $\dim C_0 = 16$. By Lemma 2.3(ii), $1 \in C$ and hence $1 - X_B \in \text{Kernel}(h)$. That is, $1 \in C_0$. Take a block $B' \neq B$ of E which is not a block of F . Let $Y = X \cap B'$. Then Y is a maximal 3-arc of F (Theorem 3.6(vi) of [8]). Write X as a disjoint union $X = Y \cup Z$. Let C_1 and C_2 be as in the proof of Lemma 2.6. Suppose, if possible, that $1 \in C_2$. Then $X_Z \in C_0$ and hence $X_Y = 1 - X_Z \in C_0$. It follows that the word $X_B - X_Y$ of weight 3 belongs to C —contradicting Lemma 2.2. So $1 \notin C_2$. If $f: C_0 \rightarrow F_3^2$ is the restriction homomorphism then $1 = f(1) \in \text{Image}(f) \supseteq C_2$ and $1 \notin C_2$. Hence $\dim \text{Image}(f) \geq \dim C_2 + 1$. Also, $\text{kernel}(f) \supseteq C_1$. Hence $\dim C_0 \geq \dim C_1 + \dim C_2 + 1 = 17$ by Lemma 2.5, a contradiction.

2.8. LEMMA. *Let C be a maximal self-orthogonal ternary code of length $n \equiv 1 \pmod{4}$. Then all the words of C^\perp have weight $\equiv 0$ or $1 \pmod{3}$. Further, a word of C^\perp is in C if and only if its weight is $0 \pmod{3}$.*

Proof. Let (\cdot, \cdot) be the standard inner product on $C^\perp \supseteq C$. Note that $|w| = (w, w) \pmod{3}$ for $w \in C^\perp$. Since C is self-orthogonal, it follows that the weight of each word of C is $0 \pmod{3}$. Let $C(i)$, $i \in F_3$, be the cosets of C in C^\perp , with $C(0) = C$. Fix $\alpha \in C(1)$. Hence $-\alpha \in C(-1)$. Thus each word of C^\perp not in C is of the form $w \pm \alpha$ with $w \in C$. Since $\alpha \in C^\perp$, we have $|w \pm \alpha| = (w \pm \alpha, w \pm \alpha) = (\alpha, \alpha) = |\alpha| \pmod{3}$. Thus the weight of a word of C^\perp not in C is a constant modulo 3. This constant cannot be 0 since that would force C^\perp to be self-orthogonal and hence self-dual—impossible as the length n is odd. Suppose, if possible, that $|w| = 2 \pmod{3}$ for all words w of C^\perp , and not of C . Let $f: C^\perp \rightarrow F_3$ be defined by $f(w) = i$ if $w \in C(i)$. Clearly f is a linear functional on C^\perp . Hence $C^* = \{(w, f(w)) : w \in C^\perp\}$ is a ternary (linear) code of length $n+1$, with $\dim C^* \geq \dim C^\perp = (n+1)/2$. Under our assumption, one checks readily that C^* is self-orthogonal and hence self-dual. Thus we have a ternary self-dual code of length $n+1 \equiv 2 \pmod{4}$. But this is impossible by Theorem 1 in [7], since -1 is a non-square in F_3 .

2.9. PROPOSITION. *If C is the ternary code of a $3-(57, 12, 2)$ design, then no word of C^\perp has weight $2 \pmod{3}$. Further, a word of C^\perp has weight $0 \pmod{3}$ if and only if it is in C .*

Proof. Proposition 2.7 and Lemma 2.8.

3. SMALL WEIGHTS

3.1 LEMMA. *Let C be a maximal self-orthogonal ternary code of length $\equiv 1 \pmod{4}$. Suppose $1 \in C$. If (a, b) is the type of a word in C^\perp then either $a = b = 0 \pmod{3}$ or $a = b = -1 \pmod{3}$.*

Proof. Let $w \in C^\perp$ be of type (a, b) . Since 1 is orthogonal to w , we have $a - b = 0 \pmod{3}$. By Lemma 2.8, we also have $a + b = 0$ or $1 \pmod{3}$. Hence the result.

3.2. More Notations. If C is the ternary code of an incidence system δ , then for any word $w \in C^\perp$ and any block B of δ , we say that B meets w in $i + j$ if $|B \cap S^+| = i$, $|B \cap S^-| = j$. Here S^+ (S^-) is the positive (negative) support of w . We denote by $[i, j]$ the number of blocks of δ which meet w in $i + j$. We call these numbers $[i, j]$ the *intersection numbers of w* .

