Designs and Codes

Lecturers: Martin Aigner and Shagnik Das
Scribe: Christopher Kusch

ABSTRACT. These are notes from the course 'Designs and Codes,' given by Martin Aigner and Shagnik Das in the Summer Semester 2017 at the Freie Universität Berlin. Nobody bears any responsibility for mistakes in the script, but Shagnik Das would be grateful to be notified of any errors found.

CHAPTER 1

Designs

1. Opening remarks

If one does not wish to get too technical,[1] one might say that a design is very regular combinatorial object. While this may be description enough for many of you, perhaps some others would prefer a more illustrative example to show that designs have been your best friends throughout your life![2] Indeed, a well-known example of a design is a d-regular graph G. Here, every edge has precisely two vertices, and every vertex is in exactly d edges, meaning all vertices are covered the same number of times — highly regular indeed.

For those who are of a more applied persuasion, further motivation can be found in chess tournaments. Given the popularity of the game,[3] it is infeasible that all pairs of contestants play against one another, so everyone can only play against some subset of the other players. Clearly it would be unfair for one player to have to play 50 games to reach the final, while his opponent might only play 12. We would prefer that everyone plays the same number of games, which naturally leads us to regular graphs.

Why, then, should we study designs, when we have known about regular graphs all our lives?[2] As mathematicians, we appreciate that chess, a zero-sum two-player game of perfect information, is trivial, and leave it for the easily-amused masses. We must turn to loftier pursuits to challenge ourselves, and hence play more serious games, like three-player chess.[4] Again, in a three-player chess tournament, one would like all players to play the same number of games. However, this is not sufficient to ensure fairness. For instance, if two players were to play all of their games together, they could collude to gain an advantage over their opponents. To prevent this from occurring, we might further require that every pair of players play the same number of games together as well.[5] This requires a stronger design, thus motivating this field of research.

Now that we are sufficiently motivated, we shall take a more mathematical tone, presenting the formal definition of a design and proving some initial results.

---

[1] Fear not, we shall get technical soon enough.

[2] As is customary, your life is deemed to have begun in Discrete Maths I, or in an equivalent course.

[3] Or sport? That is a debate for another course.

[4] At this point the lecturer displayed a three-player chessboard to the class, but the scribe did not have a camera at hand to take a picture. However, the lack of image should not be a great impediment.

[5] The eagle-eyed reader may observe that this would require all pairs of players to play with each other, the infeasibility of which served as the starting point for our discussion. However, there is no real contradiction, for three-player chess is more of a niche game than vanilla chess, attracting much smaller crowds.

2. An introduction to designs

2.1. Definitions and examples. We begin with the definition of a design, which is a collection of sets with strong regularity properties.

DEFINITION 1 (Design). Let $v \geq k \geq t \geq 0$, and let $\lambda \geq 1$ be integers. A t-(v,k,λ) *design* $\mathcal{D}$ is a collection of *blocks* (k-sets) of elements from a ground set X satisfying

(1) $|X| = v$;
(2) every $B \in \mathcal{D}$ is a subset of X of size k (that is, $B \in \binom{X}{k}$); and
(3) every t-set in X is contained in exactly λ blocks $B \in \mathcal{D}$.

The key property is item (3) above, which shows that the design $\mathcal{D}$ covers all t-sets of the ground set X exactly the same number of times, exhibiting the high-degree of regularity that makes these constructions so applicable. In some sense, t is the most significant of the parameters.

REMARK 1. Some further notational remarks.

(i) t is called the *strength* of the design, and a t-(v,k,λ) design $\mathcal{D}$ is sometimes referred to as a *t-design*.
(ii) A design may contain multiple copies of a block, and in item (3) above, we count the blocks containing a t-set with multiplicity. A *simple* design is a design without repeated blocks, and can thus be thought of as a subset of the k-sets of X: $\mathcal{D} \subseteq \binom{X}{k}$.

Let us now consider some concrete examples.

EXAMPLE 1. Some simple examples of designs:

(1) The edges of a d-regular graph G on n vertices form a 1-$(n,2,d)$ design (on the set of vertices, so $X = V(G)$ and $\mathcal{D} = E(G)$).
(2) A 0-(v,k,λ) design is simply any collection of λ k-subsets of a v-set.
(3) *Trivial designs:* $C\binom{X}{k}$, where every k-subset of X is taken C times, is, for $v = |X|$, trivially a t-(v,k,λ) design, where $\lambda = C\binom{v-t}{k-t}$.

We are interested in non-trivial designs and so we will generally assume $v > k > t$. We also assume $t \geq 2$, since it is easy to see that a 1-(v,k,λ) design exists if and only if k divides λv. A special class of designs are those with $\lambda = 1$.

DEFINITION 2 (Steiner Systems). A *Steiner system* is a t-$(v,k,1)$ design.

Steiner systems are, in some sense, the most restrictive of designs, since every t-set must be covered exactly once. Hence, once we have a block B, no other k-set intersecting B in at least t elements can be used, leaving very little space to manoeuver. Moreover, one can use Steiner systems to build t-(v,k,λ) designs by taking λ copies of the Steiner system.

REMARK 2. Some sources use the notation $S(t,k,v)$ for a Steiner system and $S_\lambda(t,k,v)$ for general designs.

We now present some examples of non-trivial designs,[6] which should interest you more than those in Example 1.

EXAMPLE 2. Some less trivial examples of designs:

(1) A famous example of a design comes from projective geometry and is called the *Fano plane*, which is a 2-$(7,3,1)$ design. As we shall see, this can be generalised to different designs.
(2) A 3-$(8,4,1)$ design can be constructed from a 3-dimensional cube, with X being the set of vertices and the blocks of $\mathcal{D}$ consisting of the vertex sets given by the 6 faces of the cube, the 6 pairs of antipodal edges and 2 independent sets of size 4.
(3) A 3-$(10,4,1)$ design: Let $X = E(K_5)$ and $\mathcal{D}$ consist of all copies of C_4, $K_{1,4}$, and $K_3 + K_2$ (triangles with a disjoint edge).

This shows us that interesting designs can exist, which leads us to a treasure trove of questions — how many designs are there? What structure does the typical design have? What does the set of t-(v,k,λ) designs look like? However, the history of mathematics is littered with cautionary tales[7] of what happens when you leap before you look, and so there is one fundamental question we must address before we can entertain thoughts of any others.

QUESTION 1. For what sets of parameters does a t-(v,k,λ) design exist? Can it be simple? What about in the asymptotic setting, where t and k are fixed, $\lambda \geq \lambda_0(t,k)$ and $v \geq v_0(t,k,\lambda)$?

For this first part of the course, we shall try to give some partial answers to this question. This will consist both of positive results — where we construct infinite families of non-trivial designs (as opposed to the seemingly esoteric constructions of Example 2) — and negative results — where we prove that no such design can exist.

2.2. Arithmetic conditions. Recall that the handshake lemma implies that if G is d-regular graph on n vertices, then nd must be even. This gives a divisibility condition showing that even in our simplest setting, we do not always have 1-$(n,2,d)$ designs. We shall now extend this result to cover general designs.

LEMMA 1. *Let $\mathcal{D}$ be a t-(v,k,λ) design, and fix some $0 \leq i \leq t$. Then every i-set $I \in \binom{X}{i}$ is contained in exactly*

$$\lambda_i := \frac{\lambda\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$$

blocks. In particular, $b := |\mathcal{D}| = \lambda_0 = \frac{\lambda\binom{v}{t}}{\binom{k}{t}}$ and $r := \lambda_1 = \frac{\lambda\binom{v-1}{t-1}}{\binom{k-1}{t-1}}$.[8] *Furthermore, a t-(v,k,λ) design is also an i-(v,k,λ_i) design for every $0 \leq i \leq t$.*

[6] Sketch your own illustrations of the examples in the margins to make up for the missing blackboard images.

[7] One specific example may have been cited in lecture, but any such reference was redacted during the preparation of these publically-available notes.

[8] This parameter r, representing the number of blocks containing any fixed element, is called the *replication number*.

PROOF. Fix $I \in \binom{X}{i}$. We are going to double-count pairs (T, B), where $I \subseteq T \subseteq B$, $T \in \binom{X}{t}$ and $B \in \mathcal{D}$.

On the one hand, there are $\binom{v-i}{t-i}$ t-sets T containing I. Since $\mathcal{D}$ is a t-(v, k, λ) design, there are λ blocks containing T. Hence the total number of pairs is $\lambda\binom{v-i}{t-i}$

On the other hand, for each block B containing I, there are $\binom{k-i}{t-i}$ choices for T such that $I \subseteq T \subseteq B$. Hence, if there are λ_I blocks containing I, the total number of pairs is $\lambda_I\binom{k-i}{t-i}$. This gives $\lambda_I = \frac{\lambda\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$, which depends only on $|I| = i$ and is otherwise independent of I. □

Note that the proof is essentially the same argument used to prove the handshake lemma. Since the values λ_i must all be integers, this immediately gives the following necessary corollary.

COROLLARY 1 (Arithmetic Conditions). *If a t-(v, k, λ) design exists, then for all $0 \leq i \leq t$,*

$$\lambda\binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}}$$

Corollary 1 gives a set of necessary conditions that can be used to quickly rule out the existence of t-(v, k, λ) designs for certain values of the parameters.

EXAMPLE 3. Steiner Triple Systems, i.e., 2-$(v, 3, 1)$ designs. Corollary 1 gives

($i = 0$) $\binom{v}{2} \equiv 0 \pmod 3$, and
($i = 1$) $v - 1 \equiv 0 \pmod 2$.

We can combine these two conditions to get $v \equiv 1 \text{ or } 3 \pmod 6$.

In the case of Steiner Triple Systems, it turns out that the arithmetic conditions of Corollary 1 are not just necessary but sufficient as well; that is, whenever $v \equiv 1 \text{ or } 3 \pmod 6$, there is a 2-$(v, 3, 1)$ design. Do these arithmetic conditions continue to prove sufficient for larger choices of parameters?

2.3. Size conditions on the ground set. The answer to the above question is, perhaps unsurprisingly[9], no. As we shall soon show, if the ground set X is too small, one cannot hope to have any non-trivial designs.

PROPOSITION 1. *Let $\mathcal{D}$ be a t-(v, k, λ) design, and suppose $0 \leq j \leq t$. Then any $J \in \binom{X}{j}$ is disjoint from the same number b_j of blocks, and $b_j = \frac{\lambda\binom{v-j}{k}}{\binom{v-t}{k-t}}$.*

Note that $j \leq t$ is important here, as a design of strength t only provides control over subsets of size up to t. In fact, the conclusion does not hold for larger values of j.

[9]Having earlier stated that we would devote this first part of the course to the existence of designs with certain parameters, it is unlikely that we would immediately find some simple necessary and sufficient conditions.

PROOF. Fix an arbitrary $J \in \binom{X}{j}$ and count the number of blocks that intersect J. By the inclusion-exclusion formula, this number is equal to

$$\sum_{x\in J}|\{B\in\mathcal{D}: x\in B\}|-\sum_{\{x,y\}\subseteq J}|\{B\in\mathcal{D}:\{x,y\}\subseteq B\}|+\sum_{\{x,y,z\}\subseteq J}|\{B\in\mathcal{D}:\{x,y,z\}\subseteq B\}|-\dots$$

or, more succinctly,

$$\sum_{\emptyset\neq I\subseteq J}(-1)^{|I|-1}\,|\{B\in\mathcal{D}: I\subseteq B\}| = \sum_{i=1}^{j}(-1)^{i-1}\binom{j}{i}\lambda_i$$

and is thus independent of J (note that we have used Lemma 1 in above equality). The number b_j is therefore well defined.

To find what b_j is, we double count pairs (J,B), where $J\in\binom{X}{j}$, $B\in\mathcal{D}$ and $B\cap J=\emptyset$. There are $\binom{v}{j}$ choices for J, each of which is disjoint from b_j blocks, giving $b_j\binom{v}{j}$ such pairs. On the other hand, there are b blocks, each disjoint from $\binom{v-k}{j}$ j-sets.

Hence $b_j\binom{v}{j}=b\binom{v-k}{j}$ and so $b_j=\frac{b\binom{v-k}{j}}{\binom{v}{j}}=\frac{\lambda\binom{v}{t}\binom{v-k}{j}}{\binom{k}{t}\binom{v}{j}}=\frac{\lambda\binom{v-j}{k}}{\binom{v-t}{k-t}}$, as claimed. □

COROLLARY 2. *A t-(v,k,λ) design $\mathcal{D}$ must be trivial if $v\le k+t$. In particular, $\mathcal{D}=C\binom{X}{k}$, where $C=\frac{\lambda}{\binom{v-t}{k-t}}$.*

PROOF. Set $j=v-k\le t$ and fix a j-set $J\in\binom{X}{j}$. By Proposition 1, there are b_j blocks disjoint from J. However, since $|X\setminus J|=v-j=k$, there is a unique possible block $B=X\setminus J$ that is disjoint from J, and so it must appear b_j times in $\mathcal{D}$. Since this is true for every j-set, all of the complements, namely $\binom{X}{k}$, appear b_j times as blocks. Set $C=b_j$. □

As mentioned earlier, Steiner systems, where $\lambda=1$, are more restricted designs, and the following result shows that much larger ground sets are needed to support them.

PROPOSITION 2 (Tits, 1964). *In any non-trivial Steiner system (a t-$(v,k,1)$ design) we must have $v\ge(t+1)(k-t+1)$.*

PROOF. Homework. □

EXAMPLE 4. Imagine, if you can, that you have a friend, and that one day your friend bursts into your room, panting, "[Your name], I need a 10-$(72,16,1)$ design." After catching her or his breath, your friend needlessly[10] adds, "It is a matter of life and death."

Eager to help, you try to determine if a design with these parameters exists. Eleven quick calculations[11] show that the numbers λ_i, $0\le i\le 10$, are all integers, and so Corollary 1 does not rule anything out.

Checking all possible collections of 16-subsets of a 72-element ground set to see if they give the required design seems like a lot of work.[12] Fortunately, we may also apply Proposition 2, which shows we need $v\ge(t+1)(k-t+1)=77$. Hence, there is no 10-$(72,16,1)$ design.

[10] After all, you already know of the many vital applications of designs.

[11] If we are going to pretend you have a friend, we might as well pretend you can compute speedily.

[12] More work, perhaps, than your fictional friend deserves.

We close with another consequence of Proposition 1, showing how we can construct new designs from old ones.

COROLLARY 3. *If $\mathcal{D}$ is a t-(v,k,λ) design with $v \geq k+t$, then $\overline{\mathcal{D}} = \{X \setminus B : B \in \mathcal{D}\}$ is also a t-design.*

Note that when we take the complements in $\overline{\mathcal{D}}$, we take them with the same multiplicity as $\mathcal{D}$. In particular, $\overline{\mathcal{D}}$ is simple if and only if $\mathcal{D}$ is.

PROOF. A t-set T is covered by the complementary block $X \setminus B \in \overline{\mathcal{D}}$ if and only if it was disjoint from the block $B \in \mathcal{D}$. By Proposition 1, each t-set is therefore covered by exactly b_t blocks in $\overline{\mathcal{D}}$, showing that $\mathcal{D}$ is indeed a t-design. □

3. Designs of strength two

3.1. A brief origin story. Historically speaking, much of the early interest in designs came from statistics, with an eye towards creating fair but efficient experiments. Of greatest importance was, by far, the case $t = 2$, which we shall now study in greater detail.

