Classical and quantum design theory

Tamás Tasnádi

BME, Institute of Mathematics

18. May, 2016.

Contents

Contents

History

Classical design theory:

- Part of combinatorial mathematics
- Deals with the construction and properties of certain system of finite sets
- Roots go back to antiquity (Lo Shu Square, 3×3 magic square)
- 18th century: Latin squares, recreational mathematics
- 19th century: Steiner system, ...
- 20th century: separate discipline (Ronald Fisher)

Quantum design theory:

- Started in the late 20th century
- Deals with the construction of certain sets of projections in a Hilbert-space

Contents

Contents

Example: Wine testing competition

Problem

Tasters have to rank different types of wines. Not all taster can taste all wines. Requirements:

- All wines should be tasted by the same number of tasters: r
- All taster should taste the same number of wines: k
- All pairs of wines should be tasted by the same number of tasters: λ

Number of tasters: b, number of wines: v

(v, k, λ) design

Definition

Given a finite set (base set) $S = \{1, 2 \dots v\}$. A collection $\mathcal{D} = \{S_1, S_2 \dots S_b\}$ of distinct subsets (blocks) of S is called a (v, k, λ) design, if $2 \leq k < v$, $1 \leq \lambda$ and

- $|S_i| = k$ for each $i = 1 \dots b$
- any two-element subset of S is contained in λ blocks.

Example

$$S = \{1, 2, 3, 4, 5, 6, 7\}, \quad v = |S| = 7, \quad k = |S_i| = 3, \quad b = |\mathcal{D}| = 7,$$

Points are covered by $r = 3$ blocks, pairs are by $\lambda = 1$ blocks.

$$S_1 = \{1, 2, 4\}, \quad S_2 = \{2, 3, 5\}, \quad S_3 = \{3, 4, 6\}, \quad S_4 = \{4, 5, 7\},$$
$$S_5 = \{5, 6, 1\}, \quad S_6 = \{6, 7, 2\}, \quad S_7 = \{7, 1, 3\}$$

Incidence matrix

$$S_1 = \{1,2,4\}, \quad S_2 = \{2,3,5\}, \quad S_3 = \{3,4,6\}, \quad S_4 = \{4,5,7\},$$
$$S_5 = \{5,6,1\}, \quad S_6 = \{6,7,2\}, \quad S_7 = \{7,1,3\}$$

incidence matrix :

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Rows code the blocks, columns code the points, $A_{i,j} = 1$, if $j \in S_i$.
The blocks are obtained by cyclic permutation. See also frame 22.

Basic properties – theorem

Let $\mathcal{D}$ be a (v, k, λ) design with b blocks.

Theorem

Each point is covered by the same number of points r, and

$$vr = bk,$$
$$(v-1)\lambda = r(k-1),$$
$$\lambda < r < b.$$

Basic properties – proof

Let $\mathcal{D}$ be a (v, k, λ) design with b blocks.

Proof.

Let $a \in S$ be fixed, and let r_a be be the number of blocks covering a. Count the cardinality of the set

$$\{(a, x, B) \mid a \neq x,\ a, x \in B \in \mathcal{D}\}$$

in two ways: $(v-1)\lambda = r_a(k-1)$

$\Longrightarrow r_a$ is independent of a.

Count the cardinality of the set

$$\{(x, B) \mid x \in B \in \mathcal{D}\}$$

in two ways: $vr = bk$.

By definition: $k < v \Longrightarrow \lambda < r < b$ (using equations above). $\square$

Complement design

Theorem

If $\mathcal{D} = \{S_1, S_2 \dots S_b\}$ *is a* (v, k, λ) *design with base set* S*, then*

$$\overline{\mathcal{D}} = \{S \setminus S_1, S \setminus S_2 \dots S \setminus S_b\}$$

is a $(v, v-k, b-2r+\lambda)$ *design, provided that* $b - 2r + \lambda \geq 1$*.*

Proof.

For any pair $\{x, y\} \subset S$ the number of $\mathcal{D}$-blocks containing neither x nor y is $b - 2r + \lambda$ (by the inclusion-exclusion principle). □

Definition

The design $\overline{\mathcal{D}}$ is called the complement design of $\mathcal{D}$.

The incidence matrix of $\overline{\mathcal{D}}$ is obtained by changing 0's to 1's and 1's to 0's in the incidence matrix of $\mathcal{D}$.

Fisher inequality

Theorem

For any (v, k, λ) *design* $\mathcal{D} = \{S_1, S_2 \dots S_b\}$: $v \leq b$.