3.3. LEMMA. Let C be the ternary code of a $1 - (v, k, \lambda_1)$ design. Suppose C is self-orthogonal. Let $[i, j] \neq 0$ be an intersection number of a word w of type (a, b) in C^\perp . Then:

$$(1) \quad i = j \pmod{3}, 0 \leq i \leq a, 0 \leq j \leq b, i + j \leq k.$$

(2) If, further, there is no word w' in C^\perp such that $0 < |w'| < |w|$ and $|w'| = |w| \pmod{3}$ then either $\pm w$ is the indicator of a block or else $i + 2j \leq k$, $2i + j \leq k$.

(3) If $i + 2j = k$ or $2i + j = k$ then there is a word in C^\perp of type (a', b') , where $a' = a - i + j$, $b' = b + i - j$.

Proof. Let B be a block meeting w in $i + j$.

(1) Since the indicator of B is orthogonal to w , we have $i = j \pmod{3}$. The inequalities are trivial.

(2) Add (respectively subtract) the indicator of B —which is in C and hence in C^\perp —to (from) w to get a word w' in C^\perp of type (a', b') when $a' = a + k - 2i - j$, $b' = b + i - j$ (respectively $a' = a - i + j$, $b' = b + k - i - 2j$). If $\pm w$ is not the indicator of a block then w' is a nonzero word. We have $|w'| = a' + b' = a + b + k - i - 2j = |w| + k - i - 2j$ (respectively $|w'| = |w| + k - 2i - j$). By (1) above, $i = j \pmod{3}$, whence $i + 2j = 2i + j = 0 \pmod{3}$; also, since C is self-orthogonal, $k = 0 \pmod{3}$. Hence $|w'| = |w| \pmod{3}$ in either case. So, by hypothesis, $|w'| \geq |w|$. Hence the required inequalities.

(3) This is proved by substituting $k = i + 2j$ or $k = 2i + j$ in the expressions for a' , b' obtained above.

3.4. LEMMA. Let C be the ternary code of a $1 - (v, k, \lambda_1)$ design, and let w be a word of type (a, b) in C^\perp . Then for any two nonnegative integers c, d with $c + d \leq t$, the intersection numbers of w satisfy

$$\sum_{i,j} \binom{i}{c} \binom{j}{d} [i, j] = \binom{a}{c} \binom{b}{d} \lambda_{c+d}. \quad (3.1)$$

Proof. Count in two ways the number of choices of c points from the positive support, d points from the negative support, and a block containing these $c + d$ points.

3.5. *On Witnesses.* In the following, we shall repeatedly face systems of linear equations of the form

$$Ax = u, \quad (3.2)$$

where $A = A_{m \times n}$ is a matrix with nonnegative integral entries and $u = u_{m \times 1}$ is a column vector with nonnegative integral entries, and we shall have to prove that (3.2) has no solution $x = x_{n \times 1}$ with nonnegative integral entries. In this context, let us say that a row vector $z = z_{1 \times m}$ is a *witness* against the system (3.2) if z has integer entries and

(i) there is a prime which divides all the entries of zA but does not divide z, u or

(ii) all the entries of zA are nonnegative but $z, u < 0$. Obviously, the production of a witness against (3.2) proves that the system has no nonnegative integral solution.

3.6. PROPOSITION. *Let C be the ternary code of a $3 - (57, 12, 2)$ design. Then the minimum weight of C^\perp is 12 and C^\perp has no word of weight 13.*

Proof. In the following, we shall make repeated use of Lemma 3.3 in order to narrow down the possibilities for the nonzero intersection numbers of the word under consideration. In each such application, full use will be made—without explicit mention—of the information available till that point.

Note that for a $3 - (57, 12, 2)$ design we have $v = 57, k = 12, \lambda_0 = 266, \lambda_1 = 56, \lambda_2 = 11, \lambda_3 = 2$. By Lemma 2.2, the minimum weight of C^\perp is at least 8, whereas by Proposition 2.9, C^\perp has no word of weight 8 or 11. So it suffices to show that C^\perp has no word of weight 9, 10, or 13. Let $w \in C^\perp$ be a word of type (a, b) with $a + b = 9, 10, \text{ or } 13$. Without loss of generality $a \geq b$. Then Lemma 3.1 and Proposition 2.7 together allow the following possibilities for (a, b) :

Case 1. $a + b = 9$. Then $(a, b) = (9, 0)$ or $(6, 3)$.

First let $(a, b) = (9, 0)$. By Lemma 3.3, the only possibly nonzero intersection numbers are $[6, 0], [3, 0]$, and $[0, 0]$.

Equation (3.1) with $(c, d) = (3, 0), (2, 0)$ yields a system (3.2) with

$$u' = (168, 396), \quad x' = \{[6, 0], [3, 0]\},$$

and

$$A = \begin{pmatrix} 20 & 1 \\ 15 & 3 \end{pmatrix}.$$

$(3, -1)$ is a witness against this system. So there is no word of type $(9, 0)$ (and hence none of type $(0, 9)$) in C^\perp .