REMARK 3. In this setting, non-trivial 2-designs are often called *Balanced Incomplete Block Designs (BIBD)*. Here the 'incomplete' refers to the fact that $k < v$, so the blocks do not contain everything, while 'balanced' corresponds to λ, the fact that every pair is covered equally.

We of course have the arithmetic conditions from Corollary 1, which in the case $t = 2$ result in the conditions

$(i = 0)$ $b = \lambda_0 = \frac{\lambda v(v-1)}{k(k-1)}$ and

$(i = 1)$ $r = \lambda_1 = \frac{\lambda(v-1)}{k-1}$,

which are equivalent to $r = \frac{\lambda(v-1)}{k-1}$ and $rv = bk$. We shall hereafter assume that these equalities hold, so that the necessary arithmetic conditions are satisfied, and see what other conditions, if any, might be necessary.

3.2. Fisher's inequality. The first result in this direction is Fisher's inequality.[13]

PROPOSITION 3 (Fisher's Inequality). *In a non-trivial 2-(v,k,λ) design, we must have $b \geq v$.*

[13]The simple name of this inequality hides a somewhat complicated provenance — suffice it to say that this inequality has been generalised and reproved by several very clever mathematicians since it first appeared. We did not have time to get into this in lecture, so we settled for two observations instead.

(1) Sir Ronald Fisher, a British scientist, is regarded both as the greatest biologist since Darwin and the father of modern statistics and experimental design, so he was likely a busy man. He was possibly, though improbably, the person after whom both of Real Madrid's Ronaldo's were named.

(2) If you have previously taken our Extremal Combinatorics course, you will recall a Fisher's Inequality from there as well, although it seemed to state the opposite inequality. That is, in some sense that will become clearer later, a dual version of our proposition here, and you should not get confused between the two.

Fisher's Inequality plays an important role in our study for at least a couple of reasons. The first is that it provides a new necessary condition, showing that the arithmetic conditions are not sufficient by themselves. Indeed, Lemma 1 merely gives $b \geq \frac{\lambda v(v-1)}{k(k-1)}$ which could, for small λ and large k, allow for $b < v$. Secondly, and perhaps more significantly, the proof of Fisher's Inequality introduces the use of linear algebraic arguments. For that, we make the following definition.

DEFINITION 3 (Incidence matrix). Given a design $\mathcal{D}$, its *incidence matrix* A is a $v \times b$ $\{0,1\}$-matrix whose rows are indexed by X and columns by blocks in $\mathcal{D}$, with

$$A_{x,B} = \begin{cases} 0 & \text{if } x \notin B \\ 1 & \text{if } x \in B \end{cases}.$$

We now demonstrate the utility of the incidence matrix by proving Fisher's Inequality.

PROOF OF PROPOSITION 3. Let $\mathcal{D}$ be a 2-(v,k,λ) design, and let A be the corresponding incidence matrix. Observe that $\text{rk}(AA^T) \leq \text{rk}(A) \leq b$, since A is a $v \times b$ matrix. Moreover, if $\mathcal{D}$ is non-trivial, then $v > k$, which implies $r > \lambda$.

Note that AA^T is a $v \times v$ matrix whose rows and columns are indexed by X. Given $x, y \in X$, we have $(AA^T)_{x,y} = \sum_{B \in \mathcal{D}} A_{x,B}A_{y,B} = |\{B \in \mathcal{D} : x, y \in B\}|$. This number is equal to λ if $x \neq y$ and r if $x = y$. Hence, performing some elementary row and column operations, we find

$$\begin{aligned}
\det(AA^T) &= \det \begin{pmatrix} r & \lambda & \lambda & \dots & \lambda \\ \lambda & r & \lambda & \dots & \lambda \\ \lambda & \lambda & r & \dots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \dots & r \end{pmatrix} = \det \begin{pmatrix} r & \lambda - r & \lambda - r & \dots & \lambda - r \\ \lambda & r - \lambda & 0 & \dots & 0 \\ \lambda & 0 & r - \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & \dots & r - \lambda \end{pmatrix} \\
&= \det \begin{pmatrix} r + (v-1)\lambda & 0 & 0 & \dots & 0 \\ \lambda & r - \lambda & 0 & \dots & 0 \\ \lambda & 0 & r - \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & \dots & r - \lambda \end{pmatrix} \\
&= (r + (v-1)\lambda)(r - \lambda)^{v-1} > 0.
\end{aligned}$$

Hence AA^T is of full rank, and so $v = \text{rk}(AA^T) \leq b$. □

Fisher's Inequality gives a lower bound on the size of a non-trivial 2-design. Since in applications to experimental design, larger designs are more expensive, special attention was paid to the smallest possible designs, which are those attaining equality in Fisher's Inequality.

DEFINITION 4 (Symmetric Designs). A 2-(v,k,λ) design is *symmetric* if $b = v$, i.e. we have equality in Proposition 3.

REMARK 4. Some initial remarks on symmetric designs:

(1) We have already encountered a symmetric design, namely the Fano plane of Example 2. The Fano plane is a 2-$(7, 3, 1)$ design with $b = v = 7$.
(2) The nomenclature is a little unfortunate; the incidence matrix of a symmetric design is in general *not* a symmetric matrix.[14]

We shall now investigate necessary conditions for the existence of symmetric designs. Our first, a fact that falls out of the proof of Proposition 3, is a rather curious algebraic/number theoretic requirement.

COROLLARY 4. *If v is even and a symmetric 2-(v, k, λ) design exists, then $k - \lambda$ must be a square.*

PROOF. Let $\mathcal{D}$ be such a design, with $b = v$. Since $rv = bk$, we also have $r = k$. Letting A be the incidence matrix of $\mathcal{D}$, we found in the proof of Proposition 3 that $\det(AA^T) = (r + (v-1)\lambda)(r-\lambda)^{r-1}$. Since $r = \frac{\lambda(v-1)}{k-1}$, we have $\lambda(v-1) = r(k-1)$, and so

$$\det(AA^T) = (r + r(k-1))(r-\lambda)^{v-1} = rk(r-\lambda)^{v-1} = k^2(k-\lambda)^{v-1}.$$

But, since A is a square matrix (as $b = v$), $\det(AA^T) = \det(A)^2$, and so the right-hand side must be a square. Hence $(k-\lambda)^{v-1}$ should be a square, which, by virtue of $v-1$ being odd, implies that $k - \lambda$ is a square. □

3.3. Dual designs. We shall now justify the name "symmetric designs" by showing these designs have an extra level of regularity: every pair of *blocks* have the same number of elements in common. This allows us to exchange the roles of elements and blocks, as we shall shortly describe in greater detail.

With regards to the notation in what follows: we denote by I the identity matrix (i.e. 1s on the diagonal, and 0s elsewhere), and by J we denote the all-one matrix (i.e. every entry is 1). We shall omit the dimensions of these square matrices, which should be clear from context. With this notation, for instance, our observation in the proof of Proposition 3 about the entries of AA^T can be summarised by $AA^T = (r-\lambda)I + \lambda J$.[15]

PROPOSITION 4. *Let $\mathcal{D}$ be a symmetric 2-(v, k, λ) design. Then, for $B \neq B' \in \mathcal{D}$,*

$$\left|B \cap B'\right| = \lambda.$$

PROOF. Let A be the incidence matrix. Since every element is in r blocks, and $r = k$, we have

$$AJ = rJ = kJ.$$

On the other hand, since every block has k elements, we also have

$$JA = kJ.$$

[14] This may seem cruelly and needlessly confusing, but the next subsection will reveal the reasoning behind this name.

[15] For symmetric designs, we will often substitute $r = k$ in this equality.

As we showed when proving Proposition 3, A is invertible, and so $J = A^{-1}(kJ)$, i.e., $A^{-1}J = k^{-1}J$, and similarly $JA^{-1} = k^{-1}J$. Now observe that A^TA is a $b \times b$ matrix with

$$(A^TA)_{B,B'} = \sum_{x \in X} A_{x,B}A_{x,B'} = \left|B \cap B'\right|$$

However,

$$\begin{aligned} A^TA &= (A^{-1}A)A^TA = A^{-1}(AA^T)A = A^{-1}(\lambda J + (k-\lambda)I)A \\ &= (\lambda A^{-1}J + (k-\lambda)A^{-1}I)A = (\lambda k^{-1}J + (k-\lambda)A^{-1})A \\ &= \lambda J + (k-\lambda)I. \end{aligned}$$

All off-diagonal entries are thus equal to λ, and so $|B \cap B'| = \lambda$ for every $B \neq B' \in \mathcal{D}$. □

COROLLARY 5 (Dual Designs). *If $\mathcal{D}$ is a symmetric 2-(v,k,λ) design with incidence matrix A, then A^T is also the incidence matrix of a symmetric 2-(v,k,λ) design, called the* dual design $\mathcal{D}^T$.

PROOF. The dual design $\mathcal{D}^T$ will have as its ground set the blocks of the original design; that is, $X(\mathcal{D}^T) = \mathcal{D}$. In particular, $v(\mathcal{D}^T) = |\mathcal{D}| = b(\mathcal{D}) = v$.

The blocks of $\mathcal{D}^T$ will thus be sets of blocks from $\mathcal{D}$, which we define as follows. For each $x \in X(\mathcal{D})$, define a block $B_x = \{B \in \mathcal{D} : x \in B\}$. Since each point is in $r = k$ blocks, we have $k(\mathcal{D}^T) = |B_x| = k$ for every $x \in X(\mathcal{D})$.

For any two distinct blocks $B \neq B' \in \mathcal{D}$ from the original design, we have

$$\{B, B'\} \subseteq B_x \Leftrightarrow x \in B \cap B'.$$

Hence, the pair $\{B, B'\}$ is covered by $|B \cap B'| = \lambda$ dual blocks $B_x \in \mathcal{D}^T$, and so $\mathcal{D}'$ is indeed a 2-(v,k,λ) design.

Finally, let A' be the incidence matrix of $\mathcal{D}^T$. We have

$$A'_{B,B_x} = 1 \Leftrightarrow B \in B_x \Leftrightarrow x \in B \Leftrightarrow A_{x,B} = 1,$$

and so, identifying the indices x and B_x, we have $A' = A^T$. □

We finish with an explicit example of a dual design.

EXAMPLE 5. Let $X = [4]$ and $\mathcal{D} = \{A, B, C, D\}$, where $A = \{1,2,3\}$, $B = \{2,3,4\}$, $C = \{1,3,4\}$ and $D = \{1,2,4\}$. This is a 2-$(4,3,2)$ design.

For the dual $\mathcal{D}^T$, we have $X = \mathcal{D}$ and $\mathcal{D}^T = \{B_1, B_2, B_3, B_4\}$, where $B_1 = \{A, C, D\}$, $B_2 = \{A, B, D\}$, $B_3 = \{A, B, C\}$ and $B_4 = \{B, C, D\}$. This is also a 2-$(4,3,2)$ design.

REMARK 5. In this case, $\mathcal{D} \cong \mathcal{D}^T$, since both designs are trivial designs $\binom{X}{3}$. A design that is isomorphic[16] to its dual is called *self-dual*, but not all symmetric designs are self-dual. For instance, there are non-self-dual 2-$(91,10,1)$ designs. These are the smallest non-self-dual designs with $\lambda = 1$, but there may be smaller such designs for larger values of λ.

[16] Two designs are *isomorphic* if there is a bijection between their ground sets that preserves blocks; that is, one design can be obtained from the other by relabelling the elements appropriately.

4. Projective Planes

We now continue our search for symmetric 2-(v, k, λ) designs, which have $b = v$, the minimum possible number of blocks. In this section we focus on the most restrictive, and therefore perhaps most interesting case: Steiner systems, where $\lambda = 1$. Do symmetric Steiner systems exist, and if so, how can we construct them?

Observe that in this setting we have $v = b = \frac{v(v-1)}{k(k-1)}$, which gives

$$v = k(k-1) + 1 = (k-1)^2 + (k-1) + 1 =: n^2 + n + 1,$$

where we set $n := k - 1$. As a result, $r = k = n + 1$.

4.1. A geometric attempt. What properties does a symmetric 2-$(v, k, 1)$ design have? For starters, every pair of points must determine a unique block. This may sound terribly familiar — indeed, replace 'block' with 'line' and a casual eavesdropper could be forgiven for assuming that we were geometers. Can our geometric colleagues inspire the creation of suitable designs?

Unfortunately, Euclidean geometry falls short of the task. A natural attempt would be to take v points in $\mathbb{R}^2$, and take the blocks to be all the lines defined by these points. However, we run into a problem: these lines will not be uniform.

THEOREM 1 (Sylvester–Gallai, 1944). *For any set of N points in $\mathbb{R}^2$ that are not all collinear, there is a line containing exactly two of the points.*

Those of you well-versed in mathematical history[17] may be surprised to see a Sylvester–Gallai theorem: how could they have been coauthors, when Sylvester passed away fifteen years prior to Gallai's birth? Indeed, this was a question posed by Sylvester in 1893[18] and, in 1944, Tibor Gallai was one of the first[19] to prove it.

SKETCH OF KELLY'S PROOF. Supposing the points do not all lie on a common line, choose the pair (p_0, ℓ_0) of a point and a line at minimum positive distance from one another. Bisecting ℓ_0 with a perpendicular from p_0, and assuming that ℓ_0 contains at least three points, we can choose a half-line of ℓ_0 with at least two points. Let p_1 and p_2 be the closest and second-closest points to p_0 on this half-line. It then follows that the distance from p_1 to the line determined by p_0 and p_2 is less than the distance between p_0 and ℓ_0, contradicting our choice of (p_0, ℓ_0). □

As a result, the only designs we would get from such a configuration of points and lines are trivial ones, i.e., $k = v$ or $\mathcal{D} = \binom{[3]}{2}$. Fortunately, there are non-Euclidean geometries, and rather than abandon such a promising idea, we shall instead seek a geometry better suited to our purposes.

[17] Which, I hope, is all of you.

[18] The question was posed under the title, "Mathematical question 11851": Sylvester appears to have been a very curious man. He was also the one to first call graphs "graphs", and so we owe him a great deal.

[19] In 1893 Woodall gave a proof later found to be incorrect. Melchior (correctly) proved a stronger result in 1941, which Erdős overlooked when he re-asked Sylvester's question in 1943, prompting Gallai's solution.

4.2. An axiomatic approach. There is no shortage of geometries out there, and one could go through them one by one to see if any fit the bill, but this would probably take more time than we have. Instead, we make like pure mathematicians and provide a list of axioms that will do the job. As combinatorialists, we shall assume that everything below is finite, without explicitly saying so.

DEFINITION 5 (Projective Plane). A *projective plane* is a pair $(P, \mathcal{L})$, where P is a set of *points* and $\mathcal{L}$ is a set of *lines*, $\mathcal{L} \subseteq 2^P$, each line being a set of points, such that

(1) If $p \neq q \in P$, then there is a unique line containing both p and q.
(2) If $L \neq L' \in \mathcal{L}$, there is a unique point $p \in L \cap L'$, i.e., $|L \cap L'| = 1$.
(3) There are four points, no three of which lie on the same line.

