BLOCK DESIGNS

October 28, 2020

0.1 INCIDENCE STRUCTURES (OR HYPERGRAPHS)

Definition 0.1 *An incidence structure (or: hypergraph)* is a triple $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$, where $\mathbf{P}$ and $\mathbf{B}$ are disjoint sets, I is a relation between the elements of $\mathbf{P}$ and $\mathbf{B}$, that is $I \subset \mathbf{P} \times \mathbf{B}$. The elements of $\mathbf{P}$ are called *points*, the elements of $\mathbf{B}$ are called *blocks*, I is the *incidence relation.* The elements of I (as ordered pairs) will be called *flags.*

Definition 0.2 Let $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ and $\mathbf{D}' = (\mathbf{P}', \mathbf{B}', I')$ be two incidence structures (hypergraphs). The mapping $\pi : \mathbf{P} \cup \mathbf{B} \to \mathbf{P}' \cup \mathbf{B}'$ is an *isomorphism,* if it is bijective and

$$\mathbf{P}^{\pi} = \mathbf{P}', \quad \mathbf{B}^{\pi} = \mathbf{B}';$$

$$pIB \iff p^{\pi} I' B^{\pi}, \ \forall p \in \mathbf{P}, \ \forall B \in \mathbf{B}.$$

We also say that $\mathbf{D}$ and $\mathbf{D}'$ are *isomorphic.* If $\mathbf{D} = \mathbf{D}'$, then π is called an *automorphism.*

Definition 0.3 The *dual* of $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ is $\mathbf{D}^* = (\mathbf{P}^*, \mathbf{B}^*, I^*)$, where $\mathbf{P}^* = \mathbf{B}$, $\mathbf{B}^* = \mathbf{P}$, and I^* is the inverse of I.

Definition 0.4 Let $p \in \mathbf{P}$ be a point. The *degree* of p is the number of blocks incident to it, that is

$$\deg(p) = \left|\{B \in \mathbf{B} \ : \ p \ I \ B\}\right|.$$

Similarly, the degree of a block is

$$\deg(B) = \left|\{p \in \ : \ p \ I \ B\}\right|.$$

It may happen that two different blocks are incident with the same set of points ("repeated blocks"). If this does not happen, then we call the hypergraph (incidence structure) *simple.* In this case we can identify the blocks with the set of points incident with them. More precisely, this means that $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ is isomorphic to $\mathbf{D}^* = (\mathbf{P}, \mathbf{B}^*, \in)$, where $\mathbf{B}^* = \{\{p : pIB\} \ : \ B \in \mathbf{B}\}$. We will almost exclusively deal with such simple structures. We can also call them *set systems.*

Definition 0.5 The pair $\mathcal{H} = (V(\mathcal{H}), E(\mathcal{H}))$ is a simple hypergraph, if the elemnts of $E(\mathcal{H})$ are subsets of $V(\mathcal{H})$. A hypergraph is *r-regular* is every point has degree r. It is called *k-uniform*, if every block has degree k.

We may note that the dual of a hypergraph will be simple if there are no points in the original structure that are incident with the same set of blocks.

Example 0.6 Let $\mathbf{P} = \{0, \ldots, 6\}$, and

$$\mathbf{B} = \{\{0,1,3\}, \{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,5,0\}, \{5,6,1\}, \{6,0,2\}\}.$$

Incidence is the relation $\in$. This structure is isomorphic to $\mathrm{PG}(2,2)$, and called the *Fano plane.*

Definition 0.7 Let $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ be a finite hypergaph. List the points: $p_1, \ldots, p_v$, and blocks: $B_1, \ldots, B_b$. The *incidence matrix* of $\mathbf{D}$ is the matrix $M = (m_{ij})$ $(i = 1, \ldots, v; j = 1, \ldots b)$, where

$$m_{ij} = \begin{cases} 1, & \text{if} \quad p_i \ I \ B_j \\ 0, & \text{otherwise.} \end{cases}$$

The *adjacency matrix* of $\mathbf{D}$ is $A = MM^T$, which is clearly symmetric. The element in row i and column j of A tells us how many blocks are incident with p_i and p_j. In particular, the main diagonal contains the degrees of the points.