Next let $(a, b) = (6, 3)$. By Lemma 3.3, the only possibly nonzero intersection numbers are $[5, 2]$, $[4, 1]$, $[3, 3]$, $[3, 0]$, $[2, 2]$, $[1, 1]$, $[0, 3]$, and $[0, 0]$.

Equation (3.1) with $(c, d) = (3, 0)$, $(2, 0)$, $(1, 2)$ yields a system (3.2) with

$$\begin{aligned} \mathbf{u}' &= (40, 165, 36), \\ \mathbf{x}' &= ([5, 2], [4, 1], [3, 3], [3, 0], [2, 2]), \end{aligned}$$

and

$$A = \begin{pmatrix} 10 & 4 & 1 & 1 & 0 \\ 10 & 6 & 3 & 3 & 1 \\ 5 & 0 & 9 & 0 & 2 \end{pmatrix}.$$

$(6, -2, 1)$ is a witness against this system. So there is no word of weight 9 in C^\perp .

Case 2. $a + b = 10$. Then $(a, b) = (8, 2)$ or $(5, 5)$.

First let $(a, b) = (8, 2)$. By Lemma 3.3, the only possibly nonzero intersection numbers are $[6, 0]$, $[5, 2]$, $[4, 1]$, $[3, 0]$, $[2, 2]$, $[1, 1]$, $[0, 0]$.

Equation (3.1) with $(c, d) = (1, 2)$, $(0, 2)$ yields a system (3.2) with

$$\mathbf{u}' = (16, 11), \quad \mathbf{x}' = ([5, 2], [2, 2]),$$

and

$$A = \begin{pmatrix} 5 & 2 \\ 1 & 1 \end{pmatrix}.$$

$(1, -2)$ is a witness against this system. Hence there is no word of type $(8, 2)$ (or of type $(2, 8)$) in C^\perp .

Next let $(a, b) = (5, 5)$. By Lemma 3.3, the only possibly nonzero intersection numbers are $[4, 4]$, $[4, 1]$, $[3, 3]$, $[3, 0]$, $[2, 2]$, $[1, 4]$, $[1, 1]$, $[0, 3]$, and $[0, 0]$.

Equation (3.1) with $(c, d) = (2, 1)$, $(2, 0)$, $(1, 2)$, $(1, 1)$, $(1, 0)$, $(0, 3)$, and $(0, 2)$ yields a system (3.2) with

$$\begin{aligned} \mathbf{u}' &= (100, 110, 100, 275, 280, 20, 110), \\ \mathbf{x}' &= ([4, 4], [4, 1], [3, 3], [3, 0], [2, 2], [1, 4], \\ &\quad [1, 1], [0, 3]), \end{aligned}$$

and

$$A = \begin{pmatrix} 24 & 6 & 9 & 0 & 2 & 0 & 0 & 0 \\ 6 & 6 & 3 & 3 & 1 & 0 & 0 & 0 \\ 24 & 0 & 9 & 0 & 2 & 6 & 0 & 0 \\ 16 & 4 & 9 & 0 & 4 & 4 & 1 & 0 \\ 4 & 4 & 3 & 3 & 2 & 1 & 1 & 0 \\ 4 & 0 & 1 & 0 & 0 & 4 & 0 & 1 \\ 6 & 0 & 3 & 0 & 1 & 6 & 0 & 3 \end{pmatrix}$$

$(1, 2, -3, 2, -2, 6, -2)$ is a witness against this system. So there is no word of weight 10 in C^\perp .

Case 3. $a + b = 13$. Then $(a, b) = (11, 2)$ or $(8, 5)$.

First let $(a, b) = (11, 2)$. By Lemma 3.3, the only possibly nonzero intersection numbers are $[6, 0]$, $[5, 2]$, $[4, 1]$, $[3, 0]$, $[2, 2]$, $[1, 1]$, and $[0, 0]$.

Equation (3.1) with $(c, d) = (3, 0)$, $(2, 1)$, $(2, 0)$, $(1, 2)$ yields a system (3.2) with

$$\mathbf{u}' = (330, 220, 605, 22),$$

$$\mathbf{x}' = ([6, 0], [5, 2], [4, 1], [3, 0], [2, 2]),$$

and

$$A = \begin{pmatrix} 20 & 10 & 4 & 1 & 0 \\ 0 & 20 & 6 & 0 & 2 \\ 15 & 10 & 6 & 3 & 1 \\ 0 & 5 & 0 & 0 & 2 \end{pmatrix}.$$

$(2, 1, 1, 1)$ is a witness against this system. So there is no word of type $(11, 2)$ (or $(2, 11)$) in C^\perp .

Next let $(a, b) = (8, 5)$. By Lemma 3.3, the only possibly nonzero intersection numbers are $[5, 2]$, $[4, 4]$, $[4, 1]$, $[3, 3]$, $[3, 0]$, $[2, 2]$, $[1, 4]$, $[1, 1]$, $[0, 3]$, and $[0, 0]$.