REMARK 6. While the points and lines are defined as abstract sets, they bear more than a striking resemblance to the points and lines we are used to seeing in geometry. In particular:

(i) Condition (2) implies that there are no parallel lines: any two lines intersect.
(ii) Condition (3) prevents degenerate cases, e.g., having all points on the only line, or all lines through the only point.

Our next result shows that these axioms capture exactly the properties we need, as they are in one-to-one correspondence with the symmetric 2-$(v, k, 1)$ designs we are seeking.

PROPOSITION 5. *Projective planes are precisely the non-trivial symmetric* 2-$(v, k, 1)$ *designs.*

PROOF. We first show that every non-trivial symmetric 2-$(v, k, 1)$ design defines a projective plane. Let $\mathcal{D}$ be such a design, and take $P = X$ and $\mathcal{L} = \mathcal{D}$. Then (1) is satisfied by the definition of a 2-$(v, k, 1)$ design, while (2) follows from Proposition 4. To show that (3) is satisfied, let B and B' be two distinct blocks. There is a unique $x \in B \cap B'$; let $u, v \in B \setminus \{x\}$ and $y, z \in B' \setminus \{x\}$.[20] If there were some $B'' \in \mathcal{D}$ such that $|B'' \cap \{u, v, y, z\}| \geq 3$, then by the pigeonhole principle, either $|B'' \cap B| \geq 2$ or $|B'' \cap B'| \geq 2$, contradicting (2). Hence $(P, \mathcal{L})$ is indeed a projective plane.

The reverse direction, that every projective plane corresponds to a non-trivial symmetric 2-$(v, k, 1)$ design, is left as a homework exercise. □

DEFINITION 6. The parameter $n = k - 1$ is called the *order* of the projective plane.[21]

4.3. Affine planes. It just so happens that there is a "two-for-one" deal with projective planes: once we have a projective plane, we get a related design called an *affine plane* for free. We now briefly explain the connection between the two.

[20] Note that by non-triviality we have $|B| = |B'| = k > t = 2$.

[21] The axioms of Definition 5 make no reference to the parameter k, but Proposition 5 shows that they are equivalent to 2-$(v, k, 1)$ designs, so the parameter k is well-defined. Indeed, it is part of the aforementioned homework exercise to prove that all lines in a projective plane have the same cardinality.

Building affine planes from projective planes. Suppose we have a projective plane $(P, \mathcal{L})$. Fix a line $L_0 \in \mathcal{L}$, and delete the line from $\mathcal{L}$ and its points from P. This gives a new pair $(P', \mathcal{L}')$, where $P' = P \setminus L_0$ and $\mathcal{L}' = (\mathcal{L} \setminus \{L_0\})|_{P'}$. We then have the following properties:

(1) Every pair in P' is still contained in a unique line in $\mathcal{L}'$.
(2) Every line in $\mathcal{L}'$ has size n, since it loses its one point of intersection with L_0.

This implies that $(P', \mathcal{L}')$ corresponds to a 2-$(n^2, n, 1)$ design, and this design is called an *affine plane of order* n.

Recovering projective planes from affine planes. The above process is invertible, which allows us to recover the projective plane. Indeed, $\mathcal{L}'$ can be partitioned into $n+1$ *parallel classes*: for every $p \in L_0$, take $\{L \in \mathcal{L} \setminus \{L_0\} : p \in L\}$. In the affine plane, lines in the same parallel class are disjoint, while those in different classes intersect uniquely.

Add a new point for each parallel class and include it in every line of the class. This ensures that every pair of lines now has a unique point of intersection. Finally, add a new *line at infinity* containing the new points. This gives the original projective plane back, with L_0 being the line at infinity, and its points being the new points that were added to each parallel class.

Of course, we assumed above that our affine plane came from a projective plane to begin with. However, one can define affine planes through an independent set of axioms, or, equivalently,[22] as 2-$(n^2, n, 1)$ designs. Any such design must admit a partition into parallel classes as above, which then allows for the introduction of a line at infinity, thereby extending the design to a projective plane.

4.4. Constructing projective planes. The observant reader will not have been hoodwinked by the mathemagical sleight of hand we have just performed: we introduced projective planes, and showed that they were equivalent to non-trivial symmetric 2-$(v, k, 1)$ designs. This does not solve our existential question, but merely translates it into another language: do projective planes exist?

As it turns out, linear algebra giveth and linear algebra taketh away! While we have earlier used it to rule out certain designs, we shall now use linear algebra to construct projective planes.

CLAIM 1. *Let $\mathbb{F}$ be a finite field, and let $V = \mathbb{F}^3$ be the three-dimensional vector space over $\mathbb{F}$. If $P = \{$one-dimensional subspaces of $V\}$ and $\mathcal{L} = \{$two-dimensional subspaces of $V\}$, then $(P, \mathcal{L})$ is a projective plane.*

PROOF. We verify the axioms of Definition 5 one by one. For (1), we observe that two distinct one-dimensional subspaces of V span a unique two-dimensional subspace. For (2), note that any two distinct two-dimensional subspaces in a three-dimensional subspace must intersect in a one-dimensional subspace. Finally, for (3), we may consider the one-dimensional subspaces

[22] This equivalence is not immediate, but is the analogue of Proposition 5 for affine planes.

spanned by the vectors

$$\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \text{ and } \begin{pmatrix}1\\1\\1\end{pmatrix}.$$

Any three of these vectors are linearly independent, and hence there is no two-dimensional subspace containing three of the one-dimensional subspaces. □

This shows that whenever we have a finite field, we have a corresponding projective plane and hence, by Proposition 5, a non-trivial symmetric 2-$(v, k, 1)$ design, as we desired.

REMARK 7. Some quick remarks regarding the construction.

(i) It is straightforward to check that the order of the projective plane is equal to the order of the finite field.
(ii) Should one so wish, these projective planes can be defined using projective coordinates.
(iii) As we have seen, we can derive an affine plane from a projective plane by removing a line. However, these affine planes can be constructed more directly. Indeed, let $P = \mathbb{F}^2$, and take $\mathcal{L}$ to be the set of all affine lines; that is,

$$\mathcal{L} = \left\{ \{\vec{a} + \gamma\vec{b} : \gamma \in \mathbb{F}\} : \vec{a} \in \mathbb{F}^2, \vec{b} \in \mathbb{F}^2 \setminus \{\vec{0}\} \right\}.$$

In fact, we have known of this construction from the start of the course, even if we didn't know we knew it.

EXAMPLE 6. The projective plane over $\mathbb{F}_2$ is simply the Fano plane of Example 2, and the above construction provides the long-awaited generalisation. For another example, the affine plane over $\mathbb{F}_3$ is a 2-$(9, 3, 1)$ design, and it is a colourful exercise to draw it.

We close with some important open problems regarding projective planes.

QUESTION 2 (Existence). Our above construction relied on the existence of a finite field, and finite fields are known to exist if and only if the order is a prime power. Does this also hold for projective planes? That is, do projective planes of order n exist if and only if n is a prime power?

QUESTION 3 (Uniqueness). The above construction is known as the *Desarguesian projective plane*. For non-prime prime power orders, other non-Desarguesian constructions are known, but no such construction is known for prime orders. If p is a prime, must a projective plane of order p be Desarguesian?

5. The Bruck–Ryser–Chowla Theorem

To answer Question 2, we shall need to develop some stronger necessary conditions for the existence of designs, as our previous conditions are not sophisticated enough to detect any differences between prime powers and other numbers. The stage is thus set for the

Bruck–Ryser–Chowla Theorem,[23] which remains to this date one of the most powerful general non-existence results we have for combinatorial designs.

THEOREM 2 (Bruck–Ryser–Chowla, 1950). *Let $\mathcal{D}$ be a non-trivial symmetric 2-(v,k,λ) design.*

(1) If v is even, then $k-\lambda$ is a square.

(2) If v is odd, then the equation

$$z^2 = (k-\lambda)y^2 + (-1)^{\frac{v-1}{2}}\lambda x^2$$

has a solution $(x,y,z) \in \mathbb{Z}^3 \setminus \{(0,0,0)\}$.

5.1. Application to projective planes. Before we proceed with the proof of the Bruck–Ryser–Chowla Theorem, we shall first see what it implies for projective planes ($\lambda = 1$). This is given in the following corollary.

COROLLARY 6. *For $n \equiv 1,2 \pmod 4$, a projective plane of order n can only exist if n is the sum of two squares.*

This may seem like a mystical condition — what do sums of squares have to do with designs? — but it is a very useful condition, thanks to the following well-known fact.[24]

FACT 1. *A natural number n is the sum of two squares if and only if every prime factor p of n with $p \equiv 3 \pmod 4$ appears with even multiplicity.*

As a consequence, we can immediately rule out the existence of projective planes of order $n \in \{6,14,21,22,30,33,\ldots\}$. To date, there has only been *one* order not covered by Corollary 6 that has since been ruled out! In 1989, Lam, Thiel and Swiercz proved the nonexistence of a projective plane of order 10, making heavy use of computational power in the process.[25] The smallest open case is thus $n = 12$.

PROOF OF COROLLARY 6. For a projective plane of order n we have $\lambda = 1$, $k-\lambda = n$, and $v = n^2+n+1$, which is always odd. Hence condition (2) of Theorem 2 applies, requiring the quadratic equation

$$z^2 = ny^2 + (-1)^{\frac{n(n+1)}{2}}x^2$$

to have a non-trivial solution.

If $n \equiv 0,3 \pmod 4$, this becomes

$$z^2 = ny^2 + x^2,$$

[23] This mathematical theorem is a little oddly named, in that its authors are not listed in alphabetical order, the reason being that the theorem is the combination of results from two different papers. In 1949, Bruck and Ryser proved the theorem in the case $\lambda = 1$, and a year Ryser and Chowla extended this to general designs. For all his efforts, Ryser's name unfortunately ended up in the middle, typically the least important position in fields where the order of the authors' names carries any significance.

[24] This fact appears to date back to Girard in 1625 and Fermat in 1640, which is hopefully long enough ago for it to have established itself as common knowledge.

[25] Lam, who was Ryser's doctoral student, notes that Ryser had advised him not to work on this problem, for fear that it would be too difficult.

which admits the non-trivial solutions $(x, 0, \pm x)$. Hence in this case Theorem 2 does not give us anything interesting.

However, if $n \equiv 1, 2 \pmod 4$, then the equation is

$$z^2 = ny^2 - x^2,$$

or, equivalent $ny^2 = x^2 + z^2$. Thus ny^2 is a sum of two squares, which by Fact 1 implies every prime factor p of ny^2 with $p \equiv 3 \pmod 4$ appears with even multiplicity. This in turn implies that every prime factor p of n with $p \equiv 3 \pmod 4$ appears with even multiplicity, which is equivalent to n being the sum of two squares. □

5.2. Number-theoretic preparations. Now that we have seen how effective Theorem 2 can be, we are eager to proceed to its proof. First, though, we shall collect a few number-theoretic results that shall be of use. The first is a classic theorem of Lagrange concerning the sums of *four* squares.[26]

THEOREM 3 (Lagrange, 1770). *Every natural number $n \in \mathbb{N}$ is expressible as the sum of four squares.*

We sadly lack the time to furnish a proof of this wonderful theorem here, but shall instead settle for the following "proof by example."

$$\begin{aligned} 1 &= 0^2 + 0^2 + 0^2 + 1^2, \\ 2 &= 0^2 + 0^2 + 1^2 + 1^2, \\ 3 &= 0^2 + 1^2 + 1^2 + 1^2, \text{ and} \\ 4 &= 1^2 + 1^2 + 1^2 + 1^2. \end{aligned}$$

If these examples are too small to convince you, here is a more random choice of n:

$$310 = 17^2 + 4^2 + 2^2 + 1^2.$$

Our next lemma follows trivially from the above result,[27] but for our purposes, its proof is more important than its statement, and so we shall prove it now.

LEMMA 2 (Euler's Identity, 1748). *If two natural numbers are the sums of sets of four squares, then so is their product.*

PROOF. Suppose $n = a_1^2 + a_2^2 + a_3^2 + a_4^2$ and $m = s_1^2 + s_2^2 + s_3^2 + s_4^2$. Define the matrix

$$H = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & -a_1 & a_4 & -a_3 \\ a_3 & -a_4 & -a_1 & a_2 \\ a_4 & a_3 & -a_2 & -a_1 \end{pmatrix},$$

and observe that $HH^T = nI$ (in particular, we have $\det H \neq 0$).

[26] This theorem may have been the inspiration behind the naming of a social network.

[27] However, Lemma 2 is used in the proof of Theorem 3, and so the lemma should be proven independently to avoid circularity.

Define a row vector $\vec{s} = (s_1, s_2, s_3, s_4) \in \mathbb{Z}^4$. Then

$$\vec{s}HH^T\vec{s}^T = \vec{s}(nI)\vec{s}^T = n\vec{s}\vec{s}^T = n(s_1^2 + s_2^2 + s_3^2 + s_4^2) = nm.$$

However, letting $\vec{u} = \vec{s}H = (u_1, u_2, u_3, u_4) \in \mathbb{Z}^4$, we have

$$\vec{s}HH^T\vec{s}^T = \vec{u}\vec{u}^T = u_1^2 + u_2^2 + u_3^2 + u_4^2.$$

Thus $nm = u_1^2 + u_2^2 + u_3^2 + u_4^2$ is the sum of four squares. □

5.3. Proof of the Theorem. Armed with these preliminaries, we now prove Theorem 2.

PROOF OF THEOREM 2. As case (1) is precisely Corollary 4, we need only prove case (2). We first set up some notation for the proof, starting with $n := k - \lambda$. Supposing the existence of a non-trivial symmetric 2-(v, k, λ) design $\mathcal{D}$, let A be its incidence matrix, and recall that $AA^T = (k - \lambda)I + \lambda J = nI + \lambda J$. Let $\vec{a}^j$ denote the j^{th} column of A, where $1 \leq j \leq v$.

We next define a set of linear forms. Given an arbitrary row vector $\vec{w} \in \mathbb{Q}^v$, define

$$L_j(\vec{w}) = \vec{w}\vec{a}^j = \sum_{i=1}^{v} a_{ij}w_i.$$

This gives rise to the following identity.

$$\begin{aligned}\sum_{j=1}^{v} L_j(\vec{w})^2 &= (L_1(\vec{w}), L_2(\vec{w}), \ldots, L_v(\vec{w}))(L_1(\vec{w}), L_2(\vec{w}), \ldots, L_v(\vec{w}))^T \\ &= (\vec{w}A)(\vec{w}A)^T = \vec{w}AA^T\vec{w}^T = \vec{w}(nI + \lambda J)\vec{w}^T = n\vec{w}\vec{w}^T + \lambda\vec{w}J\vec{w}^T\end{aligned}$$

Hence

$$(\dagger) \qquad \sum_{j=1}^{v} L_j(\vec{w})^2 = n\sum_{i=1}^{v} w_i^2 + \lambda\omega^2,$$

where $\omega = \sum_{i=1}^{v} w_i$. This identity is very close to what we require, as we have squares with the coefficients n and λ appearing, but there are too many squares. Our goal is thus to simplify this identity by removing the sums. We shall do so by introducing a clever change of variables, inspired by Lemma 2, that will allow us to cancel all but one of the summands.[28]

By Theorem 3, n is the sum of four squares, so we may write $n = a_1^2 + a_2^2 + a_3^2 + a_4^2$. Given these values, let H be the 4×4 matrix from the proof of Lemma 2, which we shall use for the change of variables. We now separate into two cases, based on $v \pmod 4$.