Lemma 0.8 *For every incidence structure we have*

$$\sum_{p \in \mathbf{P}} \deg(p) = \sum_{B \in \mathbf{B}} \deg(B). \tag{1}$$

Proof. Count the flags (incident point-block pairs) in two ways. ∎

Corollary 0.9 *Let $\mathcal{H}$ be an r-regular, k-uniform hypergraph with v points and b blocks. Then $vr = bk$.* ∎

Definition 0.10 An incidence structure with the same number of points and blocks is called *square* (or sometimes *symmetric*).

1 BLOCK DESIGNS

Definition 1.1 The simple hypergraph $\mathbf{D} = (\mathbf{P}, \mathbf{B}, \in)$ is called a *block design*, more precisely a $2-(v,k,\lambda)$*-design* if it has v points, $(|\mathbf{P}| = v)$, k-uniform (that $\forall B \in \mathbf{B} : \ |B| = k$), moreover any two distinct points are contained in precisely λ blocks. If $\lambda = 1$, the block design is called a *Steiner system.*

If $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ contains repeated blocks, and satisfies the above requirements (has v points, every block is incident with k points, every pair of points is contained in λ blocks, the we call it a *(uniform) 2-*(v,k,λ)*-structure.* If the uniformity condition is also dropped, then we call it a 2*-structure.*

The next proposition shows that block designs are regular.

Proposition 1.2 *In a* $2-(v,k,\lambda)$ *design (and a 2-*(v,k,λ)*-structure) each point has degree* r*, where*

$$r = \lambda(v-1)/(k-1),$$

the number of blocks is

$$b = \lambda v(v-1)/(k(k-1)).$$

Proof. Fix a point p. Count the flags (q, L) in two ways, where $p \in L$, $q \in L$, $p \neq q$. This is on the one hand $\deg(p)(k-1)$, on the other hand (counting from point to point) it is $(v-1)\lambda$. This gives r in advance, the formula for b comes from using $bk = vr$ (see 0.9). ∎

Corollary 1.3 *For the existence of a* $2-(v,k,\lambda)$*-design it is necessary that*

$$\begin{array}{ll}(1) & \lambda(v-1) \equiv 0 \pmod{k-1}; \\ (2) & \lambda v(v-1) \equiv 0 \pmod{k(k-1)}.\end{array} \quad ∎$$

Already around 1850 the question of constructing $2-(v,k,\lambda)$-designs was posed. The main question is whether the above divisibility conditions are also sufficient.

We will first consider the simplest case $\lambda = 1$, $k = 3$. $2-(v,3,1)$-designs are also called *Steiner triple systems.* A Steiner triple system on v points will be denoted by STS(v). The divisibility conditions give $2|v-1$ and $6|v(v-1)$. So, Steiner systems can only exist if $v \equiv 1$ or $v \equiv 3 \pmod 6$. Our aim is to show that for every $v \equiv 1$ or $v \equiv 3 \pmod 6$ there is an STS(v).

Example 1.4 (Kirkman $v \to 2v+1$ construction.) This will be a recursive construction. We show that whenever there is an STS(v), then there is also an STS($2v+1$) $= S^*$, which contains the original STS(v) as a subsystem.

Actually, if we want to guarantee that STS(v) is a subsystem, then the construction can be figured out: If STS(v) $= S$ is a subsystem, then every block (triple) meets S in 0,1, or 3 points. The number of blocks meeting S in 1 point is $v(v+1)/2$, because the blocks through a fixed point of S partition $S^* - S$ in pairs. By counting the total number of blocks one can see that there are no blocks meeting S in 0 points. So, it is enough to define the blocks meeting S in 1 point. If we consider $S^* - S$ as the complete graph K_{v+1}, then the blocks through a fixed point form a perfect matching. For different points, these perfect matchings are disjoint (if they had a common edge, then the endpoints of that edge would determine 2 blocks). If we imagine the perfect matchings as colour classes, then this gives an edge colouring of K_{v+1} with v colours. (Note that v was either 1 or 3 modulo 6, so it is odd, hence $v+1$ is even and we learnt from graph theory that the edge chromatic number of the complete graph K_{v+1} is indeed v in this case.)

