BLOCK DESIGNS

We now consider matching problems again, but from a rather different point of view. Before, we were given a matching problem and we tried to solve it, or count the number of possible solutions. Here instead we will try to find matching problems that have certain special properties, which in particular make them highly symmetrical. Highly symmetrical combinatorial objects are always interesting and often have applications. In particular, the material in this chapter can be used for efficient design of experiments where one wants to test multiple interacting factors without performing more tests than necessary. It can also be used to design computer communication systems that can detect and correct some transmission errors.

Before, we had a set J of jobs and a set P of people, and for each job $j \in J$ we had a subset $C[j] \subseteq P$ of people who are qualified to do that job. For each person p we can also consider the set $Q[p]$ of jobs that they are qualified to do. This can be expressed in symbols as $Q[p] = \{j \in J \mid p \in C[j]\}$.

The framework in this chapter will be mathematically equivalent but we will follow tradition in using slightly different terminology. We will have a set B of "blocks" and a set V of "varieties". For each block $j \in B$ we have a corresponding subset $C[j] \subseteq V$. For any variety $p \in V$ we again define $Q[p] = \{j \in B \mid p \in C[j]\}$.

Definition 1. Consider numbers $v, b, r, k, \lambda > 0$ with $k < v$ and $r < b$. A *block design* with parameters (v, b, r, k, λ) is a matching problem as above, with the following properties:

(a) $|V| = v$
(b) $|B| = b$
(c) $|Q[p]| = r$ for all $p \in V$
(d) $|C[j]| = k$ for all $j \in B$
(e) $|Q[p] \cap Q[q]| = \lambda$ for all $p, q \in V$ with $p \neq q$.

In words: there are v varieties and b blocks, every variety is in precisely r blocks, every block contains precisely k varieties, every pair of distinct varieties is in precisely λ blocks.

Remark 2. As $C[j] \subseteq V$ and $|C[j]| = k$ and $|V| = v$ it is automatic that $k \leq v$. If k were equal to v then that would mean that $C[j] = V$ for all j, which is like a job allocation problem in which every person is qualified to do every job. However, we specified as part of the definition that $k < v$, so as to exclude this uninteresting case. The condition $r < b$ also has the same effect.

Example 3. Put $B = \{1, \ldots, 12\}$ and $V = \{1, \ldots, 9\}$ and

$$C[1] = \{1,2,3\} \quad C[2] = \{4,5,6\} \quad C[3] = \{7,8,9\}$$
$$C[4] = \{1,4,7\} \quad C[5] = \{1,5,9\} \quad C[6] = \{2,5,8\}$$
$$C[7] = \{3,6,9\} \quad C[8] = \{2,6,7\} \quad C[9] = \{3,4,8\}$$
$$C[10] = \{1,6,8\} \quad C[11] = \{2,4,9\} \quad C[12] = \{3,5,7\}$$

The corresponding sets $Q[p]$ are

$$Q[1] = \{1,4,5,10\} \quad Q[2] = \{1,6,8,11\} \quad Q[3] = \{1,7,9,12\}$$
$$Q[4] = \{2,4,9,11\} \quad Q[5] = \{2,5,6,12\} \quad Q[6] = \{2,7,8,10\}$$
$$Q[7] = \{3,4,8,12\} \quad Q[8] = \{3,6,9,10\} \quad Q[9] = \{3,5,7,11\}.$$

It is now visible that $|V| = 9$ and $|B| = 12$ and $|C[j]| = 3$ for all j and $|Q[p]| = 4$ for all p. We also have

$$Q[1] \cap Q[2] = \{1\} \quad Q[3] \cap Q[4] = \{9\} \quad Q[3] \cap Q[6] = \{7\} \quad Q[4] \cap Q[9] = \{11\}.$$

In fact, we have $|Q[p] \cap Q[q]| = 1$ for all $p \neq q$, as we can see by a long but easy check of cases. Thus, the above sets give a $(9, 12, 4, 3, 1)$ block design.

