This set of notes is dedicated to the study of combinatorial structures that are somehow related to codes.

1. Designs

A design is a system of subsets of a set satisfying certain regularity conditions; we'll use the following special case:

Definition 1. *A $t-(v,k,\lambda)$ design is defined by a pair $(S,\mathcal{B})$, where S is the set of points, and $\mathcal{B}$ q family of subsets of S, called blocks, satisfying*

- $|S| = v$;
- $|B| = k$, *for each block* $B \in \mathcal{B}$;
- *for each* $T \subset S$ *such that* $|T| = t$, $T \subset B$ *for exactly* k *blocks.*

In the case $\lambda = 1$, these designs are also called **Steiner systems** and denoted $S(t,k,v)$.

A design $(S,\mathcal{B})$ may be represented by an **incidence matrix** with columns indexed by S and rows indexed by the $\mathcal{B}$, such that the entry (B,x) is 1 if $x \in B$ and 0 otherwise. In the first case we say that x and B are incident, generalizing the notion of incidence used for graphs.

Definition 2. *A design is called* ***symmetric*** *if its incidence matrix is square. Two designs with incidence matrices N and N' are* ***isomorphic*** *if there exist permutation matrices P and Q such that*

$$N' = PNQ.$$

We state some basic results:

Proposition 3. *The number $b = |\mathcal{B}|$ of blocks of a $t-(v,k,\lambda)$ design is*

$$b = \lambda \frac{\binom{v}{t}}{\binom{k}{t}}.$$

Proof. (**HW**): count in two ways the number of pairs (T,B) where T is a t-subset of S and $B \in \mathcal{B}$ a block containing T. □

Proposition 4. *Fix a i-subset I of S. The number λ_i of blocks of a $t-(v,k,\lambda)$ design that contain I is*

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

In particular any $t-(v,k,\lambda)$ design is also a $i-(v,k,\lambda_i)$ design for any $i \leq t$.

Proof. (**HW**): similar to the previous proof, only considering t-subsets of S that contain I. □

Proposition 5. *Fix a j-subset J of S, with $j \leq t$. The number λ^j of blocks of a $t-(v,k,\lambda)$ design that are disjoint from J is*

$$\lambda^j = \lambda \frac{\binom{v-j}{k}}{\binom{v-t}{k-t}}.$$

Proof. (**HW**): this is a consequence of the previous proposition, with a double application of the Principle of Inclusion-Exclusion. Use Inclusion-Exclusion, the previous proposition and a general equality of binomial coefficients to prove that

$$\lambda^j = \sum_{l=0}^{j} (-1)^l \binom{j}{l} \lambda_l = \frac{\lambda}{\binom{v-t}{k-t}} \sum_{l=0}^{j} (-1)^l \binom{j}{l} \binom{v-l}{k-l};$$

then compute, again by Inclusion-Exclusion, the number of k-subsets of S disjoint from J. □

Exercise 6. *Prove the last proposition more directly: show that λ^j depends on the design parameters and j but not on the particular set J, and count in two ways the pairs (J, B) where J is a j-subset of S nd $B \in \mathcal{B}$ is disjoint from J.*

Exercise 7. *Show that there exist no $2-(90,5,2)$ or $4-(10,5,5)$ designs.*

The parameters λ_i and λ^j of a $t-(v,k,\lambda)$ design are used in the following definition.

Definition 8. *Let $(S, \mathcal{B})$ be a $t-(v,k,\lambda)$ design.*

- *The **complementary design** for $(S, \mathcal{B})$ is $(S, \mathcal{B}')$ where*

$$\mathcal{B}' = \{S \setminus B : B \in \mathcal{B}\};$$

  it is a $t-(v, v-k, \lambda^t)$ design.
- *Let $I \subset S$, with $|I| = i < t$. The **derived** design of $(S, \mathcal{B})$, with respect to I, is the design $(S \setminus I, \mathcal{B}_I)$, where*

$$\mathcal{B}_I = \{B \setminus I : I \subset B \in \mathcal{B}\};$$

  it is a $(t-i)-(v-i, k-i, \lambda)$.