Proof.

$$[\mathbf{A}^T\mathbf{A}]_{i,j} = \begin{cases} r, & \text{if } i = j \\ \lambda, & \text{if } i \neq j \end{cases} \implies \det(\mathbf{A}^T\mathbf{A}) = rk(r-\lambda)^{v-1} > 0$$

Assume: $b < v$. Extend $\mathbf{A}$ by zero rows to obtain the square matrix $\mathbf{A}_1$. $\implies \mathbf{A}^T\mathbf{A} = \mathbf{A}_1^T\mathbf{A}_1 \implies$

$$\det(\mathbf{A}^T\mathbf{A}) = \det(\mathbf{A}_1^T\mathbf{A}_1) = \det\mathbf{A}_1^T \det\mathbf{A}_1 = 0$$

Contradiction! □

Contents

Resolvable design

Definition

A (v, k, λ) design $\mathcal{D}$ is resolvable, if $\mathcal{D}$ can be partitioned into $r \geq 2$ collections $\mathcal{D}_i$ each consisting of pairwise disjoint blocks covering the base set S.
The partition $\mathcal{D} = \biguplus_i \mathcal{D}_i$ is called resolution of $\mathcal{D}$.
The subsets $\mathcal{D}_i$ are called parallel classes.

Clearly, $|\mathcal{D}_i| = \frac{v}{k} = \frac{b}{r}$ for each $i = 1, 2 \ldots r$.

Theorem (Bose inequality)

For any resolvable (v, k, λ) design:

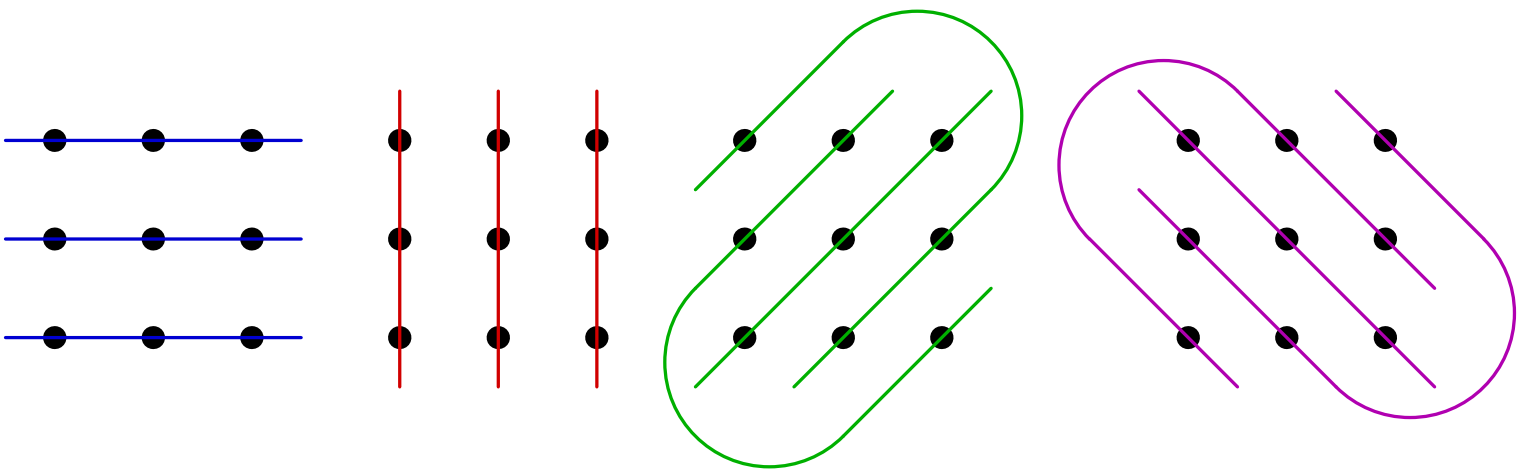
$$b \geq v + r - 1,$$

where $b = |\mathcal{D}|$ and r is the number of blocks covering a single point.