Proposition 4. *If there is a (v, b, r, k, λ)-block design, then $bk = vr$ and $bk(k-1) = \lambda v(v-1)$ and $r(k-1) = \lambda(v-1)$ and $\lambda < r$.*

Proof. Put

$$\begin{aligned} X &= \{(j,p) \in B \times V \mid p \in C[j]\} \\ &= \{(j,p) \in B \times V \mid v \in Q[p]\}. \end{aligned}$$

We can use the first description to find $|X|$: there are b ways to choose $j \in B$, and then $|C[j]| = k$ ways to choose $p \in C[j]$, so $|X| = bk$. Alternatively, we can use the second description. There are v ways to choose $p \in V$, and then $|Q[p]| = r$ ways to choose $j \in Q[p]$, so $|X| = vr$. By comparing these, we see that $bk = vr$. Now put

$$\begin{aligned} Y &= \{(j,p,q) \in B \times V \times V \mid p, q \in C[j],\ q \neq p\} \\ &= \{(j,p,q) \in B \times V \times V \mid q \neq p, j \in Q[p] \cap Q[q]\}. \end{aligned}$$

We can again use the first description to find $|Y|$: there are b ways to choose $j \in B$, then k ways to choose $p \in C[j]$, then $k-1$ ways to choose a different element $q \in C[j]$, giving $|Y| = bk(k-1)$. Alternatively, we can use the second description: there are v ways to choose $p \in V$, then $v-1$ ways to choose a different element $q \in V$, then $|Q[p] \cap Q[q]| = \lambda$ ways to choose $j \in Q[p] \cap Q[q]$, giving $|Y| = \lambda v(v-1)$. By comparing these, we get $bk(k-1) = \lambda v(v-1)$. We can now substitute our first equation $bk = vr$ into our second equation $bk(k-1) = \lambda v(v-1)$ and then divide by v to get $r(k-1) = \lambda(v-1)$. Rearranging this, we get $\lambda/r = (k-1)/(v-1)$. As one of our axioms we assumed that $k < v$, so $(k-1)/(v-1) < 1$, so $\lambda/r < 1$, so $\lambda < r$. □

It is useful to have a slight variant of the above proposition. This shows that axiom (c) in Definition 1 is not really needed, because it follows from the other axioms.

Proposition 5. *Suppose that we have a matching problem as before, and numbers $v, b, k, \lambda > 0$ with $k < v$. Suppose that $|V| = v$ and $|B| = b$ and $|C[j]| = k$ for all j and $|Q[p] \cap Q[q]| = \lambda$ for all $p \neq q$, so axioms (a), (b), (d) and (e) from Definition 1 are satisfied. Then the number $r = \lambda(v-1)/(k-1)$ is an integer and is the same as bk/v. Moreover, we have $|Q[p]| = r$ for all p, so axiom (c) is also satisfied, and we have a block design.*

Proof. We define X and Y as in the proof of Proposition 4. Most of that proof still works: we have $|X| = bk$ and $|Y| = bk(k-1) = \lambda v(v-1)$. However, if we use the second description of X we just get $|X| = \sum_p |Q[p]|$, and we do not yet know that the sets $Q[p]$ all have the same size. For this, we fix p and define

$$\begin{aligned} Z_p &= \{(j,q) \in B \times V \mid q \neq p \text{ and } j \in Q[p] \cap Q[q]\} \\ &= \{(j,q) \in B \times V \mid j \in Q[p] \text{ and } q \in C[j] \setminus \{p\}\} \end{aligned}$$

In the first description, there are $v-1$ ways to choose q and then λ ways to choose j, so $|Z_p| = \lambda(v-1)$. In the second description, there are $|Q[p]|$ ways to choose j. We then have $|C[j]| = k$ and $p \in C[j]$ (because $j \in Q[p]$) so $|C[j] \setminus \{p\}| = k-1$, so there are $k-1$ possible choices for q. This gives $|Z_p| = (k-1)|Q[p]|$, and we can compare our two formulae for $|Z_p|$ to get $|Q[p]| = \lambda(v-1)/(k-1)$. The right hand side is precisely the number called r in the statement of this proposition, so $|Q[p]| = r$ for all p. The left hand side here is clearly a nonnegative integer, so r is an integer. The formula $|X| = \sum_p |Q[p]|$ now becomes $|X| = vr$, so we again have $bk = vr$ and so $r = bk/v$. All claims are now clear. □

We next discuss an interesting construction that uses some number theory to produce a block design.

