The 36 officers problem

Eric Badstübner

July 16, 2017

1 The 36 officers problem

Theorem 1.0.1. *A transversal design $TD(6,4)$ does not exist (and hence no pair of orthogonal Latin squares of order 6).*

Let X be the set of points, $|X| = 24$, $\mathcal{A}$ the blocks, $|\mathcal{A}| = 36$, $|B| = 4$ for $B \in \mathcal{A}$, $\mathcal{G} = \{G_1, G_2, G_3, G_4\}$ the groups, $|G_i| = 6$.

Set $\mathcal{B} = \mathcal{A} \cup \mathcal{G}$, then the design $\mathcal{P} = (X, \mathcal{B})$ satisfies:

$$|X| = 24,\ |\mathcal{B}| = 40;\ 4 \text{ blocks have size } 6;\ 36 \text{ blocks have size } 4.$$

(A) Every element is in precisely 7 blocks.

(B) Any two distinct elements are in exactly one common block.

Let $M = (m_{ij})$ be the 24×40-incidence matrix

$$m_{ij} = \begin{cases} 1 & \text{if } x_i \in B_j \\ 0 & \text{if } x_i \notin B_j. \end{cases}$$

1.1 A

Consider the rows as vectors in $\mathbb{F}_2^{40}$, and denote by V the vector space generated by the rows $r_1, \cdots, r_{24}$. By (A), (B)

$$\langle r_i, r_j \rangle = 1 \text{ for any } i, j \text{ (since } 7 \equiv 1 \pmod 2).$$

Lemma 1.1.1. *The vector space $V \subseteq \mathbb{F}_2^{40}$ has* $\dim(V) \leq 20$.

Proof. Let $\{r_1, \dots, r_d\}$ be a basis of V. Now $\langle r_i, r_j + r_k\rangle = \langle r_i, r_j\rangle + \langle r_i, r_k\rangle = 0$ for all i, j, k, hence $r_1 + r_2, r_1 + r_3, \dots, r_1 + r_d \in V^\perp$, and they are clearly independent. Hence

$$\dim(V) \geq \dim(V \cap V^\perp) \geq d - 1,$$

and therefore

$$\dim(V) = 40 - \dim(V^\perp) \leq 40 - (\dim(V) - 1).$$

This implies $2\dim(V) \leq 41$, thus $\dim(V) \leq 20$. $\square$

Since M has 24 rows and $\dim(V) \leq 20$, there must be at least 4 linearly independent relations between the rows. Such a relation corresponds to a subset $Y \subseteq X$, such that $|Y \cap B_i|$ is even for $i = 1, \dots, 40$.

Examples of such are: $Y = G_1 \cup G_2,\ Y = G_1 \cup G_3,\ G_1 \cup G_4$, whose characteristic vectors are linearly independent. The other three combinations $G_i \cup G_j,\ i, j \geq 2$ are linearly dependent on these.

Hence there must be a set $Y \neq G_i \cup G_j$ which corresponds to a linearly dependent set of rows. Let us call such a set $Y \subseteq X$ an <u>even</u> set:

$$|Y \cap B_i| \text{ even for } i = 1, \dots, 40.$$

Note that the complement of an even set is even. The goal is therefore to show that such an even set cannot exist.

1.2 B

Let Y be an even set, where by taking complements we may assume $|Y| \leq 12$, and let $Q = (Y, Y \cap B_i)$ be the sub-design. Suppose $|Y| = m \leq 12$, and that Q has b_i blocks of size i. Then

$$b_0 + b_2 + b_4 + b_6 = 40, \tag{1}$$

which is clear since the number of blocks did not change and the size of each block in P is an even number at most 6. For the next equation, recall that each element of X is contained in exactly seven blocks in P and this property is carried over to Q. Hence,

$$\sum_{B \in Q} \sum_{x \in Y} \mathbb{1}_{x \in B} = \sum_{x \in Y} \sum_{B \in Q} \mathbb{1}_{x \in B},$$

which gives

$$\sum_{B \in Q} |B| = \sum_{x \in Y} 7$$

and therefore

$$2b_2 + 4b_4 + 6b_6 = 7m. \tag{2}$$

For the next equation, we double count the triples (x, y, B) in Q where $\{x, y\} \in B$.