The actual construction is now a converse to this: take a colouring of the edges of K_{v+1} with v colours, and to each colour class associate a point of STS(v). The points of our STS($2v+1$) $= S^*$ will be the points of STS(v) and the points of K_{v+1}. The blocks are the blocks of STS(v) and the following sets: $\{p, v_1, v_2\}$, where p is a point of the STS(v) and $\{v_1, v_2\}$ is an edge belonging to the colour class associated with the point p. It is not difficult to check that with this definition there will be a unique block through every pair of points.■

Staring from the Fano plane we get an STS(15). However, Kirkman's construction is not enough to construct an STS(v) for every $v \equiv 1$ or $3 \pmod{6}$. The next construction will be an explicit one.

Example 1.5 (Skolem's constructions.) We first present it for $v = 6m+1$. In this case the number of blocks is $b = m(6m+1)$. The points are simply $0, 1, \ldots, 6m$. Let us arrange the points with one exception ($6m$) in the following matrix

$$\begin{array}{cccc|cccc}
0 & 1 & \ldots & m-1 & m & m+1 & \ldots & 2m-1 \\
2m & 2m+1 & \ldots & 3m-1 & 3m & 3m+1 & \ldots & 4m-1 \\
4m & 4m+1 & \ldots & 5m-1 & 5m & 5m+1 & \ldots & 6m-1
\end{array}$$

The blocks belong to three types:

(i) $\{i, 2m+i, 4m+i\}$, where $0 \le i \le m-1$

(ii) $\{m+i, 2m+i, 6m\}$, $\{3m+i, 4m+i, 6m\}$, $\{5m+i, i, 6m\}$, again for $0 \le i \le m-1$,

(iii) Those triples $\{a, b, c\}$, in which a and b are in the same row of the matrix above and c is in the next row (mod 3), moreover

> if $a + b$ even, then $2c \equiv a + b \pmod{2m}$, and c is in the first half of the row,
>
> if $a + b$ is odd, then $2c \equiv a + b - 1 \pmod{2m}$, and c is in the second half of the row.

One can also use Skolem's method for $v = 6m + 3$. Our matrix will be

$$\begin{array}{cccc} 0 & 1 & \dots & 2m \\ 2m+1 & 2m+2 & \dots & 4m+1 \\ 4m+2 & 4m+3 & \dots & 6m+2 \end{array}$$

the points are just $\{0, 1, \dots 6m + 2\}$ and there will be two types of blocks:

(i) "vertical blocks": $\{j, j + 2m + 1, j + 4m + 2\}$, $(j = 0, \dots, 2m)$.

(ii) $\{a, b, c\}$, where a, b are in the same row, c is in the next row and $2c \equiv a+b \pmod{2m+1}$.

In both cases it can be verified that we get an STS. Of course, the $6m + 1$ case is even more tedious. ∎

Let us also mention the results about small values of v: there is a unique STS(7), the Fano-plane, a unique STS(9), the affine plane AG(2, 3). There are two STS(13), and 80 STS(15). This shows that the number of pairwise non-isomorphic STS(v) grows fast (compared to v).

If k gets larger, then the situation becomes more difficult. For $k = 4$, we get $v \equiv 1$ or $4 \pmod{12}$, and Hanani showed that for every such v there is a $2-(v, 4, 1)$ Steiner-system. For $k = 5$, the necessary condition gives $v \equiv 1$ or $5 \pmod{20}$, and again there is a Steiner system. This is due to Hanani, Wilson and Ray-Chaudhuri. The case $k = 6$ is open. In general, asymptotic existence is known (Wilson), so when v is large enough compared to k, then there is a $2 - (v, k, 1)$ Steiner-system.

Let us see further examples of block designs.

Example 1.6 Let $\mathcal{P}$ be a projective plane of order n. Then it is a $2 - (n^2 + n+1, n+1, 1)$ design. This is essentially equivalent to the axiomatic definition of projective planes (so could be an alternative definition).

Example 1.7 Let $\mathcal{A}$ be an affine plane of order n. Then $\mathcal{A}$ is a $2 - (n^2, n, 1)$ design. This is essentially equivalent to the axiomatic definition of affine planes (so could be an alternative definition).

More generally, projective and affine spaces also give examples of designs.

Example 1.8 Let Σ be the projective space $\mathrm{PG}(n,q)$. Define a hypergraph in which the points are the points of Σ, the blocks are the d-dimensional subspaces of Σ (for some fixed $1 \leq d \leq n-1$). This will be a block design with parameters

$$v = \frac{q^{n+1}-1}{q-1}, \quad k = \frac{q^{d+1}-1}{q-1},$$

$$\lambda = \frac{(q^{n-1}-1)(q^{n-2}-1)\dots(q^{n-d+1}-1)}{(q^{d-1}-1)\dots(q-1)}.$$

It will be denoted by $\mathrm{PG}_d(n,q)$. (Note that it will be a square design (that is $v=b$) if $d=n-1$, in other words, when the blocks are the hyperplanes.