Definition 6. Let p be a prime number of the form $p = 4n+3$, so

$$\mathbb{Z}/p = \{0, \pm 1, \pm 2, \dots, \pm(2n+1)\}.$$

We put

$$R = \{i \in \mathbb{Z}/p \mid i = j^2 \text{ for some } j \in \mathbb{Z}/p \text{ with } j \neq 0\},$$

and call this the set of *quadratic residues*. We then have a matching problem with $B = V = \mathbb{Z}/p$ and $C[j] = j + R$.

Remark 7. We have $m \in C[j]$ iff $m \in j + R$ iff $m - j \in R$ iff $j \in m - R$, so $Q[m] = m - R$.

Example 8. Take $p = 7$, so $p = 4n + 3$ with $n = 1$ and $\mathbb{Z}/p = \{0, \pm 1, \pm 2, \pm 3\}$. We have $(\pm 1)^2 = 1$ and $(\pm 2)^2 = 4 = -3 \pmod 7$ and $(\pm 3)^2 = 9 = 2 \pmod 7$, so $R = \{1, 2, -3\}$. This gives

$$\begin{aligned} C[0] &= \{1, 2, -3\} & Q[0] &= \{-1, -2, 3\} \\ C[1] &= \{2, 3, -2\} & Q[1] &= \{0, -1, -3\} \\ C[2] &= \{3, -3, -1\} & Q[2] &= \{1, 0, -2\} \\ C[3] &= \{-3, -2, 0\} & Q[3] &= \{2, 1, -1\} \\ C[-1] &= \{0, 1, 3\} & Q[-1] &= \{-2, -3, 2\} \\ C[-2] &= \{-1, 0, 2\} & Q[-2] &= \{-3, 3, 1\} \\ C[-3] &= \{-2, -1, 1\} & Q[-3] &= \{3, 2, 0\}. \end{aligned}$$

One can check that $|Q[l] \cap Q[m]| = 1$ whenever $l \neq m$, so this is a $(7, 7, 3, 3, 1)$-block design.

Example 9. Take $p = 11$, so $p = 4n+3$ with $n = 2$ and $\mathbb{Z}/p = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5\}$. We have $(\pm 1)^2 = 1$ and $(\pm 2)^2 = 4$ and $(\pm 3)^2 = 9 = -2 \pmod{11}$ and $(\pm 4)^2 = 16 = 5 \pmod{11}$ and $(\pm 5)^2 = 25 = 3 \pmod{11}$, so

$$R = \{1, -2, 3, 4, 5\}.$$

I particular, we have $|R| = 5$ and so $|C[j]| = 5$ for all j and $|Q[m]| = 5$ for all m. We also have

$$Q[0] \cap Q[1] = (-R) \cap (1 - R) = \{-1, 2, -3, -4, -5\} \cap \{0, 3, -2, -3, -4\} = \{-3, -4\},$$

so $|Q[0] \cap Q[1]| = 2$. In fact we have $|Q[l] \cap Q[m]| = 2$ for all $l \neq m$, so we have a $(11, 11, 5, 5, 2)$-block design. This will follow from Theorem 14, which we will prove below.

Lemma 10. *For each $i \in \{1, \dots, 2n + 1\}$, precisely one of i and $-i$ is in R. Thus, $|R| = 2n + 1$.*

This result is clearly visible in the cases $p = 7$ (where $R = \{1, 2, -3\}$) and $p = 11$ (where $R = \{1, -2, 3, 4, 5\}$).