[28] If you steal a glance at the page of calculations that lies in wait, you might wonder why we bother doing this. Recall that our goal is to develop a necessary condition that we can use to rule out the existence of certain designs. Given the large number of degrees of freedom in this identity, it would be very difficult to show the impossibility of such an identity holding. By instead simplifying the identity to a quadratic Diophantine equation, whose study dates back to antiquity, we make it much easier to apply the theorem.

First suppose $v \equiv 1 \pmod 4$. We define new variables $\vec{u} \in \mathbb{Q}^v$ by $\vec{w}M = \vec{u}$, where M is the $v \times v$ block-diagonal matrix

$$M = \begin{pmatrix} H & & & & \\ & H & & & \\ & & \ddots & & \\ & & & H & \\ & & & & 1 \end{pmatrix}.$$

Note that since H is invertible, M is as well, and so we have an invertible linear map. This implies that the original variables $\{w_i : 1 \leq i \leq v\}$ are linear combinations of the new variables $\{u_i : 1 \leq i \leq v\}$.

Furthermore, for each ℓ, $0 \leq \ell \leq \frac{v-5}{4}$, we have

$$(w_{4\ell+1}, w_{4\ell+2}, w_{4\ell+3}, w_{4\ell+4})H = (u_{4\ell+1}, u_{4\ell+2}, u_{4\ell+3}, u_{4\ell+4}).$$

Hence, as in the proof of Lemma 2, $n(w_{4\ell+1}^2 + \ldots + w_{4\ell+4}^2) = u_{4\ell+1}^2 + \ldots + u_{4\ell+4}^2$. For the last variable we simply have $w_v = u_v$.

Substituting these equations into (†), we find

$$\sum_{j=1}^{v} L_j^2 = \sum_{i=1}^{v-1} u_i^2 + nu_v^2 + \lambda\omega^2, \tag{‡}$$

where the linear forms L_j and ω are linear combinations of the variables $\{w_i : 1 \leq i \leq v\}$, and hence also of the variables $\{u_i : 1 \leq i \leq v\}$.

Thus far the variables u_i have remained arbitrary. We shall now fix values for u_i in such a way that $L_j = \pm u_j$, allowing us to cancel the corresponding summands on both sides of the equality above.

More precisely, since L_1 is a linear combination of the u_i, we have $L_1 = \sum_{i=1}^{v} \alpha_i u_i$ for some constants $\alpha_i \in \mathbb{Q}$. If $\alpha_1 \neq 1$, we shall set $L_1 = u_1$. Solving for u_1, we find $(1 - \alpha_1)u_1 = \sum_{i \geq 2} \alpha_i u_i$, or $u_1 = \frac{1}{1-\alpha_1} \sum_{i \geq 2} \alpha_i u_i$. If we have $\alpha_1 = 1$, then we instead set $L_1 = -u_1$, which we can solve to obtain $u_1 = \frac{-1}{2} \sum_{i \geq 2} \alpha_i u_i$.

In either case, $L_1^2 = u_1^2$, and so we can cancel both summands in (‡) to obtain

$$\sum_{j=2}^{v} L_j^2 = \sum_{i=2}^{v-1} u_i^2 + nu_v^2 + \lambda\omega^2,$$

where we can consider L_j and ω as linear combinations of $\{u_i : 2 \leq i \leq v\}$ (since u_1 is now also a linear combination of these variables).

Repeating this process, we can ensure $L_j = \pm u_j$ for $1 \leq j \leq v - 1$, in which case our identity will have been reduced to $L_v^2 = nu_v^2 + \lambda\omega^2$, where L_v and ω are scalar multiples (over $\mathbb{Q}$) of u_v. Multiplying through by a common denominator β, we find integral solutions to the equation $z^2 = ny^2 + \lambda x^2$, where $z = \beta L_v$, $y = \beta u_v$ and $x = \beta\omega$. Since u_v can be taken to be an arbitrary integer, this gives non-trivial integer solutions to the desired quadratic equation.

The second case, when $v \equiv 3 \pmod 4$, is handled very similarly. In this case, to get our sets of four variables for the transformation, we instead introduce an artificial variable w_{v+1} to both sides of (†), thus starting with

$$(\dagger\dagger) \qquad \sum_{j=1}^{v} L_j^2 + n w_{v+1}^2 = n \sum_{i=1}^{v+1} w_i^2 + \lambda \omega^2,$$

where $\omega = \sum_{i=1}^{v} w_i$. We now use the change of variables $\vec{w}M = \vec{u}$, where

$$M = \begin{pmatrix} H & & & \\ & H & & \\ & & \ddots & \\ & & & H \end{pmatrix}.$$

As before, this transforms (††) into

$$(\ddagger\ddagger) \qquad \sum_{j=1}^{v} L_j^2 + n w_{v+1}^2 = \sum_{i=1}^{v+1} u_i^2 + \lambda \omega^2,$$

where L_j, w_{v+1} and ω are all linear combinations of the variables $\{u_i : 1 \leq i \leq v+1\}$.

Using the same elimination process as in the first case, we can ensure $L_j = \pm u_j$ for $1 \leq j \leq v$, and then cancel the corresponding squares from (‡‡). This leaves us with the equation $n w_{v+1}^2 = u_{v+1}^2 + \lambda \omega^2$, where w_{v+1} and ω are scalar multiples of u_{v+1}. Multiplying through by a common denominator β and rearranging, we obtain a solution to $z^2 = ny^2 - \lambda x^2$ by taking $z = \beta u_{v+1}$, $y = \beta w_{v+1}$ and $x = \beta \omega$. Since u_{v+1} can be an arbitrary integer, this again gives non-trivial integer solutions to the desired quadratic equation, completing the proof of the theorem. □

6. Designs of strength $t \geq 3$

As we have previously stated, much of the early interest in designs focussed on the case $t = 2$, which was sufficient for most statistical applications. However, as the area developed, researchers, and especially combinators, started investigating designs of higher strength. Once again, the primary question was existential: for which parameters do such designs exist, and how can we construct them?

In this section, we shall briefly survey a few results in this direction. We will assume throughout that the arithmetic conditions of Corollary 1 hold, and shall seek additional necessary conditions.

6.1. The Wilson–Petrenjuk Inequality. Recall that for 2-designs, Fisher's Inequality (Proposition 3) showed that the conditions of Corollary 1 are not sufficient, since a 2-(v, k, λ) design has to have at least v blocks. For larger values of t, Lemma 1 shows that t-designs are also 2-designs, and so it follows that we still must have at least v blocks.

However, t-designs must satisfy much more stringent regularity conditions — rather than just having all $\binom{v}{2}$ pairs covered by the same number of blocks, they must have all $\binom{v}{t}$ t-sets

equally covered. One might expect that a much larger number of blocks should be needed to guarantee this higher level of regularity, and our next result shows that this is indeed true.

THEOREM 4 (The Wilson–Petrenjuk[29] Inequality). *If $t \geq 2s$ and $v \geq k + s$, then for any t-(v, k, λ) design we must have $b \geq \binom{v}{s}$.*

Note that Theorem 4 extends Fisher's Inequality, which is the case $s = 1$. Now for a spot of unsolicited advice, which is valuable both within and without mathematics: when attempting to prove a generalisation, try generalising the proof. We proved Fisher's Inequality by considering the incidence matrix of the design, whose rows were indexed by elements of the ground set. By taking an appropriate matrix product, we obtained a matrix corresponding to pairs of elements, which was useful for a 2-design. Thus, in order to study t-designs, we will need to start with a matrix indexed by larger subsets.

DEFINITION 7 (Higher incidence matrices). Let $\mathcal{D}$ be a t-(v, k, λ) design and fix some $0 \leq i \leq t$. The *higher incidence matrix* N_i is a $\binom{v}{i} \times b$ $\{0, 1\}$-matrix whose rows are indexed by the i-sets $I \in \binom{X}{i}$ and columns by blocks $B \in \mathcal{D}$, with

$$(N_i)_{I,B} = \begin{cases} 1 & \text{if } I \subseteq B, \\ 0 & \text{otherwise.} \end{cases}$$

REMARK 8. Some quick observations:

(i) When $i = 1$, we recover the incidence matrix; that is, $N_1 = A$.
(ii) Unsurprisingly, the higher incidence matrices are very regular structures. Each row of N_i has exactly λ_i ones (by Lemma 1), while each column has exactly $\binom{k}{i}$ ones.

An important class of higher incidence matrices are those for the trivial design $\mathcal{D} = \binom{X}{k}$. Note that N_t for this design encodes all the information regarding containing of t-sets inside k-sets, and thus warrants its own piece of notation.

DEFINITION 8. Given $t \leq k$, let $W_{t,k}$ be the higher incidence matrix N_t for $\mathcal{D} = \binom{X}{k}$.

We shall also require the following general result about designs, which is in the spirit of results we proved in Section 2. Indeed, it can be proven using Proposition 1.

LEMMA 3. *Let $\mathcal{D}$ be a t-(v, k, λ) design, and fix $i, j \geq 0$ with $i + j \leq t$. Then, for any i-set $I \in \binom{X}{i}$ and j-set $J \in \binom{X}{j}$ with $I \cap J = \emptyset$, the number of blocks $B \in \mathcal{D}$ with $I \subseteq B$ and $B \cap J = \emptyset$ is*

$$b_{i,j} = \frac{\lambda \binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}.$$

[29] Once again we find some non-standard alphabetisation, which means it is time for another historical aside. This theorem is again the combination of two separate papers: in 1968, Petrenjuk proved the case $s = 2$, and then Ray-Chaudhuri and Wilson proved the general result in 1975. The fact that these papers came some thirty years after Fisher's Inequality (which was stated by Fisher in 1940) indicates the extent to which 2-designs dominated the developmental stages of the field of combinatorial designs.

Furthermore, for every $0 \leq a \leq t$, we have the identity

$$\lambda_{t-a} = \sum_{i=0}^{a} \binom{a}{i} b_{t-i,i}.$$

PROOF. The proof is left as an exercise for the reader. □

We are now in position to prove the Wilson–Petrenjuk Inequality.

PROOF OF THEOREM 4. Since our desired lower bound depends only on v and s, and not on t or λ, we may appeal to Lemma 1 and assume $t = 2s$. Now consider the higher incidence matrix N_s, which is a $\binom{v}{s} \times b$ matrix and thus has $\mathrm{rk}(N_s) \leq b$.

Following our proof of Fisher's Inequality, we define the matrix $M = N_s N_s^T$. This is an $\binom{v}{s} \times \binom{v}{s}$ matrix with $\mathrm{rk}(M) \leq \mathrm{rk}(N_s) \leq b$, and hence it suffices to show that M has full rank. Unlike with Fisher's Inequality, we will not be able to easily compute the determinant of this matrix directly.[30] Instead, we shall decompose M cleverly.

CLAIM 2. $M = \sum_{i=0}^{s} b_{t-i,i} W_{i,s}^T W_{i,s}$.

PROOF. Both the left- and right-hand sides of the equation are $\binom{v}{s} \times \binom{v}{s}$ matrices, indexed by $\binom{X}{s}$. Given $E, F \in \binom{X}{s}$, we have

$$\begin{aligned} M_{E,F} = (N_s N_s^T)_{E,F} &= \sum_{B \in \mathcal{D}} (N_s)_{E,B} (N_s)_{F,B} \\ &= |\{B \in \mathcal{D} : E, F \subseteq B\}| = |\{B \in \mathcal{D} : E \cup F \subseteq B\}| \\ &= \lambda_{|E \cup F|} = \lambda_{|E|+|F|-|E \cap F|} = \lambda_{t-|E \cap F|}, \end{aligned}$$

where in the last line we used Lemma 1 together with the fact that $|E| + |F| = 2s = t$.

On the other hand, we also have

$$(W_{i,s}^T W_{i,s})_{E,F} = \sum_{I \in \binom{X}{i}} (W_{i,s})_{I,E} (W_{i,s})_{I,F} = \left| \left\{ I \in \binom{X}{i} : I \subseteq E \cap F \right\} \right| = \binom{|E \cap F|}{i}.$$

Thus the sum on the right-hand side evaluates to

$$\sum_{i=0}^{s} b_{t-i,i} (W_{i,s}^T W_{i,s})_{E,F} = \sum_{i=0}^{s} \binom{|E \cap F|}{i} b_{t-i,i} = \sum_{i=0}^{|E \cap F|} \binom{|E \cap F|}{i} b_{t-i,i} = \lambda_{t-|E \cap F|}$$

where the last equality follows from Lemma 3. This proves the claim. □

We now use this decomposition of M to show the following.

CLAIM 3. *M is positive definite.*

[30] To understand why not, observe that the rows and columns of M are indexed by the s-sets $\binom{X}{s}$. When $s = 1$, two s-sets are either the same or disjoint. For larger values of s, though, these s-sets can intersect in different ways, which makes the matrix M somewhat more complicated.

PROOF. We need to show that for every non-zero $\vec{x}$,

$$\vec{x}^T M \vec{x} = \sum_{i=0}^{s} b_{t-i,i} \vec{x}^T W_{i,s}^T W_{i,s} \vec{x} > 0.$$

For all i, we have $\vec{x}^T W_{i,s}^T W_{i,s} \vec{x} = (W_{i,s}\vec{x})^T W_{i,s}\vec{x} = \|W_{i,s}\vec{x}\|_2^2 \geq 0$, and so M is certainly positive *semi*definite. Moreover, for $i = s$, $W_{s,s}$ is the identity matrix, so $b_{t-s,s} W_{s,s}^T W_{s,s}$ is positive definite if $b_{t-s,s}$ is positive. Since $t = 2s$, $b_{t-s,s} = b_{s,s}$ counts, for two disjoint s-sets, the number of blocks that contain the first and are disjoint from the second. Fix the first s-set and let B be any block containing it. Since we assume $v \geq k + s$, there is an s-set disjoint from B. By taking this to be the second s-set, we see that $b_{s,s}$ is indeed positive, and hence M is positive definite. □

It follows that M has full rank,[31] and hence $\binom{v}{s} = \text{rk}(M) \leq b$, proving Theorem 4. □

REMARK 9. A t-design is called *tight* if it satisfies Theorem 4 with equality. When $v = k + s$, $\binom{v}{s} = \binom{v}{k}$, so the trivial design $\binom{X}{k}$ is tight. However, for $s > 1$ and $v > k + s$, there is only one pair of tight designs known —- a Steiner system and its complement.

6.2. The existence of non-trivial t-designs. Theorem 4 provides an additional necessary condition for t-designs, using the higher incidence matrices to show there are no small t-designs. As we have seen previously, though, the same methods used to prove non-existence results can also be employed in the construction of designs. In this instance, the negative and positive results do not just share the same ingredients, but also the same author; as we shall now see, Wilson used the higher incidence matrices to show that the necessary arithmetic conditions of Corollary 1 are also sufficient for the existence of non-trivial t-designs.[32]

The key, though straightforward, observation, captured in the claim below, is that the construction of t-designs is really an exercise in linear algebra.