Remark 1.9 The expression for λ is the so-called Gaussian binomial coefficient

$$\begin{bmatrix} n \\ d \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-d+1}-1)}{(q^d-1)(q^{d-1}-1)\dots(q-1)}.$$

From linear algebra we know that it gives the number of d-dimensional subspaces in an n-dimensional vector space. Using this notation the parameters of $\mathrm{PG}_d(n,q)$ are

$$v = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q; \quad k = \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q, \quad \lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q.$$

The other parameters (r,b) can also be given easily:

$$r = \begin{bmatrix} n \\ d \end{bmatrix}_q; \quad b = \begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q.$$

Example 1.10 We can copy the previous example for affine spaces. The design $\mathrm{AG}_d(n,q)$ has the points of the affine space as points, blocks are d-dimensional affine subspaces (that is cosets of vector subspaces). The parameters are

$$v = q^n, \quad k = q^d, \quad \lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q,$$

$$r = \begin{bmatrix} n \\ d \end{bmatrix}_q, \quad b = q^{n-d} \begin{bmatrix} n \\ d \end{bmatrix}_q.$$

There are other geometric, algebraic etc. constructions of block designs. However, in the examples the parameter λ grows fast. For the existence, we know the following asymptotic result.

Theorem 1.11 (Wilson's theorem) *If k and λ are fixed, then there is a v_0 so that for every $v > v_0$ satisfying the conditions in 1.3, there is a $2-(v,k,\lambda)$ design.*

2 FISHER'S INEQUALITY

Theorem 2.1 (Fisher's inequality) *If $k < v$ in a $2-(v,k,\lambda)$ design, then $b \geq v$.*

Proof. Consider the adjacency matrix A of the design. This matrix has r in the main diagonal, λ elsewhere. We wish to show, that it is non-singular. To do this, we will compute its determinant. Subtract the first row from the others. Then we keep the first row and will have $r-\lambda$ in the main diagonal. The first column becomes $\lambda - r$. Add all the columns to the first one. Then the matrix will be upper triangular. The first element in the first row will be $r+(v-1)\lambda$. This implies that A is non-singular, so it has rank v. As A is MM^T, M (and M^T) also has rank v, so b cannot be smaller than v. This shows $b \geq v$. ∎

Let us see another useful way to compute the determinant of the adjacency matrix. J will always denote the all-1 matrix.

Lemma 2.2 $\det(xI + yJ) = (x+yn)x^{n-1}$ *(I, J are $n \times n$ matrices).*

Proof. The all-1 vector $\mathbf{j}$ is an eigenvector of $A = xI + yJ$, the corresponding eigenvalue is $x+yn$. A is symmetric, so it has an orthonormal basis consisting of eigenvectors, actually, $\mathbf{j}$ can be one of the basis vectors. The other elements $\mathbf{v}$ of the basis are perpendicular to $\mathbf{j}$, so we have $\mathbf{v}J = 0$. From this $\mathbf{v}(xI+yJ) = x\mathbf{v}$ follows, which implies that x is an eigenvalue with multiplicity $(n-1)$. ∎

Corollary 2.3 *The adjacency matrix of a non-trivial ($k < v$) block design has determinant $rk(r-\lambda)^{v-1}$. So the rank of the adjacency matrix is v.*

Proof. We saw that $\det(MM^T) = (r-\lambda)^{v-1}(r+(v-1)\lambda)$. Using 1.3 we see that $(v-1)\lambda) = (k-1)r$, so $(r+(v-1)\lambda) = rk$. ∎

In the extremal case $b = v$ we get further nice properties.

Theorem 2.4 *For a non-trivial ($k < v$) block design the following are equivalent:*

(a) $b = v$;

(b) $r = k$;

(c) every two distinct blocks have λ points in common;

(d) every two distinct blocks have the same number (say μ) of common points.