Proof. This is a standard piece of number theory. One key ingredient is a theorem saying that $(\mathbb{Z}/p) \setminus \{0\}$ is cyclic of order $4n + 2$ when considered as a group under multiplication. If g is a generator, one can deduce that g^{2n+1} must be equal to -1. We will not give further details here. □

From Lemma 10 it is clear that $|C[j]| = 2n + 1$ for all j, and that $|Q[m]| = 2n + 1$ for all m. However, it is not yet clear what we can say about $|Q[l] \cap Q[m]|$ when $l \neq m$. For this we need some more definitions.

Definition 11. We put $D = \{(u, v) \in R \times R \mid u \neq v\}$, so $|D| = |R|(|R| - 1)$. As $|R| = 2n + 1$, this gives $|D| = (4n + 2)n$. Also, for $x \in \mathbb{Z}/p$ with $x \neq 0$ we put $D_x = \{(u, v) \in D \mid u - v = x\}$. We note that D is the disjoint union of the subsets D_x, so $|D| = \sum_x |D_x|$.

Lemma 12. *$|D_x| = n$ for all x.*

Proof. Recall from Lemma 12 that either x or $-x$ is a square. Suppose for the moment that x is a square. Suppose that $(u, v) \in D_1$, so u and v are squares with $u - v = 1$. It is clear that the product of two squares is a square, so ux and vx are squares with $ux - vx = x$, so $(ux, vx) \in D_x$. Conversely, if $(u', v') \in D_x$ then $(u'/x, v'/x) \in D_1$. From this it is clear that $|D_x| = |D_1|$.

Now suppose instead that $-x$ is a square. If $(u, v) \in D_1$ then $-vx$ and $-ux$ are squares with $(-vx) - (-ux) = (u - v)x = x$, so $(-vx, -ux) \in D_x$. Conversely, if $(u', v') \in D_x$ then $(-v'/x, -u'/x) \in D_1$. From this it is again clear that $|D_x| = |D_1|$.

We now see that $|D_x| = |D_1|$ in all cases, and the number of possibilities for x is $p - 1 = 4n + 2$. The equation $|D| = \sum_x |D_x|$ now becomes $|D| = (4n+2)|D_1|$. However, we saw previously that $|D| = (4n+2)n$, so $|D_1| = n$, so $|D_x| = n$ for all x. □

Example 13. We will show how the above lemma works out in the case where $p = 11$ and so $n = 2$ and $R = \{1, -2, 3, 4, 5\}$. The table below shows the differences $u - v$ for $u, v \in R$ with $u \neq v$.

u \ v	1	-2	3	4	5
1	■	3	-2	-3	-4
-2	-3	■	-5	5	4
3	2	5	■	-1	-2
4	3	-5	1	■	-1
5	4	-4	2	1	■

We can read off the sets D_x from this. For example, to find D_5 we look in the table and see that 5 appears in the position where $u = -2$ and $v = 4$, and also in the position where $u = 3$ and $v = -2$. We therefore have $D_5 = \{(-2, 4), (3, -2)\}$. The complete list of sets D_x is as follows:

$$D_1 = \{(4,3),(5,4)\} \qquad D_{-1} = \{(3,4),(4,5)\}$$
$$D_2 = \{(3,1),(5,3)\} \qquad D_{-2} = \{(1,3),(3,5)\}$$
$$D_3 = \{(1,-2),(4,1)\} \qquad D_{-3} = \{(-2,1),(1,4)\}$$
$$D_4 = \{(-2,5),(5,1)\} \qquad D_{-4} = \{(5,-2),(1,5)\}$$
$$D_5 = \{(-2,4),(3,-2)\} \qquad D_{-5} = \{(4,-2),(-2,3)\}$$

We find that $|D_x| = 2 = n$ in every case, as predicted by the lemma.