$$\sum_{B \in Q} \sum_{\{x,y\} \in \binom{X}{2}} \mathbb{1}_{\{x,y\} \subseteq B} = \sum_{\{x,y\} \in \binom{X}{2}} \sum_{B \in Q} \mathbb{1}_{\{x,y\} \subseteq B},$$

yielding

$$\sum_{B \in Q} \binom{|B|}{2} = \sum_{\{x,y\} \in \binom{X}{2}} 1,$$

and hence

$$b_2 + 6b_4 + 15b_6 = \frac{m(m-1)}{2}. \tag{3}$$

Subtracting half of (2) from (3) yields

$$4b_4 + 12b_6 = \frac{m(m-8)}{2},$$

that is

$$b_4 + 3b_6 = \frac{m(m-8)}{8} = \frac{m^2}{8} - m. \tag{4}$$

It follows that $m \geq 8$ and $m \equiv 0 \pmod 4$, and therefore $m = 8$ or $m = 12$.

Now note that if Y_1, Y_2 are even sets, then so is their symmetric difference $Y_1 \Delta Y_2 = (Y_1 \cup Y_2) \setminus (Y_1 \cap Y_2) = (Y_1 \setminus Y_2) \cup (Y_2 \setminus Y_1)$. To see this, recall that for $i \in [24]$, r_i is the ith row of the incidence matrix of our original design P. Then

$$0 = \sum_{i \in Y_1} r_i + \sum_{j \in Y_2} r_j = \sum_{i \in Y_1 \setminus Y_2} r_i + \sum_{i' \in Y_1 \cap Y_2} r_{i'} + \sum_{j' \in Y_1 \cap Y_2} r_{j'} + \sum_{j \in Y_2 \setminus Y_1} r_j,$$

where on the right hand side the two summands in the middle sum up to zero. Hence we get

$$\sum_{i \in Y_1 \setminus Y_2} r_i + \sum_{j \in Y_2 \setminus Y_1} r_j = \sum_{k \in (Y_1 \setminus Y_2) \cup (Y_2 \setminus Y_1)} r_k = 0.$$

Now suppose $|Y| = 12$. Then the following distributions of the points among the 4 groups are the only possibilities (up to permutation of the groups):

$$Y: \quad 6\,4\,2\,0 \quad ; \quad 6\,2\,2\,2 \quad ; \quad 4\,4\,4\,0 \quad ; \quad 4\,4\,2\,2.$$

Note that 6 6 0 0 is excluded since then $Y = G_i \cup G_j$ for some $i \neq j$. Take $(G_1 \cup G_2)\Delta Y$, then we get even sets with distribution

$$Y' : \quad 0\,2\,2\,0 \quad ; \quad 0\,4\,2\,2 \quad ; \quad 2\,2\,4\,0 \quad ; \quad 2\,2\,2\,2.$$

The first is impossible since we require $m \geq 8$ for every even set. Each of the other cases yields $m = 8$.

Theorem 1.2.1 (conclusion)**.** *If an even set Y exists at all, then there is one with $|Y| = 8$.*

1.3 C

We will assume in the following that $|Y| = 8$. It follows immediately from equation (4) that in this case $b_4 = b_6 = 0$. Inserting into (3) gives $b_2 = 28$ and so $b_0 = 12$ by (1). Hence no 3 elements are in a block $Y \cap B$, which means

$$|Y \cap G_i| = 2, \quad i = 1, \ldots, 4.$$

Let $\hat{Q}$ be the complementary design, corresponding to the even $X \setminus Y$,

$$\hat{Q} = (X \setminus Y, (X \setminus Y) \cap B_i).$$

$\hat{Q}$ has 16 points, 4 blocks of size 4 of the form $(X \setminus Y) \cap G_i$, 12 blocks of size 4 in $\mathcal{A}$ ($b_0 = 12$) and 24 blocks of size 2 in $\mathcal{A}$ ($b_2 = 28$ and we already counted the 4 groups).