Proof. The equivalence of (a) and (b) is trivial because of $vk = br$. To prove (c), we will compute M^TM. If $r = k$, then $v = b$ and $MJ = JM$, so M can be interchanged with $MM^T = \lambda J + (r-\lambda)I$, hence $M^2M^T = MM^TM$. As MM^T is non-singular, M is also non.singular, it has an inverse M^{-1}. So $M^TM = M^{-1}MM^TM = M^{-1}M^2M^T = MM^T$. So we get $MM^T = M^TM$. The elements of the matrix M^TM (sometimes called the block adjacency matrix) are the intersection sizes $|B \cap B'|$, so every two distinct blocks intersect in λ points. So (b) implies (c). (c)→(d) is trivial. If (d) holds, then the dual of the block design is also a block design (v and b are interchanged and we have μ as λ in the dual). Applying Fisher's inequality for the original block design gives $b \geq v$, applying it to the dual design gives $v \geq b$. Hence $b = v$, which is (a). ∎

3 t-DESIGNS

Definition 3.1 The simple incidence structure $\mathbf{D} = (\mathbf{P}, \mathbf{B}, I)$ is called a $t-(v,k,\lambda)$ *design*, ($v > k > 1$, $k \geq t \geq 1$), if the number of points is v, every block is incident with k points and every t distinct points are in precisely λ blocks. If repeated blocks are allowed then we call it a (uniform) $t-(v,k,\lambda)$ *structure.*

For $t = 2$ we get the notion of designs back and for $t = 1$ this definition just gives regular, uniform hypergraphs.

Let us start with the necessary divisibility conditions for t-designs, generalizing Corollary 1.3.

Proposition 3.2 *If there exists a $t-(v,k,\lambda)$ design, then for every $i = 0, 1, \ldots, t-1$,*

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

is an integer.

Proof. The number λ_i is the number of blocks thtough a set I of i points. Indeed, let us add $t-i$ points to I to get t distinct points. After adding these points there are λ block thorugh the t points. These $t-i$ points can be chosen in $\binom{v-i}{t-i}$ ways. We obtain the same block $\binom{k-i}{t-i}$ times, so we have to divide with this. ∎

If we put $i = t-1$, then we get $k-t+1|\lambda(v-t+1)$. For $i = 0$ we get the number of blocks, b, for $i = 1$, we get r.

This result also shows that a $t-(v,k,\lambda)$ design is also an $i-(v,k,\lambda_i)$-design (with the same set of points and blocks).

Example 3.3 1) If **B** is the set of all k-element subsets of **P** then we get the a k-uniform hypergraph, which is a t-design for every $t \leq k$, the value of λ is $\lambda = \binom{v-t}{k-t}$. This is a trivial example, and will be excluded most of the time.

2) The affine space $\mathrm{AG}_2(n, 2)$ $(n \geq 3)$ is a $3-(2^n, 4, 1)$ design.

There are other geometric examples, circle geometries give $3-(q^2+1, q+1, 1)$-designs.

It is in general diffucult to construct non-trivial t-designs with large t. The situation is simpler if we allow repeated blocks.

Theorem 3.4 *Assume $t < k < v - t$. Then for a suitable λ there is a $t-(v, k, \lambda)$-structure, in which not all k-element subsets are blocks.*

We skip the proof.

Later we will see the so-called Witt designs connected to the Golay codes, which have $t = 4, 5$. For quite a while there were no non-trivial t-designs known for $t \geq 6$. The first examples with $t = 6$ were constructed by Magliveras and Leavitt (in the seventies). Then Luc Teirlinck showed that t can be arbitrary large (in the eighties).

Theorem 3.5 (Teirlinck's theorem.) *For a given t let*

$$\mu = \prod_{i=1}^{t} \left(\left[\{ \binom{i}{n} \ : \ n = 1, \ldots, i \} \right] \cdot [\{1, \ldots, i+1\}] \right).$$

Then for every $v \equiv t \pmod{\mu}$ the $(t+1)$-element subsets of a v-element set X can be partitioned into $t-(v, t+1, \mu)$-designs. In particular, there exist $t-(v, t+1, \mu)$-designs if $v \equiv t \pmod{\mu}$, $\lambda \equiv 0 \pmod{\mu}$, and $v > \lambda + t$. ∎

The proof is difficult. The symbol $[,]$ denotes the least common multiple in the formula. There is a very recent, incredibly strong result by Peter Keevash, who proved the analogue of Wilson's theorem for t-designs: *if all the divisibity conditions in Proposition 3.2 are satisfied and v is large enough compared to t, k, λ, then there exists a $t-(v, k, \lambda)$ design.*

The famous Fisher inequality was extended to t-designs by Ray-Chaudhuri and Wilson.