Theorem 14. *The matching problem in Definition 6 is a $(4n+3, 4n+3, 2n+1, 2n+1, n)$-block design.*

Proof. All that is left is to show that $|Q[l] \cap Q[m]| = n$ for all $l \neq m$. Recall that $Q[l] = l - R$, so $j \in Q[l]$ iff $l - j \in R$. Thus, if $j \in Q[l] \cap Q[m]$ we see that $l - j, m - j \in R$ and of course $(l - j) - (m - j) = l - m$ so $(l - j, m - j) \in D_{l-m}$. We can therefore define a map $f\colon Q[l] \cap Q[m] \to D_{l-m}$ by $f(j) = (l - j, m - j)$. In the opposite direction, suppose that $(u, v) \in D_{l-m}$, so $u, v \in R$ with $u - v = l - m$ or equivalently $l - u = m - v$. If we put $j = l - u = m - v$ then we find that $j \in Q[l]$ (because $Q[l] = l - R$ and $j = l - u$) and also $j \in Q[m]$ (because $Q[m] = m - R$ and $j = m - v$), so $j \in Q[l] \cap Q[m]$. Using this we see that f is a bijection, so $|Q[l] \cap Q[m]| = |D_{l-m}|$. We also know from Lemma 12 that $|D_{l-m}| = n$, so $|Q[l] \cap Q[m]| = n$ as required. □

We now discuss some relationships between matrix algebra and the theory of block designs.

Definition 15. Suppose we have a matching problem as before, with $|B| = b$ and $|V| = v$, but we do not necessarily assume that this is a block design. We define a $b \times v$ matrix M by

$$M_{jp} = \begin{cases} 1 & \text{if } p \in C[j] \\ 0 & \text{if } p \notin C[j]. \end{cases}$$

Remark 16. In earlier chapters, we drew a board with the square in position (j, p) coloured white if $p \in C[j]$, and coloured black if $p \notin C[j]$. The matrix M is essentially the same thing but with 1's corresponding to white squares and 0's corresponding to black squares.

Example 17. For the block design in Example 3 we have

$$M = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Note that the transpose M^T is a $v \times b$ matrix, so the product $M^T M$ is defined and is a $v \times v$ matrix. We will need some other $v \times v$ matrices, as follows.

Definition 18. We let I denote the $v \times v$ identity matrix, so I_{pq} is 1 if $p = q$ and 0 if $p \neq q$. We also let 1_m denote the column vector of length m with all entries equal to one. We let J denote the $v \times v$ matrix with $J_{pq} = 1$ for all p and q, so all of the columns are 1_v. Note that $(J - I)_{pq}$ is 0 if $p = q$ and 1 if $p \neq q$.

Example 19. In the case $v = 4$ we have

$$I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad J = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \qquad J - I = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}.$$

In the theorem below, we will consider the matrix $rI + \lambda(J - I)$, which has diagonal entries equal to r and off-diagonal entries equal to λ. In the case $n = 4$ we get

$$rI + \lambda(J - I) = \begin{bmatrix} r & \lambda & \lambda & \lambda \\ \lambda & r & \lambda & \lambda \\ \lambda & \lambda & r & \lambda \\ \lambda & \lambda & \lambda & r \end{bmatrix}.$$

Theorem 20. *Our matching problem is a (v, b, r, k, λ)-block design iff $M.1_v = k.1_b$ and $M^T M = rI + \lambda(J - I) = (r - \lambda)I + \lambda J$.*

Proof. We will use the following standard formulae for vector and matrix algebra: the product of a matrix P and a vector u is $(Pu)_i = \sum_j P_{ij} v_j$, and the product of two matrices is $(PQ)_{ik} = \sum_j P_{ij} Q_{jk}$.

From these we get $(M.1_v)_j = \sum_p M_{jp} (1_v)_p$. Here $(1_v)_p = 1$ for all p, so we just get $(M.1_v)_j = \sum_p M_{jp}$. In this sum we get a contribution of 1 for each $p \in C[j]$, and 0 for each $p \notin C[j]$, so the sum is just equal to $|C[j]|$. Thus $M.1_v$ is just the vector $(|C[1]|, \ldots, |C[b]|)$, and this is equal to $k.1_b$ iff $|C[j]| = k$ for all j. Thus, the condition $M.1_v = k.1_b$ is equivalent to axiom (d) in Definition 1.