CLAIM 4. *A t-(v, k, λ) design exists if and only if there is some vector $\vec{c} \in \mathbb{Z}_{\geq 0}^{\binom{X}{k}}$ such that*

$$W_{t,k}\vec{c} = \lambda \vec{1},$$

where $\vec{1} \in \mathbb{Z}_{\geq 0}^{\binom{X}{t}}$ is the all-one vector.

PROOF. Such vectors $\vec{c}$ can be thought of as characteristic vectors for collections of k-sets $\mathcal{D}$, where for every set $K \in \binom{X}{k}$, c_K denotes the number of times K appears in $\mathcal{D}$. For every t-set $T \in \binom{X}{t}$, $(W_{t,k}\vec{c})_T$ counts (with multiplicity) the number of k-sets in $\mathcal{D}$ containing T. Thus $\mathcal{D}$ is a t-(v, k, λ) design if and only if $W_{t,k}\vec{c}$ is the all-λ vector. □

Of course, things are not quite so simple. Vector spaces in linear algebra are defined over fields, and if we allow vectors with rational coordinates, the matrix equation is easily seen to

[31] Indeed, were this not the case, there would be some non-zero vector $\vec{x}$ with $M\vec{x} = \vec{0}$, but then $\vec{x}^T M \vec{x} = 0$.

[32] His paper was rather charmingly titled, "The necessary conditions for t-designs are sufficient for something."

be satisfied by taking $\vec{c} = \binom{v-t}{k-t}^{-1}\lambda\vec{1}$ (where $\vec{1}$ is now the all-one vector in $\mathbb{Q}^{\binom{X}{k}}$). The challenge, therefore, is to find a solution with non-negative integer coordinates.[33] Meeting the challenge and then some, Wilson showed that the generalisation of the necessary arithmetic conditions of Corollary 1 is sufficient for *integer* solutions to matrix equations involving $W_{t,k}$.

THEOREM 5 (Wilson, 1973). *Let $k \geq t \geq 0$ and $v \geq k+t$ be integers, and let $\vec{a} \in \mathbb{Z}^{\binom{X}{t}}$. There is an integral solution $\vec{c} \in \mathbb{Z}^{\binom{X}{k}}$ to the equation $W_{t,k}\vec{c} = \vec{a}$ if and only if for every $I \subseteq X$ with $|I| = i \leq t$, we have*

$$(*) \qquad \sum_{T \in \binom{X}{t} : I \subseteq T} a_T \equiv 0 \pmod{\binom{k-i}{t-i}}.$$

In fact, Wilson gave necessary and sufficient conditions for all values of $v \geq k$, not just $v \geq k+t$. When $k \leq v \leq k+t$, in addition to the arithmetic conditions above, one also requires that the target vector $\vec{a}$ lies in the column space of $W_{t,k}$. The following lemma gives information concerning $W_{t,k}$ in this range.

LEMMA 4. *If $v \leq k+t$, the columns of $W_{t,k}$ are linearly independent.*

PROOF. This is yet another exercise for the reader. □

However, we know from Corollary 2 that any design with $v \leq k+t$ must be trivial, so we shall focus on the case $v \geq k+t$. We shall prove Theorem 5 in due course, but first observe that the theorem allows vectors with coordinates in $\mathbb{Z}$, not just $\mathbb{Z}_{\geq 0}$. These solutions correspond to *signed* designs, where we in some sense allow blocks to be taken with negative multiplicity.

Such flexibility is necessary, for, as shown by Theorem 4, the arithmetic conditions of Corollary 1 alone are not sufficient for the existence of an actual design. However, as we now prove, Theorem 5 implies they *are* sufficient when λ is sufficiently large.

COROLLARY 7. *Given integers $k \geq t \geq 0$ and $v \geq k+t$, there is some $\lambda_0 = \lambda_0(v,k,t)$ such that if $\lambda \geq \lambda_0$ satisfies $\lambda\binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}}$ for every $0 \leq i \leq t$, then there is a t-(v,k,λ) design.*

PROOF. Define

$$\Lambda = \left\{\lambda : -\binom{v-t}{k-t} \leq \lambda < 0, \text{ and, for all } 0 \leq i \leq t, \ \lambda\binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}}\right\},$$

and note that Λ is finite, with its size bounded by v, k and t. For $\vec{a} = \lambda\vec{1}$ and $I \subseteq X$, $|I| = i \leq t$, we have

$$\sum_{T \in \binom{X}{t} : I \subseteq T} a_T = \lambda\left|\left\{T \in \binom{X}{t} : I \subseteq T\right\}\right| = \lambda\binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}},$$

[33] While you might think that there should not be such a great difference between rational and integral solutions, numerous examples throughout mathematics show that this is sadly not so. For instance, Linear Programming is solvable in polynomial time, while Integer Linear Programming is $\mathcal{NP}$-complete.

and hence the conditions of Theorem 5 are satisfied. It follows that there is some $\vec{c}_\lambda \in \mathbb{Z}^{\binom{X}{k}}$ with $W_{t,k}\vec{c}_\lambda = \lambda\vec{1}$ for all $\lambda \in \Lambda$.

Take $-N$ to be the most negative coordinate in all of these vectors, so that

$$-N = \min_{\lambda\in\Lambda, K\in\binom{X}{k}} (\vec{c}_\lambda)_K,$$

and set $\lambda_0 = (N-1)\binom{v-t}{k-t}$.

If $\lambda \geq \lambda_0$ satisfies the arithmetic conditions, we can write $\lambda = m\binom{v-t}{k-t} + \lambda'$, where $-\binom{v-t}{k-t} \leq \lambda' < 0$ (and hence $m \geq N$). Since the arithmetic conditions are linear in λ, and are satisfied by both λ and $m\binom{v-t}{k-t}$, it follows that $\lambda' \in \Lambda$. Taking $\vec{c} = m\vec{1} + \vec{c}_{\lambda'}$, we have

$$W_{t,k}\vec{c} = W_{t,k}m\vec{1} + W_{t,k}\vec{c}_{\lambda'} = m\binom{v-t}{k-t}\vec{1} + \lambda'\vec{1} = \lambda\vec{1}.$$

Moreover, for every $K \in \binom{X}{k}$, we have $c_K = m + (\vec{c}_{\lambda'})_K \geq m - N \geq 0$, and so $\vec{c} \in \mathbb{Z}_{\geq 0}^{\binom{X}{k}}$ corresponds to an actual t-(v,k,λ) design, as required. □

We conclude this section by proving the theorem of Wilson.

PROOF OF THEOREM 5. We first prove that the conditions in $(*)$ in the theorem are indeed necessary for an integral solution to the matrix equation.

Suppose there is a solution $\vec{c} \in \mathbb{Z}^{\binom{X}{k}}$ to the equation $W_{t,k}\vec{c} = \vec{a}$, and fix some $I \subseteq X$ with $|I| \leq t$. We shall evaluate the double sum

$$(\dagger) \qquad \sum_{\substack{T\in\binom{X}{t}, K\in\binom{X}{k} \\ I\subseteq T\subseteq K}} c_K.$$

By summing over T first, we find (†) is equal to

$$\sum_{\substack{T\in\binom{X}{t} \\ I\subseteq T}} \sum_{\substack{K\in\binom{X}{k} \\ T\subseteq K}} c_K = \sum_{\substack{T\in\binom{X}{t} \\ I\subseteq T}} (W_{t,k}\vec{c})_T = \sum_{\substack{T\in\binom{X}{t} \\ I\subseteq T}} a_T,$$

giving the left-hand side of $(*)$.

Summing over K first shows that (†) is also equal to

$$\sum_{\substack{K\in\binom{X}{k} \\ I\subseteq K}} \sum_{\substack{T\in\binom{X}{t} \\ I\subseteq T\subseteq K}} c_K = \sum_{\substack{K\in\binom{X}{k} \\ I\subseteq K}} c_K \sum_{\substack{T\in\binom{K}{t} \\ I\subseteq T}} 1 = \binom{k-i}{t-i} \sum_{\substack{K\in\binom{X}{k} \\ I\subseteq K}} c_K.$$

This gives

$$(\ddagger) \qquad \sum_{\substack{T\in\binom{X}{t} \\ I\subseteq T}} a_T = \binom{k-i}{t-i} \sum_{\substack{K\in\binom{X}{k} \\ I\subseteq K}} c_K.$$

Since $\vec{c} \in \mathbb{Z}^{\binom{X}{k}}$, the sum in the right-hand side of (‡) must be an integer, and hence the left-hand side is indeed divisible by $\binom{k-i}{t-i}$. Thus the equations $(*)$ in the statement of the theorem are indeed necessary.

We now proceed to show the equations $(*)$ are also sufficient. We use induction on t.

Base case: $t = 0$. This is trivial since, $\binom{X}{0} = \{\emptyset\}$, and $W_{0,k} = \begin{pmatrix} 1 & 1 & \dots & 1 \end{pmatrix}$. So, given any $a_\emptyset \in \mathbb{Z}$, $\vec{c} = (a_\emptyset, 0, \dots, 0)^T$ is a solution.

Induction step: $t \geq 1$. We prove the induction step via a second induction, this time on v.

v-Base case: $v = k + t$. By Lemma 4, the colums of $W_{t,k}$ are linearly independent. Here we have $\binom{v}{k}$ columns in a $\binom{v}{t}$- dimensional space, but since $v = k + t$, $\binom{v}{t} = \binom{v}{k}$, and hence the columns of $W_{t,k}$ form a basis for $\mathbb{Q}^{\binom{X}{t}}$. Thus $W_{t,k}$ is invertible, and so there is a unique $\vec{c} \in \mathbb{Q}^{\binom{X}{k}}$ such that $W_{t,k}\vec{c} = \vec{a}$.

We will show that in fact $\vec{c} \in \mathbb{Z}^{\binom{X}{k}}$. First recall from $(\ddagger)$ that for $I \subseteq X$ with $|I| \leq t$,

$$\sum_{\substack{T \in \binom{X}{t} \\ I \subseteq T}} a_T = \binom{k-i}{t-i} \sum_{\substack{K \in \binom{X}{k} \\ I \subseteq K}} c_K.$$

Since $\vec{a}$ satisfies $(*)$, the left-hand side is divisible by $\binom{k-i}{t-i}$, from which it follows that for every $I \subseteq X$, $|I| \leq t$, we have

$(\dagger\dagger)$
$$\sum_{\substack{K \in \binom{X}{k} \\ I \subseteq K}} c_K \in \mathbb{Z}.$$

We now need to show that each individual coordinate of $\vec{c}$ is integral. To that end, fix a k-set $K_0 \in \binom{X}{k}$. Since $v = k + t$, there is a unique t-set $T_0 = X \setminus K_0$ disjoint from K_0. We count (with the rational multiplicities from $\vec{c}$) the number of blocks disjoint from T_0. Since K_0 is the only k-set disjoint from T_0, this is simply c_{K_0}. However, by inclusion-exclusion, we obtain the equation

$$c_{K_0} = \sum_{I \subseteq T_0} (-1)^{|I|} \sum_{\substack{K \in \binom{X}{k} \\ I \subseteq K}} c_K.$$[34]

[34] To see why this equation holds, we can exchange the order of summation on the right-hand side - first sum over $K \in \binom{X}{k}$, and then over suitable I. The right-hand side is thus equal to

$$\sum_{K \in \binom{X}{k}} \sum_{I \subseteq K \cap T_0} (-1)^{|I|} c_K = \sum_{K \in \binom{X}{k}} c_K \sum_{i=0}^{|K \cap T_0|} \binom{|K \cap T_0|}{i} (-1)^i = \sum_{K \cap X k} c_K \left(1 + (-1)\right)^{|K \cap T_0|} = \sum_{K \in \mathbb{X} k} c_K \cdot 0^{|K \cap T_0|},$$

where in the first inequality we group the possible sets I by their size $i = |I|$, and the second equality we appeal to the Binomial Theorem. Hence the contribution of K to the right-hand side is zero, unless $|K \cap T_0| = 0$, in which case it is c_K. However, the only k-set disjoint from T_0 is K_0, and hence this double sum is equal to c_{K_0}.

To understand why we refer to this as inclusion-exclusion, note that if $c_K \equiv 1$, then on the left-hand side we are simply counting the number of k-sets that are disjoint from T_0. We obtain this by subtracting from the collection of all k-sets (i.e., those that contain $\emptyset$) the number of k-sets that intersect T_0. If, for $x \in X$, $\mathcal{D}_x$ is the collection of k-sets that contain x, then what we want to subtract is $|\cup_{x \in T_0} \mathcal{D}_x|$, which can be found using inclusion-exclusion. Taking this approach results in the double sum we have above.

Introducing the terms c_K adds individual weights to the k-sets, but, as we have proved in this footnote, this weighted inclusion-exclusion principle remains valid.

By (††), it follows that each of the inner sums on the right-hand side is an integer, and hence $c_{K_0} \in \mathbb{Z}$. Since K_0 was arbitrary, we have $\vec{c} \in \mathbb{Z}^{\binom{X}{k}}$, as required.

v-Induction step: $v \geq k+t+1, k \geq t \geq 1$. We are given a vector $\vec{a} \in \mathbb{Z}^{\binom{X}{t}}$ satisfying $(*)$, and we wish to find $\vec{c} \in \mathbb{Z}^{\binom{X}{k}}$ with $W_{t,k}\vec{c} = \vec{a}$.

Fix an arbitrary $x_0 \in X$. Our construction is in two stages. First we use k-sets containing x_0 to cover all t-sets containing x_0 the right number of times. In the second stage, we use k-sets avoiding x_0 to ensure we also correctly cover the t-sets not containing x_0. Note that this second stage cannot affect the number of times a t-set containing x_0 is covered, and hence we will have $W_{t,k}\vec{c} = \vec{a}$.

Stage I. We first solve the matrix equation for the t-sets containing x_0, for which we need only consider t-sets and k-sets containing x_0. We may reduce the set-up to one where we can apply induction by removing x_0 from all the sets.

Let $X' = X \setminus \{x_0\}$, let $T' = T \setminus \{x_0\}$ for all t-sets containing x_0, and similarly for a k-set K containing x_0, let $K' = K \setminus \{x_0\}$. This gives a system with $v' = v-1, t' = t-1$ and $k' = k-1$. Define the target vector $\vec{a'} \in \mathbb{Z}^{\binom{X'}{t'}}$ by setting $a'_{T'} = a_{T' \cup \{x_0\}}$ for all $T' \in \binom{X'}{t'}$.

We now verify that $\vec{a'}$ satisfies $(*)$ in this reduced system. Indeed, for $I' \subseteq X'$ with $|I'| \leq t'$, we have

$$\sum_{\substack{T' \in \binom{X'}{t'} \\ I' \subseteq T'}} a'_{T'} = \sum_{\substack{T' \in \binom{X'}{t'} \\ I' \subseteq T'}} a_{T' \cup \{x_0\}} = \sum_{\substack{T \in \binom{X}{t} \\ I' \cup \{x_0\} \subseteq T'}} a_T.$$

Since $|I' \cup \{x_0\}| \leq t'+1 = t$, and $\vec{a}$ satisfies $(*)$ for the original parameters, it follows that this sum is divisible by $\binom{k-(|I'|+1)}{t-(|I'|+1)}$. However, this is equal to $\binom{k'-|I'|}{t'-|I'|}$, and so it follows that $\vec{a'}$ satisfies $(*)$ in this reduced space as well.