Equation (3.1) with $(c, d) = (0, 1)$, $(0, 2)$, $(0, 3)$, $(1, 0)$, $(2, 0)$, $(3, 0)$, $(1, 2)$, and $(2, 1)$ yields a system (3.2) with

$$\mathbf{u}' = (280, 110, 20, 448, 308, 112, 160, 280),$$

$$\mathbf{x}' = ([5, 2], [4, 4], [4, 1], [3, 3], [3, 0], [2, 2], [1, 4],$$

$$[1, 1], [0, 3]),$$

and

$$A = \begin{pmatrix} 2 & 4 & 1 & 3 & 0 & 2 & 4 & 1 & 3 \\ 1 & 6 & 0 & 3 & 0 & 1 & 6 & 0 & 3 \\ 0 & 4 & 0 & 1 & 0 & 0 & 4 & 0 & 1 \\ 5 & 4 & 4 & 3 & 3 & 2 & 1 & 1 & 0 \\ 10 & 6 & 6 & 3 & 3 & 1 & 0 & 0 & 0 \\ 10 & 4 & 4 & 1 & 1 & 0 & 0 & 0 & 0 \\ 5 & 24 & 0 & 9 & 0 & 2 & 6 & 0 & 0 \\ 20 & 24 & 6 & 9 & 0 & 2 & 0 & 0 & 0 \end{pmatrix}$$

$(1, -2, -2, -1, 2, 2, 2, -2)$ is a witness against this system. So there is no word of weight 13 in C^\perp .

4. THE CONTRADICTION

4.1. LEMMA. *There is no maximal self-orthogonal code C of length 57 such that the minimum weight of C^\perp is 12 and C^\perp has no word of weight 13.*

Proof. The Hamming weight enumerator $C(x, y)$ of such a code C may be written as

$$C(x, y) = y^{57} + \sum_{k=0}^{15} a_k \cdot x^{3k+12} y^{45-3k} \quad (4.1)$$

By McWilliam's identity [2, 4], the Hamming weight enumerator $C^\perp(x, y)$ of C^\perp is given by

$$C^\perp(x, y) = 3^{-28} \cdot C(y-x, y+2x). \quad (4.2)$$

By assumption on C and Lemma 2.8, C^\perp has no word of weight t for the following values of t :

$$t = 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 17, 20, 23, 26, 29. \quad (4.3)$$

Therefore the coefficient of $x^t y^{57-t}$ in the right-hand side of (4.2) equals zero for the value of t listed in (4.3). Using (4.1), this yields equations in the a_k 's which, together with the obvious equation $\sum_{k=0}^{15} a_k = 3^{28} - 1$, constitutes a system of 16 linear equations in the 16 unknowns a_k . By the aid of a computer, we find that the matrix of coefficients of this system is nonsingular, so that the a_k 's are uniquely determined—all these a_k 's turn out to be fractional. Contradiction.

Finally, we have:

4.2. THEOREM. *There is no $3 - (57, 12, 2)$ design.*

Proof. Follows from Propositions 2.7 and 3.6 and Lemma 4.1.

ACKNOWLEDGMENT

The author thanks S. S. Sane for suggesting that it may be worthwhile to investigate the ternary code of a $3 - (57, 12, 2)$ design.

REFERENCES

1. P. J. CAMERON, Extending symmetric design, *J. Combin. Theory Ser. A* 14 (1973), 215–220.
2. P. J. CAMERON AND J. H. VAN LINT, "Graphs, Codes and Designs," London Mathematical Society Lecture Note Series, Vol. 43, Cambridge Univ. Press, Cambridge, 1980.
3. R. H. F. DENNISTON, On biplanes with 56 points, *Ars. Combin.* 9 (1980), 167–179.
4. M. HALL, JR., Coding theory of designs, in "Finite Geometries and Designs" (P. J. Cameron, J. W. P. Hirschfeld, and D. R. Hughes, Eds.), pp. 134–145, London Mathematical Society Lecture Note Series, Vol. 49, Cambridge Univ. Press, Cambridge, 1980.
5. C. W. H. LAM, L. THIEL, S. SWIEREZ, AND J. MCKAY, The nonexistence of ovals in a projective plane of order 10, *Discrete Math.* 45 (1983), 319–321.
6. D. M. MESNER, Negative Latin square designs, Inst. Statist. Mimeo. Ser. No. 410, Chapel Hill, NC, 1964.
7. V. PLESS, On the uniqueness of the Golay codes, *J. Combin. Theory* 5 (1968), 215–228.
8. S. S. SANE, S. S. SHRIKHANDE, AND N. M. SINGHI, Maximal arcs in designs, *Graphs Combin.* 1 (1985), 97–106.