We now consider the product $M^T M$. We have $(M^T)_{pj} = M_{jp}$, so

$$(M^T M)_{pq} = \sum_j (M^T)_{pj} M_{jq} = \sum_j M_{jp} M_{jq}.$$

The j'th term here is 1 if both p and q lie in $C[j]$, and zero otherwise. Equivalently, the j'th term is 1 if $j \in Q[p] \cap Q[q]$, and zero otherwise. Taking the sum over j, we get $(M^T M)_{pq} = |Q[p] \cap Q[q]|$. In the case $p = q$ this just reduces to $(M^T M)_{pp} = |Q[p]|$.

We want to compare $M^T M$ with the matrix $N = rI + \lambda(J - I)$, which has $N_{pp} = r$ and $N_{pq} = \lambda$ for $p \neq q$. We find that $M^T M = N$ iff $|Q[p]| = r$ for all p, and $|Q[p] \cap Q[q]| = \lambda$ for all $p \neq q$. These are just axioms (c) and (e) in Definition 1, so the claim is now clear. □

Lemma 21. *The matrix J have eigenvalues 0 (repeated $v - 1$ times) and v (repeated once).*

Proof. Let $e_1, \dots, e_v$ be the standard basis of $\mathbb{R}^v$. Define an alternative basis $a_1, \dots, a_v$ by $a_1 = e_1 - e_2$, $a_2 = e_2 - e_3$ and so on up to $a_{v-1} = e_{v-1} - e_v$, folloewd by $a_n = e_1 + \cdots + e_v = 1_v$. For example, when $v = 4$ we have

$$a_1 = \begin{bmatrix} 1 \\ -1 \\ 0 \\ 0 \end{bmatrix} \qquad a_2 = \begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \end{bmatrix} \qquad a_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ -1 \end{bmatrix} \qquad a_4 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

It is then easy to check that $Ja_1 = \cdots = Ja_{v-1} = 0$ but $Ja_v = v\, a_v$. In other words, the vectors a_i are eigenvectors for J with eigenvalues $0, 0, \dots, 0, v$. The claim is clear from this. □

Corollary 22. *If our matching problem is a block design, then* $\det(M^T M) > 0$ *and* $M^T M$ *is invertible.*

Proof. By the theorem, $M^T M = (r - \lambda)I + \lambda J$. By Lemma 21, the matrix J has eigenvalues 0 and v, so λJ has eigenvalues 0 and λv, so $(r - \lambda)I + \lambda J$ has eigenvalues $r - \lambda$ and $r - \lambda + \lambda v = r + (v - 1)\lambda$. Moreover, the first of these is repeated $v - 1$ times, but the second occurs only once. The determinant is the product of the eigenvalues, which is $(r - \lambda)^{v-1}(r + (v - 1)\lambda)$. We also know from Proposition 4 that $\lambda < r$, so $r - \lambda > 0$, so $\det(M^T M) > 0$. It is a standard fact from linear algebra that a square matrix with nonzero determinant is invertible. □

Corollary 23. *If our matching problem is a block design, then* $b \geq v$.

Proof. Suppose instead that $b < v$; we will derive a contradiction. Let the columns of M be $u_1, \dots, u_v$, so $u_p \in \mathbb{R}^b$ for all p. As $b < v$, the length of this list is larger than the dimension of the space $\mathbb{R}^b$, so the vectors u_p must be linearly dependent, by a standard theorem of linear algebra. Thus, there is an equation $c_1 u_1 + \cdots + c_v u_v = 0$ where the coefficients c_i are not all zero. We can form a vector c with entries $(c_1, \dots, c_v)$, so $c \neq 0$. After thinking about how matrix multiplication works, we see that $Mc = 0$ and so $M^T Mc = 0$. As $M^T M$ is invertible, it follows that $c = 0$, which is a contradiction. □

Note that the conclusion $b \geq v$ is a purely combinatorial fact, so it is interesting that we have had to make a detour into linear algebra to prove it.

Definition 24. A *symmetric* design is one in which $b = v$. Corollary 23 tells us that in some sense these are maximally efficient. Recall from Proposition 4 that $bk = rv$. From this we see that a symmetric design also satisfies $k = r$.

Note that the quadratic residue design from Definition 6 and Theorem 14 is symmetric, but the design in Example 3 is not.