By the (t-)induction hypothesis, the necessary conditions $(*)$ are also sufficient for an integral solution, and so we find a vector $\vec{c'} \in \mathbb{Z}^{\binom{X'}{k'}}$ with $W_{t',k'}\vec{c'} = \vec{a'}$. Now define $\tilde{\vec{c}} \in \mathbb{Z}^{\binom{X}{k}}$ by taking

$$\tilde{c}_K = \begin{cases} c'_{K'} & \text{if } x_0 \in K, \\ 0 & \text{otherwise.} \end{cases}$$

Then, if $T \in \binom{X}{t}$ is a t-set containing x_0, we have $(W_{t,k}\tilde{\vec{c}})_T = (W_{t',k'}\vec{c'})_{T'} = a'_{T'} = a_T$, and so $\tilde{\vec{c}}$ satisfies the matrix equation for all t-sets containing x_0.

Stage II. We now complete our solution by handling the t-sets that do not contain x_0. We shall only use k-sets also not containing x_0, and hence will not disturb our solution from Stage I for those t-sets that do contain x_0.

Let $\tilde{\vec{a}} = W_{t,k}\tilde{\vec{c}}$, and define $\vec{a''} = \vec{a} - \tilde{\vec{a}} \in \mathbb{Z}^{\binom{X}{t}}$. Since $\tilde{\vec{c}} \in \mathbb{Z}^{\binom{X}{k}}$, the necessity of $(*)$ shows that $\tilde{\vec{a}}$ satisfies those equations. By assumption, $\vec{a}$ does as well. Since the equations of $(*)$ are linear in $\vec{a}$, it follows that $\vec{a''}$ must also satisfy $(*)$.

By our work in Stage I, we have $a''_T = 0$ for any $T \in \binom{X}{t}$ with $x_0 \in T$. Since we only wish to use k-sets not containing x_0, we may remove the element x_0 from our ground set, instead

working with t- and k-sets over $X'' = X \setminus \{x_0\}$.[35] We now have $v'' = v - 1$, with k and t unchanged.

Hence we can treat $\vec{a''}$ as a vector in $\mathbb{Z}^{\binom{X''}{t}}$. Since $(*)$ does not involve v, it follows that $\vec{a''}$ still satisfies the necessary conditions over this smaller ground set.[36] Using the v-induction hypothesis, we know that the necessary conditions are also sufficient for an integral solution, and hence there is some $\vec{c''} \in \mathbb{Z}^{\binom{X''}{k}}$ with $W''_{t,k}\vec{c''} = \vec{a''}$.

Extending by zeroes for any t- and k-sets containing x_0, we can lift this solution back to the full ground set X, so that $\vec{c''} \in \mathbb{Z}^{\binom{X}{k}}$. Setting $\vec{c} = \vec{\tilde{c}} + \vec{c''} \in \mathbb{Z}^{\binom{X}{k}}$, we find

$$W_{t,k}\vec{c} = W_{t,k}\vec{\tilde{c}} + W_{t,k}\vec{c''} = \vec{\tilde{a}} + \vec{a''} = \vec{\tilde{a}} + \left(\vec{a} - \vec{\tilde{a}}\right) = \vec{a},$$

giving the desired integral solution, completing the induction, and thus the proof. □

7. Hadamard Designs

This section was lectured by Ander Lamaison and Patrick Morris.

We now return to our earlier study of 2-designs, and shall in this section introduce an important class of symmetric 2-designs.

7.1. Possible sizes of the ground set. We begin by observing that the parameter λ cannot be too large.

LEMMA 5. *Let $\mathcal{D}$ be a non-trivial symmetric 2-(v, k, λ) design. Then $\lambda \leq k - 2$.*

PROOF. For a symmetric design, we have $v = b = \frac{\lambda v(v-1)}{k(k-1)}$, which can be solved to give $k(k-1) = \lambda(v-1)$. Since the design is non-trivial, $v \geq k + t = k + 2$, and so $v - 1 > k$, which implies $\lambda < k - 1$. □

We define n to be $k - \lambda$,[37] noting that $n \geq 2$. The next result restricts the possible size of the ground set of a symmetric 2-design.

PROPOSITION 6. *If a non-trivial symmetric 2-(v, k, λ) design exists, then*

$$4n - 1 \leq v \leq n^2 + n + 1.$$

PROOF. We have

$$v - 1 = \frac{k(k-1)}{\lambda} = \frac{(n+\lambda)(n+\lambda-1)}{\lambda} = \frac{n(n-1)}{\lambda} + 2n - 1 + \lambda,$$

[35] This is the same ground set as X' from Stage I, but we use the different notation to emphasise that we are now in Stage II.

[36] In projecting $\vec{a''}$ from $\mathbb{Z}^{\binom{X}{t}}$ to $\mathbb{Z}^{\binom{X''}{t}}$, we do lose some coordinates of $\vec{a''}$, but $a''_T = 0$ for all those t-sets T (which all contain x_0), and hence the equations are unaffected.

[37] One reason to make this definition is that it will make several later calculations cleaner. Additionally, note that $n = b_{1,1}$ (as in Lemma 3), which perhaps gives some combinatorial reason behind the importance of this parameter.

and hence

$$v = \frac{n(n-1)}{\lambda} + 2n + \lambda =: g(\lambda).$$

Taking derivates gives $g'(\lambda) = 1 - \frac{n(n-1)}{\lambda^2}$ and $g''(\lambda) > 0$ for $\lambda > 0$, and so g is convex on $(0, \infty)$ with a minimum at $\lambda = \sqrt{n(n-1)}$. This implies that the minimum of $g(\lambda)$ for $\lambda \in \mathbb{N}$ is attained when $\lambda \in \{n-1, n\}$, so $v = g(\lambda) \geq g(n) = 4n - 1$. This gives the desired lower bound. For the upper bound, observe that $v \in \mathbb{N}$ implies $\lambda | n(n-1)$. By convexity, $g(\lambda)$ is maximised when $\lambda \in \{1, n(n-1)\}$, which shows $v = g(\lambda) \leq g(1) = n^2 + n + 1$. □

The projective planes match the upper bound with equality, which shows that it cannot be improved. We also give a special name to designs — should they exist — that attain the lower bound.

DEFINITION 9 (Hadamard design). A *Hadamard design* is a symmetric 2-$(4n-1, 2n-1, n-1)$ design.

REMARK 10. Some remarks on Proposition 6.

(i) The symmetric 2-designs come in complementary pairs, $\mathcal{D}$ and $\overline{\mathcal{D}}$ (see Corollary 3). If, from each pair, we choose the design with $k \leq \frac{1}{2}v$, then the projective planes correspond to the sparsest possible symmetric designs, with their blocks spread out over the maximum number of elements. On the other hand, Hadamard designs represent the densest possible designs, with as few elements as can be.

(ii) If $\mathcal{D}$ is symmetric 2-(v, k, λ) design with $v = 4n - 1$, then $\mathcal{D}$ must be either a 2-$(4n-1, 2n-1, n-1)$ design or its complement — no other values for k or λ are possible. Indeed, the convexity of $g(\lambda)$ implies that it is minimised over $\mathbb{N}$ if and only if $\lambda \in \{n-1, n\}$.

7.2. Hadamard matrices. As might be indicated by their names, Hadamard designs bear a close connection to Hadamard matrices, which are useful in several mathematical fields.

DEFINITION 10 (Hadamard matrix). A *Hadamard matrix* is an $m \times m$ $\{-1, 1\}$-matrix H such that $HH^T = mI$.

Note that this is equivalent to requiring that the rows of the matrix be mutually orthogonal. The same is true of its columns.

EXAMPLE 7. Some small examples of Hadamard matrices are

$$\begin{pmatrix} 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix}.$$

Note that if H is a Hadamard matrix, then so too is any matrix obtained from H by permuting rows and/or columns, and multiplying any of the rows and columns by -1. Applying these operations, we can transform a Hadamard matrix into one in a standard form.

DEFINITION 11 (Normalised Hadamard matrix). Let H be a Hadamard matrix. We say H is *normalised* if both the first row and column only have positive entries.

Our next result restricts the possible sizes of Hadamard matrices.

LEMMA 6. *If an $m \times m$ Hadamard matrix exists, then either $m \leq 2$ or $m = 4n$ for some $n \in \mathbb{N}$.*

PROOF. Suppose $m \geq 3$. If such a matrix H exists, we may assume that it is normalised, with the first row only having positive entries. We can separate the columns into four types, based on the signs of the entries in the second and third rows. By reordering the columns appropriately, we may assume that columns of the same type

We may further reorder the columns so that they are arranged in four consecutive blocks based on the entries in the second and third rows. The matrix thus takes the form

$$H = \left(\begin{array}{cccccccccccc} & & & & & & & & & & & \\ +1 & \dots & +1 & +1 & \dots & +1 & +1 & \dots & +1 & +1 & \dots & +1 \\ +1 & \dots & +1 & +1 & \dots & +1 & -1 & \dots & -1 & -1 & \dots & -1 \\ +1 & \dots & +1 & -1 & \dots & -1 & +1 & \dots & +1 & -1 & \dots & -1 \\ * & \dots & * & * & \dots & * & * & \dots & * & * & \dots & * \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \dots & * & * & \dots & * & * & \dots & * & * & \dots & * \\ \underbrace{}_{a} & & & \underbrace{}_{b} & & & \underbrace{}_{c} & & & \underbrace{}_{d} & & \end{array} \right),$$

where a, b, c and d are the number of columns of the four types respectively.

Since there are m columns in total, we must have $a + b + c + d = m$. The orthogonality of the first two rows implies $a + b - c - d = 0$. Similarly, the orthogonality of the first and third rows requires $a - b + c - d = 0$, while the second and third rows give $a - b - c + d = 0$. Summing these four equations, we find $4a = m$, and hence m must be divisible by 4. □

REMARK 11. Note that there was nothing special about the second and third rows here; we could have used any two rows for the argument. Furthermore, one can solve the linear equations to find $a = b = c = d = \frac{m}{4}$.

7.3. Building Hadamard designs. We now demonstrate the connection between Hadamard designs and Hadamard matrices.

PROPOSITION 7. *A Hadamard design of order n (i.e., a 2-$(4n-1, 2n-1, n-1)$ design) exists if and only if a $4n \times 4n$ Hadamard matrix exists.*

PROOF. First suppose we have a normalised $4n \times 4n$ Hadamard matrix H, and let H' be the $(4n-1) \times (4n-1)$ submatrix obtained after deleting the first row and column. Let $M = \frac{1}{2}(H' + J)$, so that M is a $\{0,1\}$-matrix: every $+1$ becomes a 1 and every -1 becomes a 0. We claim that M is the incidence matrix of a Hadamard design.

Indeed, every column of H must have had $2n$ positive entries to be orthogonal to the positive first column. Since one of these entries was removed with the first row, it follows that every column of M has exactly $2n-1$ ones, and hence $k = 2n-1$. The proof of

Lemma 6, together with Remark 11, shows that any two rows of H, apart from the first, must share exactly n positive entries. Again, one is removed with the first column, and hence any two rows of M have $n-1$ ones in common. This therefore corresponds to a 2-design with $\lambda = n-1$. Since H', and therefore M, has $4n-1$ rows, we have $v = 4n-1$, giving the desired Hadamard design.

For the other direction, we observe that the above argument is reversible. If M is the incidence matrix of a 2-$(4n-1, 2n-1, n-1)$ design, let $H' = 2M - J$, and let H be obtained by adding a column and row whose entries are all $+1$. It can be easily checked that H must be a $4n \times 4n$ Hadamard matrix. □

As in the case of projective planes, then, we have translated our question about the existence of Hadamard designs into a question about the existence of Hadamard matrices. Lemma 6 shows that a Hadamard matrix necessarily has size either 1, 2 or a multiple of 4. It is conjectured that this is sufficient as well.

CONJECTURE 1. *For every $n \in \mathbb{N}$, a $4n \times 4n$ Hadamard matrix exists.*

This long-standing conjecture has attracted a lot of attention over the years, with numerous constructions having been found, some of which we shall meet in the next subsection. However, the conjecture itself remains wide open, with the first unknown case being that of 668×668 Hadamard matrices.

7.4. Constructing Hadamard matrices. We shall now show how one may construct Hadamard matrices of certain sizes, thereby resolving Conjecture 1 for some values of n, while also, via Proposition 7, providing Hadamard designs of the appropriate orders. Our first construction shows how one can build large Hadamard designs from smaller ones.

PROPOSITION 8. *If $m \times m$ and $n \times n$ Hadamard matrices exist, then an $mn \times mn$ Hadamard matrix also exists.*

PROOF. We construct the larger matrix using the *Kronecker product*, which we now introduce. Suppose A and B are $m \times m$ and $n \times n$ matrices respectively. The Kronecker product $A \otimes B$ is the $mn \times mn$ block matrix given by

$$\begin{pmatrix} a_{1,1}B & \dots & a_{1,m}B \\ \vdots & \ddots & \vdots \\ a_{m,1}B & \dots & a_{m,m}B \end{pmatrix}.$$

The key properties of the Kronecker product are that $(A \otimes B)^T = A^T \otimes B^T$ and, for an $m \times m$ matrix C and an $n \times n$ matrix D, $(A \otimes B)(C \otimes D) = AC \otimes BD$.

Given this, it follows that if A and B are Hadamard matrices, then so too is $A \otimes B$, since

$$(A \otimes B)(A \otimes B)^T = (A \otimes B)(A^T \otimes B^T) = AA^T \otimes BB^T = mI_m \otimes nI_n = mnI_{mn}. \qquad \square$$

We can already use this simple product to build an infinite sequence of Hadamard matrices, a construction due to Sylvester.

COROLLARY 8. *There exists a $2^m \times 2^m$ Hadamard matrix for all $m \geq 1$.*

PROOF. We have already seen a 2×2 Hadamard matrix H in Example 7. Starting with H, repeatedly taking Kronecker products with H gives Hadamard matrices of size 2^m for all $m \geq 2$. □

Hence, in order to prove Conjecture 1, it suffices to prove it for odd values of n, since all other sizes can be obtained by taking a Kronecker product with the appropriate $2^m \times 2^m$ Hadamard matrix. This leaves us with the task of finding Hadamard matrices of order 12, 20, 28, 36, and so on. Our next result resolves some of these cases.

THEOREM 6 (Paley, 1933). *A $4n \times 4n$ Hadamard matrix exists whenever $4n-1$ is a prime power.*

We first collect some useful information regarding squares in finite fields.

LEMMA 7. *Let p be an odd prime, $s \in \mathbb{N}$, and Q the set of non-zero squares in $\mathbb{F}_{p^s}$. Then*

(1) $|Q| = \frac{1}{2}(p^s - 1)$,
(2) if $p^s \equiv 1 \pmod 4$, then for all $x \in \mathbb{F}_{p^s} \setminus \{0\}$, $x \in Q$ if and only if $-x \in Q$, and
(3) if $p^s \equiv 3 \pmod 4$, then for all $x \in \mathbb{F}_{p^s} \setminus \{0\}$, $x \in Q$ if and only if $-x \notin Q$.