Exercise 9. *Confirm the parameters of the complementary and derived designs.*

Exercise 10. *Let $(S, \mathcal{B})$ be a $t-(v,k,\lambda)$ design, I a i-subset of S and J a j-subset of S with $i+j \le t$, $0 < j$. Show that number λ_i^j of blocks $B \in \mathcal{B}$ containing I and disjoint from J satisfies*

$$\lambda_i^j = \lambda \frac{\binom{v-i-j}{k-i}}{\binom{v-t}{k-t}}, \qquad \lambda_i^j = \lambda_i^{j-1} - \lambda_{i+1}^{j-1}.$$

Exercise 11. *Let $(S, \mathcal{B})$ be a $t-(v,k,\lambda)$ design and J a j-subset of S with $j \le t$. Determine the parameters of the **residual design** for $(S, \mathcal{B})$ with respect to J whit set of points $S \setminus J$ and set of blocks*

$$\{B \in \mathcal{B} : J \cap B = \emptyset\}.$$

The following exercise gives an example of a design constructed from graph:

Exercise 12. *K_n denotes the simple complete graph with n vertices.*
Let S be the set of edges of K_6 and define the blocks to be the subsets of 3 edges that form either a triangle or a perfect matching (ie, they are mutually disjoint). Show that this defines a design and determine its parameters.

1.1. **Hadamard matrices and designs.**

Definition 13. *An Hadamard matrix of order n is a $n \times n$ matrix H with entries ± 1 satisfying $HH^T = nI$ (where I denotes the identity matrix).*

Starting from a Hadamard matrix H and multiplying rows and/or columns by -1 or multiplying on both sides by the same permutation matrix, we obtain a new Hadamard matrix with all entries in the first row and column equal to 1. Such a matrix is said to be **normalized**. Two Hadamard matrices are equivalent if one can be obtained from the other by transformations of this type.

Exercise 14. *Find all equivalence classes of Hadamard matrices of order 2, 4 and 8.*

Exercise 15. *Show that if H is a Hadamard matrix then $H^T H = nI$.*

Theorem 16. *If H is a Hadamard matrix of order n, then $n = 1$, $n = 2$ or $n \equiv 0 \mod 4$.*

Proof. Suppose $n > 2$ and assume H is normalized. we may permut columns in such a way that they are partioned in four blocks of consecutive columns, with a, b, c and d columns, respectively, and with the first three rows as follows:

$$\text{block1}: \begin{matrix} 1 \\ 1 \\ 1 \end{matrix}, \quad \text{block2}: \begin{matrix} 1 \\ 1 \\ -1 \end{matrix}, \quad \text{block3}: \begin{matrix} 1 \\ -1 \\ 1 \end{matrix}, \quad \text{block4}: \begin{matrix} 1 \\ -1 \\ -1 \end{matrix}$$

The inner products between these rows imply the conditions

$$\begin{cases} a+b+c+d=n \\ a+b-c-d=0 \\ a-b+c-d=0 \\ a-b-c+d=0 \end{cases}$$

Adding equations we find that $4a = n$ (and in fact $a = b = c = d$). $\square$

There is a long-standing and still unproved conjecture that there exist Hadamard matrices of order n for any $n \equiv 0 \mod 4$.
There are however some general constructions of Hadamard matrices. Given a $m \times n$ matrix A and another matrix B, their Kronecker product is

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}.$$

Theorem 17. *If H_m and H_n are Hadamard matrices of order respectively m and n, then $H_m \otimes H_n$ is a Hadamard matrix of order mn.*

Proof. Two general properties of the Kronecker product are

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD), \qquad (A \otimes B)^T = A^T \otimes B^T.$$

Putting

$$A = C = H_m, \qquad B = D = H_n$$

the result follows. The details are left as an exercise (**HW**). □

Exercise 18. *Prove that if H s a Hadamard matrix, then*

$$\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$$

is also Hadamard.
Show how this follows from the previous theorem.

A second method is the Paley construction. It is based on algebraic concepts, which will be better understood after an ntroduction to the theory of Finite Fields. For now, we will consider the particular case of $\mathbb{F}_p$, with p prime, which may be identified with the congruence classes of integers modulo p.
For this field, there exists the character χ defined by

$$\chi(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0 \text{ is a square} \\ -1 & \text{if } x \text{ is not a square} \end{cases}$$

The following properties of χ are easily deduced (**HW**):

- $\forall x, y \in \mathbb{F}_p \chi(xy) = \chi(x)\chi(y)$;
- $\sum_{x \in \mathbb{F}_p} \chi(x) = 0$;
- $\forall x \neq 0 \ \sum_{y \in \mathbb{F}_p} \chi(y)\chi(x+y) = -1$.