Theorem 3.6 *Let **D** be a $t-(v, k, \lambda)$-design, where $t = 2s$ and $k \leq v - s$. Then $b \geq \binom{v}{s}$.*

Note that the same holds for $t = 2s + 1$, since a $(2s+1)$-design is automatically a $2s$-design. Ray-Chaudhuri and Wilson also proved a dual result. We state it without proof.

Theorem 3.7 (Ray-Chaudhuri, Wilson) *Let $s \leq k \leq v - s$ and let $\mathbf{B}$ be a system of k-element subsets of a set V $(|V| = v)$, for which $|B \cap B'|$ takes at most s values (for $B \neq B' \in \mathbf{B}$). Then $\mathbf{B} \leq \binom{v}{s}$.* ∎

4 SQUARE DESIGNS

Let us recall that a block design is square if $b = v$, or equivalently if $r = k$. For square designs er have that two distinct block meet in λ points. We also saw in Lemma 2.2 that $\det(MM^T) = rk(r - \lambda)^{v-1}$ for the incidence mnatrix M.

Using $k = r$ and $\det(M)$ =$\det(M^T)$ we get

$$(\det(M))^2 = (k - \lambda)^{v-1}k^2.$$

Corollary 4.1 (Schützenberger) *If there is a a square $2-(v, k, \lambda)$-design, then $(k - \lambda)^{v-1}$ is a square. If v is even, then $k - \lambda$ has to be a square.* ∎

Definition 4.2 For a square $2 - (v, k, \lambda)$-design we call $n = (k - \lambda)$ the *order* of the (square) design.

The next theorem will give a necessary condition for the existence of a square design if v is odd.

Theorem 4.3 (Bruck–Chowla–Ryser) *Assume that v is odd and there is a square $2 - (v, k, \lambda)$-design. Then the diphantine equation*

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

has a non-trivial integer solution.

Non-trivial means that the solution is different from $x = y = z = 0$. The proof is difficult and is omitted.

For projective planes, the condition is very simple. This was proved by Bruck and Ryser one year before the Bruck, Chowla, Ryser theorem above.

Theorem 4.4 *If there is a projective plane of order n (a square $2-(n^2+n+1, n+1, 1)$ design) and $n \equiv 1$ or $2 \pmod 4$, the n can be written as the sum of two integer squares.*

The theorem rules out the existence of a plane of order 6. It leaves open the case $n = 10$ but Lam, Swiercz and Thiel showed (using a computer) that there is no plane of order 10. So far, this is the only example known, when the square design could exist but it does not exist.

Example 4.5 The design $\mathrm{PG}_{n-1}(n,q)$ is a square design. The parameters are $v = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q$, $k = \begin{bmatrix} n \\ 1 \end{bmatrix}_q$, and $\lambda = \begin{bmatrix} n-1 \\ n-2 \end{bmatrix}_q = \begin{bmatrix} n-1 \\ 1 \end{bmatrix}_q$.

In the particular case when $n = 2$, we have $\lambda = 1$. In general, axiomatically defined projective planes of order n are square designs with $\lambda = 1$ (so there are infinitely many of them). For $\lambda > 1$ it is not known whether there infinitely many square designs with the given λ.

4.1 HADAMARD MATRICES AND DESIGNS

An important infinite family of square designs is the family of Hadamard designs.

Definition 4.6 A block design with parameters $2-(4\lambda+3, 2\lambda+1, \lambda)$ is called an *Hadamard design.*

Note that such a design has $b = v$, because $b = \lambda v(v-1)/k(k-1)$.

Definition 4.7 An $n \times n$ matrix H is called an *Hadamard matrix* if every element of H is ± 1 and $HH^T = nI$.

Note that from $HH^T = nI$ it follows that $H^T H = nI$. The terminology is motivated by the following inequality of Hadamard for certain determinants:

If we have $|a_{ij}| \leq 1$ for the elements of an $n \times n$ matrix A, then det$(A) \leq n^{n/2}$ and we have equality in this bound if and only if the matrix is an Hadamard matrix.

The intuitive content of the inequality is that the maximum volume of a parallelotop is attained for the cube.

Example 4.8 The design $\mathrm{PG}_{n-1}(n,2)$ is an Hadamard design.