PROOF. We will use the algebraic fact that the multiplicative group of $\mathbb{F}_{p^s}$ is cyclic. In other words, there is a generator $\alpha \in \mathbb{F}_{p^s} \setminus \{0\}$ such that $\{\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{p^s-1}\} = \mathbb{F}_{p^s} \setminus \{0\}$. In particular, the map $m \mapsto \alpha^m$ must be a bijection between $[p^s - 1]$ and $\mathbb{F}_{p^s} \setminus \{0\}$.

By Fermat's Little Theorem, $\alpha^{p^s-1} = 1$. It follows that $Q = \{\alpha^2, \alpha^4, \ldots, \alpha^{p^s-1}\}$, since for any $x \in \mathbb{F}_{p^s} \setminus \{0\}$, we have $x = \alpha^m$ for some $m \in [p^s - 1]$, and thus $x^2 = \alpha^{2m} = \alpha^{2m'}$, where $2m' \equiv 2m \pmod{p^s - 1}$. Hence $|Q| = \frac{1}{2}(p^s - 1)$.

For (2) and (3), observe that $x^2 = 1$ is a quadratic polynomial, and hence can only have the two roots 1 and -1 in $\mathbb{F}_{p^s}$. Since $(\alpha^{\frac{1}{2}(p^s-1)})^2 = \alpha^{p^s-1} = 1$, and $\alpha^{\frac{1}{2}(p^s-1)} \neq \alpha^{p^s-1} = 1$, we must have $\alpha^{\frac{1}{2}(p^s-1)} = -1$. Hence, if $x = \alpha^m$, then $-x = \alpha^{m+\frac{1}{2}(p^s-1)}$.

When $p^s \equiv 1 \pmod 4$, $\frac{1}{2}(p^s - 1)$ is even. It follows that either m and $m + \frac{1}{2}(p^s - 1)$ are both even, in which case both x and $-x$ are in Q, or they are both odd, in which case neither of x nor $-x$ are in Q.

On the other hand, if $p^s \equiv 3 \pmod 4$, $\frac{1}{2}(p^s - 1)$ is odd. Thus m and $m + \frac{1}{2}(p^s - 1)$ have opposite parity, and so exactly one of x and $-x$ is in Q. □

We can now construct $4n \times 4n$ Hadamard matrices whenever $4n - 1$ is a prime power.

PROOF OF THEOREM 6. Suppose $4n - 1 = p^s$ for some $s \in \mathbb{N}$ and p an odd prime. We will construct a 2-$(4n - 1, 2n - 1, n - 1)$ Hadamard design. By Proposition 7, the existence of the claimed Hadamard matrix follows.

For the design, we take the ground set to be $X = \mathbb{F}_{p^s}$. As in Lemma 7, let Q be the set of non-zero squares; that is, $Q = \{y^2 : y \in \mathbb{F}_{p^s} \setminus \{0\}\}$. The blocks of the design will be all the translates of Q, so $\mathcal{D} = \{a + Q : a \in \mathbb{F}_{p^s}\}$.

We have $v = |X| = p^s = 4n - 1$, while Lemma 7 gives $k = |B| = |Q| = \frac{1}{2}(p^s - 1) = 2n - 1$ for every block $B \in \mathcal{D}$. To show that this is indeed the desired design, we need to show

that every pair of elements is contained in exactly $n-1$ blocks, which is the content of the following claim.

CLAIM 5. *Every pair $\{x, x'\}$ of distinct elements of X appears in exactly $n-1$ blocks.*

PROOF. Observe that x, x' both appear in the block $a+Q$ if and only if there are non-zero squares $q, q' \in Q$ such that $x - q = x' - q' = a$. Hence the number of blocks containing both x and x' is equal to the number of pairs $(q, q') \in Q^2$ such that $x - q = x' - q'$, since there can be at most one value of q' for each q, and x and q determine a uniquely.

Given such a pair (q, q'), we must have some $u, u' \in \mathbb{F}_{p^s} \setminus \{0\}$ such that $q = u^2$ and $q' = (u')^2$. In fact, we have four choices for u and u', since we may replace u with $-u$, and similarly for u'. Hence the number of blocks containing the pair $\{x, x'\}$ is equal to

$$\frac{1}{4}\left\{(u, u') \in (\mathbb{F}_{p^s} \setminus \{0\})^2 : x - u^2 = x' - (u')^2\right\}.$$

Rearranging this last equality, we must have $x - x' = (u')^2 - u^2 = (u' + u)(u' - u)$. Every solution gives, for some $\ell \in \mathbb{F}_{p^s} \setminus \{0\}$, a solution to the linear system

$$\begin{aligned} u' + u &= \ell, \text{ and} \\ u' - u &= \ell^{-1}(x - x'). \end{aligned}$$

There is a unique solution (u, u') for every choice of $\ell \in \mathbb{F}_{p^s} \setminus \{0\}$. However, we must discount the solutions for which $u = 0$ or $u' = 0$. If $u = 0$, then $\ell = u' = \ell^{-1}(x - x')$, and hence $\ell^2 = x - x'$. On the other hand, if $u' = 0$, then $\ell = u = -\ell^{-1}(x - x')$, and so $\ell^2 = -(x - x')$. Since $p^s = 4n - 1 \equiv 3 \pmod 4$, Lemma 7 implies that exactly one of these cases holds. Hence we lose two possible values of ℓ, since if ℓ is ruled out, then so too is $-\ell$.

This means the number of valid choices for ℓ, and hence the number of pairs (u, u') as above, is $p^s - 3 = 4n - 4$. Hence the number of blocks containing the pair $\{x, x'\}$ is a quarter of this quantity, or $n - 1$. □

This shows that these blocks give the needed design, finishing the proof of Theorem 6. □

REMARK 12. Some remarks on Theorem 6.

(i) This constructs $4n \times 4n$ Hadamard matrices for $n = 3, 7, 11$ and 15, amongst others, but not for, e.g., $n = 19$.

(ii) In the proof, it was crucial that the prime power p^s be congruent to 3 modulo 4, so that -1 was not a square. This ensured that every pair was covered exactly the same number of times. This fails if $p^s \equiv 1 \pmod 4$, which of course it must, since otherwise we would have a large Hadamard matrix whose size was not divisible by four, contradicting Lemma 6.

(iii) However, the set of blocks obtained with $p^s \equiv 1 \pmod 4$ is still quite regular, and very close to a design. Indeed, one can obtain a Paley design by cleverly defining new blocks over a ground set that is twice as large, as shown in the van Lint–Wilson textbook. This shows that there is a $4n \times 4n$ Hadamard matrix whenver $2n - 1$ is a prime power. This covers, for instance, the case $n = 19$.

8. The quest for simple designs

To close[38] our chapter on the theory of combinatorial designs, we return to Question 1, the fundamental question asking for which parameters we have a t-(n, k, λ) design. So far we have seen a number of non-existence results, including Fisher's Inequality (Proposition 3), the Wilson–Petrenjuk Inequalities (Theorem 4) and the Bruck–Ryser–Chowla Theorem (Theorem 2). We have also seen some constructions of designs, including the projective and affine planes (Section 4) and the Hadamard designs (Section 7).

Our most general existence result, though, is Wilson's theorem on general t-designs (Corollary 7). Recall that Wilson showed for any v, k and t, and λ sufficiently large, the necessary arithmetic conditions of Corollary 1 were also sufficient for the existence of a t-(v, k, λ) design. However, the designs obtained are somewhat unsatisfactory, as they are far from simple — we added many copies of the trivial design to construct these designs. Much subsequent focus, therefore, fell on the problem of determining when *simple* designs could be constructed, and we shall briefly[39] survey some of the highlights of this line of research.

The first result we present is another theorem of Wilson, this time showing the sufficiency of the arithmetic conditions for 2-designs.

THEOREM 7 (Wilson, 1975). *For all integers k and λ, and for every v sufficiently large ($v \geq v_0(k, \lambda)$) that satisfies the arithmetic conditions of Corollary 1, a 2-(v, k, λ) design exists.*

We will not get into the proof of Theorem 7 at all, save for the following brief remark. When v is a prime power, the desired design is constructed algebraically, using the finite field of order v. For the remaining values of v, there is no such finite field, and so a recursive construction is used instead. This combines smaller designs to build the design on a ground set of size v.

While this statement does not guarantee that the designs are simple, when we take $\lambda = 1$ (i.e., a Steiner system), the design is forced to be simple. This thus shows that the arithmetic conditions are sufficient for 2-designs when v is large enough.[40] We remark that in 1965, Hanani had shown that apart from 2-$(15, 5, 2)$ designs, which do not exist, the arithmetic conditions are also sufficient for 2-(v, k, λ) designs with $k \leq 5$.

This essentially settles the problem for 2-designs, which, as you will recall, were of primary importance in the early years of design theory. As interest grew in designs with larger strengths, only a sporadic sequence of Steiner systems with $t \geq 4$ were found. While some simple designs with $t \in \{5, 6\}$ were found, it was believed that there were no simple non-trivial designs with $t \geq 7$. However, the following remarkable result put paid to that misconception.

[38] Modulo next week's lecture on Kirkman's Schoolgirl Problem.

[39] Very, very, very indecently briefly, to be more accurate.

[40] Recall that Fisher's Inequality shows that some such condition is necessary.

THEOREM 8 (Teirlinck, 1987). *For $t \geq 0$, let*

$$\lambda = \prod_{j=1}^{t} \left(\operatorname{lcm}(2, 3, \ldots, j+1) \operatorname{lcm} \left(\binom{j}{1}, \binom{j}{2}, ..., \binom{j}{\lfloor j/2 \rfloor} \right) \right),$$ [41]

and suppose $v \geq t+1$ is such that $v \equiv t \pmod{\lambda}$. Then there is a simple t-$(v, t+1, \lambda)$ design.

Teirlinck thus proved the existence of simple designs of any strength. In fact, Teirlinck proved considerably more — he showed that the collection $\binom{X}{t+1}$ of all $(t+1)$-sets could be partitioned into $\frac{v-t}{\lambda}$ disjoint t-$(v, t+1, \lambda)$ designs. This forces the designs to be simple and, if $v \geq 2\lambda + t$, non-trivial.

This theorem was thus a sensation, but one drawback was that it only gives designs with $k = t+1$, and also the parameter λ is very large in terms of t. What happens when we have arbitrary (but fixed) t, k and v?

An important step was to loosen the requirements of a Steiner system. Rather than asking for every t-set to be covered exactly once by a collection of k-sets, one could instead ask for every t-set to be covered *at least* once. The natural extremal question is then how many k-sets are needed to cover all the t-sets. Clearly a Steiner system, if it exists, would be optimal, and in 1963, Erdős and Hanani conjectured that there was always a covering system whose size was asymptotically close to that of a Steiner system.[42]

This conjecture was proven in 1985 by Rödl, using the famous Rödl Nibble, which is a semi-random method. Essentially, he showed that one could construct asymptotically-optimal covering families by choosing the k-sets randomly.[43] This use of the probabilistic method in a construction is in sharp contrast with the very careful and precise algebraic constructions we have seen so far.

Very recently, Keevash made a hugely significant breakthrough, as shown below.

THEOREM 9 (Keevash, 2014+). *Given $k \geq t \geq 0$, and v sufficiently large ($v \geq v_0(k, t)$) satisfying the arithmetic conditions of Corollary 1, a t-$(v, k, 1)$ design exists.*

Here he shows that for any t and k, the necessary arithmetic conditions are again sufficient for the existence of Steiner systems, provided v is sufficiently large. This thus extends Theorem 7 to designs of arbitrary strength.[44] This theorem is a true *tour de force*, and we cannot do the proof justice here, but we remark that Keevash combines both the algebraic and probabilistic approaches to construct these designs. Roughly speaking, the idea is to first set aside a very precise algebraic construction, which will have a great deal of symmetry and

[41] Observe that this choice of λ ensures that the arithmetic conditions are satisfied.

[42] Note that for a covering system, there are no arithmetic conditions, so these will exist even when a Steiner system could not possibly exist. The conjecture states that there is a covering system that covers almost all t-sets exactly once (and is thus asymptotically as efficient as possible).

[43] The name "Nibble" comes from the fact that one cannot just choose all the sets in one go, but must select them in small random batches, thus attacking the problem with small "bites" at a time.

[44] Note that we can obtain simple t-(v, k, λ) designs by combining randomly-permuted copies of the Steiner system on the same ground set, as you did on Exercise Sheet 1.

regularity. From the remaining k-sets, one then takes a large random construction, which will be close to a Steiner system. However, there may be a few t-sets that are uncovered, and a few that are covered too many times. We then use the algebraic construction to fix the random sets (developing the methods of Theorem 5), until we obtain a true Steiner system. Following the appearance of Keevash's seminal paper, Glock, Kuhn, Lo and Osthus in 2016 published another proof of the same result, using purely combinatorial machinery.

It may seem that Theorem 9 completely settles the existence problem. While this is true in the asymptotic sense, one should note that the theorem requires v to be "sufficiently large." As our non-existence results have shown, it is for small values of the parameters (be it v, b or λ) that the arithmetic conditions may not be sufficient for the existence simple non-trivial t-(v, k, λ) designs. Since applications may indeed require the parameters to be too small for the general existence results to apply, the construction of small designs remains a problem of interest.

9. Kirkman's Schoolgirl Problem

This section was lectured by Simona Boyadzhiyska and Giulia Codenotti.

Recall that a Steiner triple system is a 2-$(v, 3, 1)$-design; that is, a collection of triples that covers every pair exactly once. The divisibility conditions of Corollary 1 imply that if a Steiner triple system exists, then $v \equiv 1, 3 \pmod 6$, and we have heard that this necessary condition is in fact sufficient as well. In this section we will further investigate the case $v \equiv 3 \pmod 6$ by considering Kirkman's famous Schoolgirl Problem.[45]

QUESTION 4 (Kirkman's Schoolgirl Problem, 1850). Suppose 15 schoolgirls walk to school in five rows of three, seven days a week. Is it possible that no two girls walk together in the same row twice?

We are thus interested in arrangements of 15 girls in blocks of three such that every pair appears at most once. However, over the course of the seven days, each girl walks alongside 14 other girls, and hence we must have every pair of girls appearing exactly once. Thus what Kirkman really asked for is a 2-$(15, 3, 1)$-design, with one additional property: the rows the girls walk in each day must form a perfect matching of the ground set.

DEFINITION 12. A design whose blocks can be partitioned into perfect matchings (so-called *parallel classes*) is called *resolvable*.

[45] Not only is this a fascinating name for a problem, but it has a fascinating history too! Kirkman — that is, Reverend (!) Thomas Penyngton Kirkman — posed this question as a problem in "The Lady's and Gentleman's Diary", a recreational mathematics magazine that ran for some thirty years in the mid 1800's. (What a time to be alive! Nowadays people post videos on YouTube of their friends struggling with, "Your sister was half your age when you were six. How old is she now that you are seventy?") The problem attracted a fair amount of attention, being worked on by the likes of Cayley and Sylvester, among others. There was also a priority dispute, with Sylvester claiming Kirkman his ideas, while Kirkman himself was dismayed that it was this problem for which he would be remembered, rather than the considerable paper he had written on combinatorics some years earlier.

EXAMPLE 8. We encountered a resolvable design in the first exercise on the second homework assignment.

We can now restate Kirkman's Schoolgirl Problem in our new terminology.