With $\mathbb{F}_p$ ordered as $\{0, 1, \cdots, p-1\}$, the matrix Q s defined by

$$Q_{ij} = \chi(i - j).$$

Q is symmetric (respectively anti-symmetric) if $p \equiv 1 \mod 4$ (respectively $p \equiv -1 \mod 4$). The respective Paley matrix is the $(p+1) \times (p+1)$ matrix

$$C = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ \pm 1 & & & \\ \vdots & & Q & \\ \pm 1 & & & \end{pmatrix}$$

where the sign in the first column is chosen to keep the symmetry or antisymmetry.

It follows that C satisfies $CC^T = pI$. A matrix with zero diagonal and ± 1 on the other entries satisfying this equality is called a **conference matrix**.

The connection with Hadamard matrices is given by

Proposition 19. a) *If C is a antisymmetric conference matrix $I + C$ is a Hadamard matrix.*

b) *If C is a symmetric conference matrix, then*

$$\begin{pmatrix} I+C & -I+C \\ -I+C & -I-C \end{pmatrix}$$

is a Hadamard matrix.

Proof. (**HW**). □

Hadamard matrices give rise to designs:

Proposition 20. *Let H is a normalized Hadamard matrix of order $4k$ and M be the matrix obtained erasing the first row and column.*
Let S be the set of the rows of M; Identifying each column with the set of rows that have a 1 in that column, the set $\mathcal{B}$ of the columns determines a $2-(4k-1, 2k-1, k-1)$ design.

Proof. (**HW**). □

Proposition 21. *Let H be a Hadamard matrix of order $4u^2$ and all row-sums equal to $2u$. If we replace each -1 by a 0 we obtain the incidence matrix of a $2-(4u^2, 2u^2+u, u^2+u)$ design.*

Proof. (**HW**). □

1.2. **Designs and Codes.** Designs occur naturally in error-correcting codes and may be used to prove the non-existence of codes with certain parameters, to help in the computation of their weight distribution or to construct codes from other structures.

Example 22. *If $S = \{1, \cdots, 7\}$ and $\mathcal{B}$ is the set of codewords with weight 3 in the binary $[7, 4, 3]$ Hamming code, $(S, \mathcal{B})$ is a $2-(7, 3, 1)$ design (**HW**). This design is also called the **Fano plane** and pictured as a triangle: the points occupy the vertices and the middle of the sides, together with a central point in the interior; in this geometric interpretation, the blocks are identified with lines.*
*This design may be constructed as follows (**HW**): Let $S = \mathbb{Z}_{/7}$ and define, for $x \in S$, $B_x = \{x, x+1, x+3\}$.*

Exercise 23. *Define, in the same way as described in the last paragraph, a $2-(13, 4, 1)$ design.*

Probably, the most significant example of the link between designs and codes is given by the Golay binary codes. We show how these codes may be defined from a design, which in turn is obtained algebraically.

Exercise 24. *Define a 11×11 matrix Q, with rows and columns indexed by the elements of $\mathbb{F}_{11}$ and entries in $\mathbb{F}_2$, by*

$$Q_{xy} = \begin{cases} 1 & \text{if } x-y \text{ is a square} \\ 0 & \text{if } x-y \text{ is not a square} \end{cases}$$

Show that Q is the incidence matrix of a $2-(11, 6, 3)$ design.

Exercise 25. *Let G be the 12×24 matrix $G = [I_{12}\, A]$ where I_{12} denotes the identity matrix and*

$$A = \begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & Q & \\ 1 & & & \end{bmatrix}.$$

Show that this is the generator standard form matrix for a $[24, 12, 8]$ binary code (the extended binary code).

Hadamard and conference matrices also give rise to codes. Replacing in a Hadamard matrix of order n each 1 by a 0 and each -1 by a 1, we get the binary Hadamard matrix A_n.

Proposition 26. a) *The rows of A_n with first column deleted constitute a $(n-1, n, n/2)$ binary code.*

b) *The rows of A_n together with their complements constitute a $(n, 2n, n/2)$ code.*

An example of a similar construction from a conference matrix:

Exercise 27. *Let C be a conference matrix of order n of the form*

$$C = \begin{pmatrix} 0 & \mathbf{1} \\ \mathbf{1}^T & S \end{pmatrix}$$

where $\mathbf{1}$ is the $n-1$ dimensional vector with all entries equal to 1. Denoting by J the matrix of order $n-1$ with all entries equal to 1 (ie $J = \mathbf{1}^T\mathbf{1}$), the rows of $\frac{1}{2}(S+I+J)$ together with those of $\frac{1}{2}(-S+I+J)$ constitute a $(n-1, 2n, \frac{n-2}{2})$ binary code.

Remark 28. *With $n = 10$ we obtain a $(9, 20, 4)$ code which is optimal: $A_2(9, 4) = 20$.*