Let $Y = \{a, b, c, \ldots, h\}$, $X \setminus Y = \{1, 2, \ldots, 16\}$ and let the groups be

$$G_1 = \{1, 2, 3, 4, a, b\}, \quad G_2 = \{5, 6, 7, 8, c, d\},$$

$$G_3 = \{9, 10, 11, 12, e, f\}, \quad G_4 = \{13, 14, 15, 16, g, h\}.$$

The main tool in studying $\hat{Q}$ is the graph $G(V, E)$ with the following properties:

(i) $V = \{1, 2, \ldots, 16\}$.

(ii) $ij \in E$ iff $\{i, j\}$ is a 2-block in $\hat{Q}$.

We immediately see that $|E| = 24$.

Lemma 1.3.1. *(a) G is 3-regular.*

(b) Every $x \in V$ has exactly one neighbour in each group G_i which does not contain x.

(c) G is triangle-free.

Proof. Choose $x \in V$ and suppose x is in a blocks of size 2 in $\hat{Q}$ and b blocks of size 4. Then

$$a + b = 7,$$

since x is contained in 7 blocks. Also for a fixed x we have

$$\sum_{\substack{B \in \hat{Q} \\ x \in B}} \sum_{\substack{y \in X \setminus Y \\ y \neq x}} \mathbb{1}_{\{x,y\} \subseteq B} = \sum_{\substack{y \in X \setminus Y \\ y \neq x}} \sum_{\substack{B \in \hat{Q} \\ x \in B}} \mathbb{1}_{\{x,y\} \subseteq B},$$

which gives

$$\sum_{\substack{B \in \hat{Q} \\ x \in B}} (|B| - 1) = \sum_{\substack{y \in X \setminus Y \\ y \neq x}} 1,$$

and so

$$a + 3b = 15.$$

This gives $a = 3$ and $b = 4$; hence G is 3-regular.

Look at these 3 blocks $B_i \in \mathcal{B}$ with $x \in B_i$, $|B_i \cap Y| = |B_i \cap (X \setminus Y)| = 2$. Suppose w.l.o.g. $x \in G_1$. Then the B_i's must contain in Y 2 points from G_2, G_3, 2 points from G_2, G_4 and 2 from G_3, G_4. The respective elements $y \in (X \setminus Y) \cap B_i$, $y \neq x$, must be in G_4, G_3 and G_2 respectively, which proves (b).

To prove (c) let $1, 5, 9$ be a triangle in G. In the original design P we have a block $1, 5, e, g$, say, and a block and a block $1, 9, c, h$. Then the following choices for the block containing 5 and 9 are:

$$5, 9, a, g \quad ; \quad 5, 9, a, h \quad ; \quad 5, 9, b, g \quad ; \quad 5, 9, b, h.$$

In each case we obtain a duplication $5, g$ or $9, h$, a contradiction. $\square$

Remark. We did not only prove that G is 3-regular but also that each $x \in X \setminus Y$ is in exactly four 4-blocks in $\hat{Q}$, one of which corresponds to the group x is contained in.

Lemma 1.3.2. *The three neighbours of a vertex in G are not in a common block of $\hat{Q}$.*

Proof. Suppose the opposite. Let the neighbours of 1 be $5, 9, 13$ and suppose $\{2, 5, 9, 13\}$ is a block of $\hat{Q}$. W.l.o.g. we have the following 4-blocks which contain 1:

$$1, 6, 10, 14 \quad ; \quad 1, 7, 11, 15 \quad ; \quad 1, 8, 12, 16$$

and the following 4-blocks in $\hat{Q}$ containing 2:

$$2,5,9,13 \quad ; \quad 2,6,11,16 \quad ; \quad 2,7,12,14.$$

(Note: Once $2,6,11$ is chosen, the last two blocks are forced.) The neighbours of 2 in G are therefore $8,10,15$. Since the three pairs $8,10$; $8,15$; $10,15$ are not edges in G (G is triangle-free), they must appear in 4-blocks in $\hat{Q}$. The same statement is true for the pairs $5,9$; $5,13$; $9,13$. Apart from the 4-blocks containing 1 resp. 2 (and the groups), there are 6 more 4-blocks in $\hat{Q}$, of which three contain 3 and three contain 4. Furthermore, no pair out of $5,9,13$ can be in a common 4-block with 3 or 4. Hence, the pairs $8,10$; $8,15$; $10,15$ must appear in 4-blocks of the following form:

$$3,5,\cdot,\cdot \quad ; \quad 3,\cdot,9,\cdot \quad ; \quad 3,\cdot,\cdot,13$$

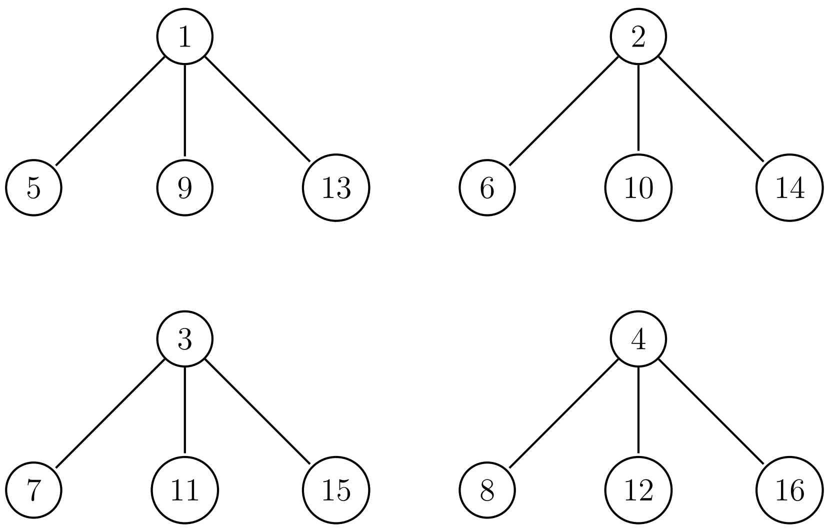
and

$$4,5,\cdot,\cdot \quad ; \quad 4,\cdot,9,\cdot \quad ; \quad 4,\cdot,\cdot,13.$$

By the pigeonhole principle, two of the pairs $8,10$; $8,15$ and $10,15$ must be in a common 4-block with one of the numbers 3 or 4 which yields a duplication. $\square$

1.4 D

Suppose we have w.l.o.g. the following setup in G:



Suppose there are a_1 4-blocks containing 1 together with one of the pairs $\{6,10\},\{6,14\},\ldots,\{12,16\}$ in $\hat{Q}$, similarly for a_i, $i=2,3,4$. By Lemma

1.3.2, 1 can appear with at most one pair out of a triple $\{6, 10, 14\}$, $\{7, 11, 15\}$, $\{8, 12, 16\}$, hence we have $a_i \leq 3$; thus

$$a_1 + a_2 + a_3 + a_4 \leq 12.$$

On the other hand, everyone of the pairs $\{5, 9\}, \ldots, \{12, 16\}$ must appear in a 4-block containing 1, 2, 3 or 4, thus

$$a_1 + a_2 + a_3 + a_4 \geq 4 \cdot 3 = 12,$$

hence $a_1 = a_2 = a_3 = a_4 = 3$. Suppose w.l.o.g. 1 is contained in the following 4-blocks:

- If $1, \underline{6, 10}, 15$ is chosen, then $1, \underline{7, 11}, 16$ and $1, \underline{8, 12}, 14$ are forced.

Finally, consider the pair $\{5, 9\}$. It is contained in a 4-block in $\hat{Q}$ and this block must contain one of $\{2, 3, 4\}$. Suppose it is

$$2, 5, 9, x \quad \text{(where } x = 15 \text{ or } x = 16\text{)}.$$

- If $x = 15$, then $2, \underline{7, 11}, \cdot$ is forced (and $7, 11$ repeated).
- If $x = 16$, then $2, \underline{8, 12}, \cdot$ is forced (and $8, 12$ repeated).

We conclude that the pair $\{5, 9\}$ is in no 4-block of $\hat{Q}$. But by Lemma 1.3.1, there must be a 4-block containing it. This final contradiction completes the proof. $\square$