QUESTION 5. Does a resolvable 2-$(15, 3, 1)$ design exist?

As we shall soon see, such designs do indeed exist, and thus one may answer Kirkman's question in the affirmative.[46] In fact, as it turns out, there are precisely 7 non-isomorphic solutions. Their discovery led to greater interest in these special classes of designs, upon which Kirkman's name was bestowed.

DEFINITION 13. A resolvable 2-$(v, 3, 1)$ design is called a *Kirkman triple system* and is denoted by $\mathrm{KTS}(v)$

Ever curious, we are led to the natural existence question.

QUESTION 6. For which v do we have a $\mathrm{KTS}(v)$?

Since a Kirkman triple system is a Steiner triple system, we naturally require $v \equiv 1, 3 \pmod 6$. However, the existence of even a single perfect matching further necessitates $v \equiv 3 \pmod 6$. In fact, this trivially necessary condition turns out to also be sufficient. We will return to this at the end of this section, but we first provide some constructions.

9.1. Constructions of Kirkman triple systems. We now present two rather different constructions of Kirkman triple systems: the first will be geometric in nature, while the second is algebraic.

9.1.1. *A Geometric construction.* This construction bears some similarities to the affine spaces discussed in Section 4, although we shall wok in higher dimensions. Indeed, consider the n-dimensional space over $\mathbb{F}_3$, i.e. $\mathbb{F}_3^n$. Let the set of points $P = \mathbb{F}_3^n$ form the ground set for our design, and the set of lines

$$\mathcal{L} = \left\{ \{\vec{a} + \lambda\vec{b} \ : \lambda \in \mathbb{F}_3\} \ : \vec{a}, \vec{b} \in \mathbb{F}_3^n, \vec{b} \neq 0 \right\}$$

will be the blocks of the triple system.

CLAIM 6. *$\mathcal{L}$ forms a resolvable 2-$(3^n, 3, 1)$ design over the ground set P.*

PROOF. Note that P has 3^n elements, and every block in $\mathcal{L}$ has size 3. Every pair $\vec{x}, \vec{y}$ appears together in a block: we may take $\vec{a} = \vec{x}$ and $\vec{b} = \vec{y} - \vec{x}$. Furthermore, this block is unique, as two pairs $(\vec{a}_1, \vec{b}_1)$ and $(\vec{a}_2, \vec{b}_2)$ give the same block if and only if $\vec{b}_2 = c\vec{b}_1$ and $\vec{a}_2 = \vec{a}_1 + d\vec{b}_1$ for some $c, d \in \mathbb{F}_3$. It therefore follows that $\mathcal{L}$ is a 2-$(3^n, 3, 1)$ design.

We will now show that $\mathcal{L}$ is resolvable. For each $\vec{b} \in P \setminus \{\vec{0}\}$, consider the lines of slope $\vec{b}$,

$$\mathcal{B}_{\vec{b}} = \left\{ \{\vec{a} + \lambda\vec{b} \ : \ \lambda \in \mathbb{F}_3\} : \vec{a} \in \mathbb{F}_3^n \right\}.$$

[46] One may also answer it in the negative, but then one would be wrong.

Note that, by our earlier remark, $\mathcal{B}_{\vec{b}} = \mathcal{B}_{2\vec{b}}$.

Fix some $\vec{b} \in P \setminus \{\vec{0}\}$, and let B_1 and B_2 be two distinct blocks in $\mathcal{B}_{\vec{b}}$, with $B_i = \{\vec{a}_i + \lambda\vec{b} : \lambda \in \mathbb{F}_3\}$. If there is some $\vec{x} \in B_1 \cap B_2$, then $\vec{a}_1 + \lambda_1\vec{b} = \vec{x} = \vec{a}_2 + \lambda_2\vec{b}$, which implies $\vec{a}_2 = \vec{a}_1 + (\lambda_1 - \lambda_2)\vec{b}$, and thus $B_1 = B_2$, giving a contradiction. Hence any two blocks in $\mathcal{B}_{\vec{b}}$ are disjoint. Finally, for every $\vec{x} \in P$, by taking $\vec{a} = \vec{x}$ we have $\vec{x} \in \{\vec{a} + \lambda\vec{b} : \lambda \in \mathbb{F}_3\}$. Thus each $\mathcal{B}_{\vec{b}}$ is a perfect matching and so $\mathcal{L}$ is indeed a Kirkman triple system. □

EXAMPLE 9. Pictured below is the case $n = 2$, which gives rise to a resolvable 2-$(9, 3, 1)$ design, or a $\mathrm{KTS}(9)$. This corresponds to Kirkman's Schoolgirl Problem with just nine schoolgirls walking for four days. The lines below depict the rows in which they should walk, while the colours represent the different days.

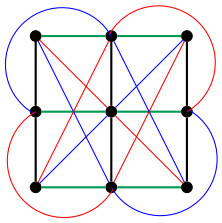

FIGURE 1. A geometric construction of a $\mathrm{KTS}(9)$.

9.1.2. *An algebraic construction.* While the construction on $\mathbb{F}_3^n$ is certainly a nice one, it only provides Kirkman triple systems over ground sets whose sizes are powers of three. In particular, it does not solve the original problem of Kirkman, which called for a design on 15 elements. Hence we now present an algebraic construction of a $\mathrm{KTS}(15)$.

DEFINITION 14. Consider $\mathbb{Q}$ and $\alpha_1, ..., \alpha_n \in \mathbb{C}$. Then $\mathbb{Q}(\alpha_1, ..., \alpha_n)$ is the smallest subfield of $\mathbb{C}$ that contains $\mathbb{Q}$ and $\alpha_1, ..., \alpha_n$.

EXAMPLE 10. $\mathbb{Q}(\sqrt{2}) = \{c + d\sqrt{2} \ : \ c, d \in \mathbb{Q}\}$, and $\mathbb{Q}(\sqrt{2}, 4, \sqrt{8}) = \mathbb{Q}(\sqrt{2})$.

Now consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$. Note that, for example $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}) \supseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \supseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}$. Now let $S = \{2^{a_1}3^{a_2}5^{a_3}7^{a_4} \ : a_i \in \{0, 1\}\} \setminus \{1\}$. One can show that

- K contains exactly 15 subfields of the form $\mathbb{Q}(\sqrt{d})$, one for each $d \in S$.
- For $d_1, d_2, d_3, d_4 \in S$ with $d_1 \neq d_2$, if $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) \subseteq \mathbb{Q}(\sqrt{d_3}, \sqrt{d_4})$, then $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) = \mathbb{Q}(\sqrt{d_3}, \sqrt{d_4})$.
- Each field of the form $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ contains exactly 3 subfields of the form $\mathbb{Q}(\sqrt{d})$, namely $\mathbb{Q}(\sqrt{d_1}), \mathbb{Q}(\sqrt{d_2})$ and $\mathbb{Q}(\sqrt{d_1 d_2})$.

Now, how many fields $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ does K contain?
Note that if $d_1, d_2 \in S$, there is a unique $d_3 \in S$ such that $\sqrt{d_1 d_2} = q\sqrt{d_3}$, for some $q \in \mathbb{Q}$.
For d_1, d_2, d_3 we have $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}) = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_3}) = \mathbb{Q}(\sqrt{d_2}, \sqrt{d_3})$. So there are $\binom{15}{2}/3 = 35$

such fields.
Define $(X, \mathcal{D})$ by $X = \{\mathbb{Q}(\sqrt{d}) : d \in S\}$ and $\mathcal{D} = \left\{\{\mathbb{Q}(\sqrt{d_1}), \mathbb{Q}(\sqrt{d_2}), \mathbb{Q}(\sqrt{d_1 d_2})\} \ : d_1, d_2 \in S\right\}$ (without multiplicity). This gives a 2-$(15, 3, 1)$ design. Moreover, as shown by the table below, this design happens to be resolvable.

Mon	Tue	Wed	Thu	Fri	Sat	Sun
2, 3, 6	2, 5, 10	2, 7, 14	2, 15, 30	2, 21, 42	2, 35, 70	2, 105, 210
5, 21, 105	3, 70, 210	3, 5, 15	3, 14, 42	3, 35, 105	3, 7, 21	3, 10, 30
7, 30, 210	6, 14, 21	6, 35, 210	5, 7, 35	5, 6, 30	5, 42, 210	5, 14, 70
10, 14, 35	7, 15, 105	10, 42, 105	6, 70, 105	7, 10, 70	6, 10, 15	6, 7, 42
15, 42, 70	30, 35, 42	21, 30, 70	10, 21, 210	14, 15, 210	14, 30, 105	15, 21, 35

Hence these sets of subfields $\{\mathbb{Q}(\sqrt{d_1}), \mathbb{Q}(\sqrt{d_2}), \mathbb{Q}(\sqrt{d_1 d_2})\}$ that correspond to the subfields $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ produce a $\mathrm{KTS}(15)$, solving Kirkman's Schoolgirl Problem. We would like to point out that extending this construction to one using n distinct primes gives an $\mathrm{STS}(v)$ for $v = 2^n - 1$. However, this design is not always resolvable.

9.2. Kirkman triple systems — the necessary condition is sufficient. In the previous subsection we gave a couple of constructions of Kirkman triple systems for some specific parameters. The question of which values of v admitted a resolvable triple system attracted a fair amount of attention. The aim of this section is to present Ray-Chaudhuri and Wilson's solution.[47]

THEOREM 10 (Ray-Chaudhuri–Wilson, 1971). *A Kirkman triple system* $\mathrm{KTS}(v)$ *exists if and only if* $v \equiv 3 \pmod 6$.

We have already observed the necessity of the condition $v \equiv 3 \pmod 6$. It therefore remains to construct a $\mathrm{KTS}(v)$ for every such v. Ray-Chaudhuri and Wilson achieved this in two stages. The first stage consisted of various explicit constructions, like the previous subsection. These were often algebraic in nature, using finite fields, and thus required v to be related to a prime power. For instance, they explicitly constructed a $\mathrm{KTS}(2q + 1)$ whenever q was a prime power, $q \equiv 1 \pmod 3$.

These explicit constructions served as the basic building blocks. To obtain Kirkman triple systems for all admissable values of v, the second stage of the proof consisted of a recursive construction, building large Kirkman tirple systems out of smaller ones. This required a slight generalisation of our notion of designs; given a set K, a t-(v, K, λ) is a collection of blocks that covers every t-set of the v elements exactly λ times, but instead of being uniform, the blocks can have any size that appears in K.

THEOREM 11. *Suppose there exists a* 2-$(3n+1, K, 1)$ *design, where* $K = \{k_1, \ldots, k_\ell\}$*, and further that we have a* $\mathrm{KTS}(2k_i + 1)$ *for every* $1 \leq i \leq \ell$*. Then there exists a* $\mathrm{KTS}(6n + 3)$.

[47] In lecture, this presentation was accompanied by a number of wonderfully explanatory blackboard images, which have regrettably not made their way into these notes. As a result of the lack of sketches, this subsection might appear rather sketchy.

The next result, which we shall not prove, shows the necessary generalised designs always exist, while also giving some explicit Kirkman triple systems needed to start the recursion.

THEOREM 12. *For every $n \geq 1$, there is a 2-$(3n+1, \{4, 7, 10, 19\}, 1)$ design. Moreover, there exist a* KTS(9)*, a* KTS(15)*, a* KTS(21) *and a* $KTS(39)$.

Clearly, Theorems 11 and 12 together imply Theorem 10. We conclude this section by giving the construction behind Theorem 11.

PROOF OF THEOREM 11. Let $(X, \mathcal{B})$ be the 2-$(3n+1, K, 1)$ design. Recall that $\mathcal{B}$ is a collection of blocks, whose sizes belong to $K = \{k_1, \ldots, k_\ell\}$, such that every pair of elements in X is covered by a unique block. Our goal is to construct $(S, \mathcal{T})$, a KTS$(6n+3)$ on $S = (X \times \{1, 2\}) \cup \{\infty\}$. Note that $|S| = 2|X| + 1 = 6n + 3$.

Now let $B \in \mathcal{B}$ be a block from the design, which must have some size $k_i \in K$. Note that $S(B) = (B \times \{1, 2\}) \cup \{\infty\} \subseteq S$ has size $2k_i + 1$, and hence we can take a KTS$(2k_i + 1)$ over the elements in $S(B)$, with blocks $\mathcal{T}(B)$. By naming elements in $(S(B), \mathcal{T}(B))$ appropriately, we can ensure that $\{(x, 1), (x, 2), \infty\} \in \mathcal{T}(B)$ for every $x \in B$.

Finally, take $\mathcal{T} = \bigcup_{B \in \mathcal{B}} \mathcal{T}(B)$. We claim that $(S, \mathcal{T})$ is a KTS$(6n+3)$.

We have already seen that $|S| = 6n + 3$, and evidently every block in $\mathcal{T}$ contains exactly three elements. We now show that $(S, \mathcal{T})$ is a Steiner triple system. To start, observe that for every $x \in X$, the pairs $\{(x, 1), (x, 2)\}$ and $\{(x, i), \infty\}$ are covered by the triples $\{(x, 1), (x, 2), \infty\}$. As this triple appears in every $\mathcal{T}(B)$ where $x \in B$, it follows that this is the unique triple covering these pairs.

Now suppose we have the pair $\{(x, i), (y, j)\}$ for some $x \neq y \in B$ and $i, j \in \{1, 2\}$. By virtue of the design properties of $(X, \mathcal{B})$, there is a unique block B containing both x and y. Hence the triples from $\mathcal{T}(B)$ are the only triples that could cover this pair. Since $(S(B), \mathcal{T}(B))$ is a Kirkman triple system, there is a unique block $T \in \mathcal{T}(B) \subseteq \mathcal{T}$ with $\{(x, i), (y, j)\} \subset T$.

Hence we have constructed a Steiner triple system, and it just remains to show that it is resolvable. To do so, we shall have to partition its blocks into $3n + 1$ parallel classes.

Notice that for each $B \in \mathcal{B}$, $(S(B), \mathcal{T}(B))$ is a Kirkman triple system, and hence $\mathcal{T}(B)$ can be partitioned into parallel classes. Each such parallel class can be labelled as $\mathcal{P}_x(B)$, where $x \in B$ is the unique element such that $\{(x, 1), (x, 2), \infty\} \in \mathcal{P}_x(B)$.[48] For $x \in X$, let $\mathcal{P}_x = \bigcup_{B \ni x} \mathcal{P}_x(B)$.

$\mathcal{P}_x$ clearly covers the elements $\infty, (x, 1)$ and $(x, 2)$, since $\{(x, 1), (x, 2), \infty\} \in \mathcal{P}_x(B)$ for every block B containing x. For any other element (y, i), there is a unique block B containing both x and y, and then (y, i) is covered by a unique block in $\mathcal{P}_x(B)$.

It follows that each $\mathcal{P}_x$ is indeed a parallel class, and hence $\{\mathcal{P}_x : x \in X\}$ shows that our Steiner triple system is resolvable, and is thus the desired Kirkman triple system. □

[48] The element ∞ must belong to a unique block in $\mathcal{P}_x(B)$, and the elements of $S(B)$ were named so that the blocks containing ∞ in $\mathcal{T}(B)$ were all of the form $\{(y, 1), (y, 2), \infty\}$ for $y \in B$.