Example 4.9 The following matrices

$$(1)\,, \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{és} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

are Hadamard matrices.

In general, except for the first two examples above, the order of an Hadamard matrix is always divisible by 4. To see this, observe that we can multiply any row or column of an Hadamard matrix by -1 and the resulting matrix will also be an Hadamard matrix. Besides this we can also permute the rows and columns without losing the Hadamard property. Using these transformations, we may assume that the first row and column consists of $+1$'s, and in the second row first we have m times $+1$, and then $n-m$ -1's. Since the first and second row are orthogonal, the number $n = 2m$, and in the second row we have m $+1$'s and then m -1's. If there is another row (so $n > 2$), then let us denote by x the number of $+1$'s in the first m positions. Since this row is orthogonal to the first row, the number of $+1$'s in the second m positions is $m - x$. Hence the scalar product of the second and third row is $x \cdot 1 + (m-x)(-1) + (m-x)(-1) + x \cdot 1 = 0$. This gives $4x - 2m = 0$, so m is even and $n = 2m$ is divisible by 4. This proves the next theorem.

Theorem 4.10 *The order of an Hadamard matrix is 1,2 or divisible by 4.* ∎

Let us remark that for every two rows of an Hadamard-matrix there are m columns, where they both have a $+1$, m columns, where they both have a -1, and similarly the patterns $+1, -1$ and $-1, +1$ occur m times.

It is an important open conjecture that for every n divisible by 4, there is an Hadamard matrix of order n. The smallest value for which an $n \times n$ Hadamard matrix is not known, is $n = 428$.

The next theorem shows the relation between Hadamard matrices and Hadamard designs.

Theorem 4.11 *There is a $4n \times 4n$ Hadamard matrix, if and only if there is an Hadamard design with parameters $2-(4n-1, 2n-1, n-1)$.*

Proof. By the comments before Theorem 4.10 we may assume that the first row and column consist of $+1$'s. In the remaining $(4n-1) \times (4n-1)$ matrix replace the -1's by 0. The resulting matrix is the incidence matrix of an Hadamard design. Indeed $v = 4n - 1$ and $k = 2n - 1$ are immediate. We have to show that any two rows contain precisely $n-1$ common $+1$'s (columns where we have $+1$ in both rows), because in the original Hadamard matrix there were m such columns (including the first one which was deleted).

The other direction is similar, if we take two rows of the adjacency matrix, then there are $n-1$ columns, where they both have a $+1$. There are $r - \lambda = n$ columns, where one of the rows contains a 1, the other one a 0. If we add a first row and column, consisting only $+1$'s, then we can see that each pattern $(0-0, 1-0, 0-1, 1-1)$ occurs n times, hence after replacing the 0's by -1, we get that the rows are orthogonal. ∎

The next construction is a recursive one.

Proposition 4.12 *If H_n is an $n \times n$ Hadamard matrix, H_m is an $m \times m$ Hadamard matrix, then their Kronecker product $H_n \otimes H_m$ is also an Hadamard matrix.*

We just have to recall the definition of the Kronecker product.

Starting from a 2×2 Hadamard matrix and applying the previous construction repeatedly we get an Hadamard matrix for every power of 2. This construction is due to Sylvester and one can show that the Hadamard design corresponding to it is the projective space $\mathrm{PG}(n, 2)$.

Let us see now an explicit construction using finite fields. It gives an Hadamard matrix for $n = 12$ (the first value not covered by Sylvester's construction).

Example 4.13 Let $q \equiv 3 \pmod 4$ be a prime power. Let F be $\mathrm{GF}(q)$, and S be the set of non-zero squares. Define $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ in the following way:

Let $\mathbf{P} = F$, $\mathbf{B} = \{S + x \ : \ x \in F\}$. This is an Hadamard design, and the construction is called *Paley's construction.*

The parameters are $v = q$, $k = (q-1)/2$, $\lambda = (q-3)/4$. The existence of λ is not trivial; we will sketch the proof. We have to show that every pair a, b is contained in the same number of blocks. The set of blocks is invariant under translation, so it is enough to show this for a pair $0, a$. Multiplication by a square is also an automorphism of the structure, so it is enough to consider a square a and a non-square a. They are $+1$ and -1. $0, 1 \in S + u$, if there is a non-zero square x^2 such that $0 = x^2 + u$ and another y^2 which satisfies $1 = y^2 + u$. Subtracting these two equations gives $1 = y^2 - x^2$. If we do the same with -1 instead of 1, then we get the equation $-1 = y^2 - x^2$. In both cases $x, y \neq 0$, so the two equations are essentially the same, they clearly have the same number of solutions. This shows that λ exists. The structure satisfies $v = b$, so λ can be computed and we indeed get $\lambda = (q-3)/4$.

Definition 4.14 *Let* $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ *be a* $t - (v, k, \lambda)$ *design,* P *be a point. The design* $\mathbf{D'}_P = (\mathbf{P} \setminus \{P\}, \{B \setminus \{P\} : B \in \mathbf{B}, P \in B\})$ *is called the* derived design *of* $\mathbf{D}$*. It is easy to see that* $\mathbf{D'}_P$ *is a* $(t-1) - (v-1, k-1, \lambda)$ *design.*

The converse of derivation is more interesting, we will call it *one point extension* of a design. This is sometimes a good method to construct a design with large(r) t.

Definition 4.15 *Let* $\mathbf{D} = (\mathbf{P}, \mathbf{B})$ *be a* $t - (v, k, \lambda)$ *design,* $\infty \notin \mathbf{P}$ *be a new point. A design* $\mathbf{D}^* = (\mathbf{P} \cup \{\infty\}, \mathbf{B}^*)$ *is called a* one point extension *of* $\mathbf{D}$ *if the derived design of* $\mathbf{D}^*$ *with respect to* ∞ *is* $\mathbf{D}$*. It is easy to see that* $\mathbf{D}^*$ *is a* $(t+1) - (v+1, k+1, \lambda)$ *design, if it exists.*

The difficulty in constructing a one point extension is that we only know that the blocks containing ∞ are $B \cup \{\infty\}$, for the blocks of $\mathbf{D}$, which is typically a small fraction of the blocks. This immediately gives a necessary condition for a design to have a one point extension.

Proposition 4.16 *If a* $2-(v,k,\lambda)$ *design has a one point extension, then* $k+1$ *divides* $b(v+1)$.

Proof. We use the notation in the above definition and write a $*$ to the parametrs of $\mathbf{D}^*$. As the number of blocks in $\mathbf{D}^*$ containing ∞ is b, we have $r^* = b$. As $v^*r^* = k^*b^*$, $v^* = v+1$, and $k^* = k+1$, we indeed get that $k+1$ divides $b(v+1)$. ∎

Corollary 4.17 *If a projective plane of order* n *(a* $2-(n^2+n+1,n+1,1)$ *design) has a one point extension, then* $n = 2,4$.

Proof. The divisibility condition gives $n+2|(n^2+n+2)(n^2+n+1)$. Consider the right hand side modulo $n+2$, we get that it is $4\cdot 3$. So $n+2$ divides 12, from which $n = 2,4$ or 10. As there is no projective plane of order 10, we have $n = 2,4$. ∎

For $n = 4$, ther is a one-point extension, we will see it at the Golay codes. The Fano plane is an Hadamard design (with $\lambda = 1$), so the extendability follows from the next theorem.

Theorem 4.18 *Let* $\mathbf{D}$ *be an Hadamard design with parameters* $2-(v = 4\lambda+3, k = 2\lambda+1, \lambda)$. *Then it has a one point extension, which is a* $3-(4\lambda+4, 2\lambda+2, \lambda)$ *design.*

Proof. Let us add a new point ∞. The new blocks are $B\cup\{\infty\}$ and the complements of the blocks, that is $\mathbf{P}\setminus B$, for blocks $B\in\mathbf{B}$. We have to prove that for every 3 points there are λ new blocks containing them. This is trivial if one of the points is ∞. If not, then in the original Hadamard design we have to determine how many blocks contain all three points P_1, P_2, P_3 and how many contain none of them. Let us denote these numbers (for the given points P_1, P_2, P_3) by c_3 and c_0 respectively. Using the principle of inclusion-exclusion we get

$$c_0 = b - 3r + 3\lambda - c_3.$$

Since $b = v = 4\lambda+3$, $r = k = 2\lambda+1$, we indeed get that $c_0 + c_3 = \lambda$. ∎

Let us remark, that affine planes $\mathrm{AG}(2,q)$ have a one point extension (these are the “circle geometries” mentioned earlier).