Example: Finite affine plane of order 3

$$v = 9, \qquad k = 3, \qquad \lambda = 1, \qquad r = 4, \qquad b = 12$$

Parallel classes:

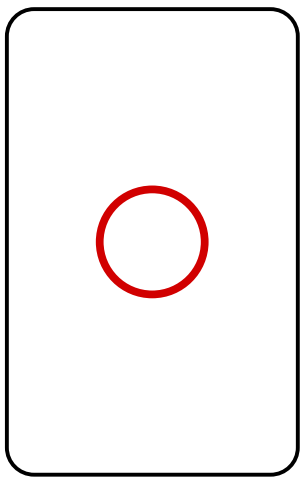
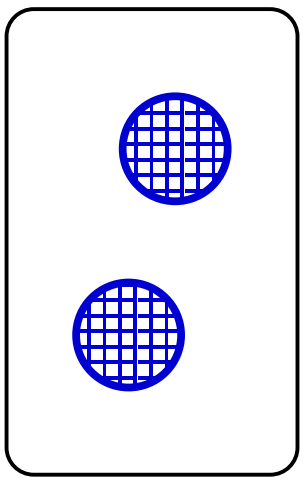
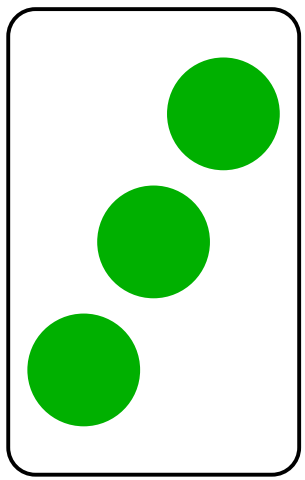


Example: The game SET I

Cards have 4 attributes, each with 3 different values:

1. symbol: circle, triangle, square
2. colour: red, green, blue
3. shading: filled, chequered, open
4. number: one, two, three

Three cards form a set if each attribute is either different or the same. Example:

Example: The game SET II

Aim: As fast as possible find sets in a group of 12 cards.
Mathematics: SET is a resolvable $(81, 3, 1)$ design:

- Number of cards: $v = 3^4 = 81$
- Number of cards in a set (block): $k = 3$
- To each pair of cards there is a unique third card to form a set, $\lambda = 1$
- Number of sets (blocks): $b = \binom{81}{2}\frac{1}{3} = 1080$
- Each card is in $r = \frac{81-1}{2} = 40$ sets
- Isomorphic to $AG(4, 3)$ (4 dimensional finite affine space of order 3)

Contents

Symmetric design

Definition

A (v, k, λ) design $\mathcal{D}$ is symmetric if $v = b$, i.e., its incidence matrix is a square matrix. For a symmetric design let $n = k - \lambda$. A symmetric design is trivial if $n = 1$.

Properties of symmetric designs

- $k = r$ (since $b = v$ and $vr = bk$)
- not resolvable (since $b \geq v + r - 1$ and $r \geq 2$ for resolvable design)
- $n = k - \lambda \geq 1$ (since $k < v$ and $\lambda(v - 1) = k(k - 1)$)
- $n = 1 \iff v - k = 1 = b - k \iff$ trivial symmetric design
- $|S_i \cap S_j| = \lambda$ for all $i \neq j$, $i, j = 1, 2 \ldots v$

Inequality for symmetric designs

Theorem

For any nontrivial, symmetric (v, k, λ) *design*

$$4n - 1 \leq v \leq n^2 + n + 1, \qquad \text{where} \qquad n = k - \lambda \geq 2.$$

Two extreme cases:

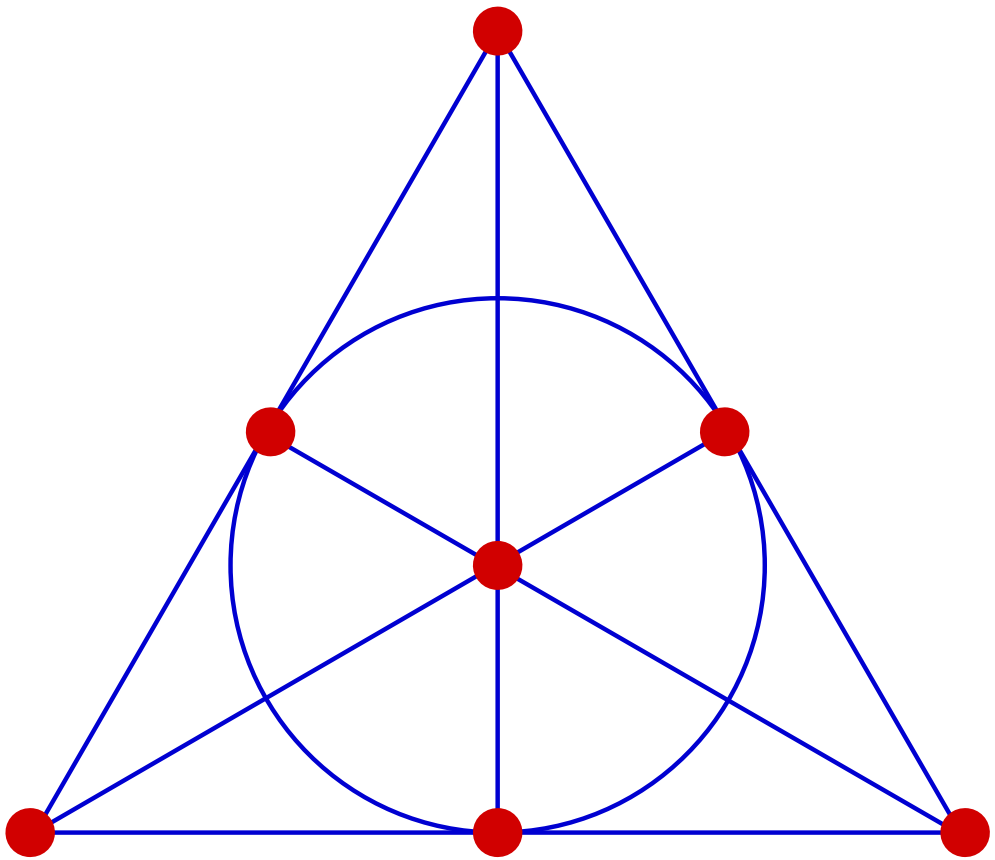
Theorem

If $\mathcal{D}$ *is a nontrivial, symmetric* (v, k, λ) *design with* $v = n^2 + n + 1$, *then either* $\mathcal{D}$ *or* $\overline{\mathcal{D}}$ *is an* $(n^2 + n + 1, n + 1, 1)$ *design, which is called a finite projective plane of order* n.

Theorem

If $\mathcal{D}$ *is a nontrivial, symmetric* (v, k, λ) *design with* $v = 4n - 1$, *then either* $\mathcal{D}$ *or* $\overline{\mathcal{D}}$ *is a* $(4n - 1, 2n - 1, n - 1)$ *design, which is called an Hadamard design of order* n.

Fano plane = projective plane of order 2 = (7,3,1) design



See also frame 9.

Example: The game Dobble

- There are $b' = 55$ cards
- On each card there are $k = 8$ different figures
- Altogether there are $v > 50$ figures
- Each pair of cards have exactly one figure in common
- Isomorphic to the finite projective plane of order $n = 7$, i.e., a symmetric (57,8,1) design
- By some reason the manufacturer omitted two cards

Aim: Find the common figure in given pairs of cards as fast as possible.

Projective plane of order $n = (n^2 + n + 1, n + 1, 1)$ design

Geometry:

- a single line goes through any pair of points
- it contains $n^2 + n + 1$ points and $n^2 + n + 1$ lines
- each line has $n + 1$ points, each point holds $n + 1$ lines

Known facts

- exists, if n is a prime power (The construction is based on factorising vector spaces over finite fields.)
- does not exist, if $n = 4k + 1$ or $n = 4k + 2$ and n is not a sum of two squares (this rules out $n = 6$)
- does not exist for $n = 10$ (massive computer calculations)

Not known:

- existence for any other n? (even $n = 12$ is open)
- uniqueness of prime order projective planes?

Latin squares I

Definition

A matrix of size $n \times n$ is a Latin square of order n if each row and each column contains all elements of the set $\{1, 2 \ldots n\}$ exactly once.

Two Latin squares $A = (a_{i,j})$ and $B = (b_{i,j})$ are called orthogonal if the ordered pairs $(a_{i,j}, b_{i,j})$ are distinct for all i and j.

Example:

$$A = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array}, \quad B = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 3 & 1 & 2 \\ \hline 2 & 3 & 1 \\ \hline \end{array}, \quad \Longrightarrow \quad \begin{array}{|c|c|c|}\hline (1,1) & (2,2) & (3,3) \\ \hline (2,3) & (3,1) & (1,2) \\ \hline (3,2) & (1,3) & (2,1) \\ \hline \end{array}$$

Latin squares II

Theorem

There are at most $n-1$ mutually orthogonal Latin squares of order n.

Theorem

The followings are equivalent:

- *existence of an affine plane of order n, i.e., an $(n^2, n, 1)$ design;*
- *existence of a projective plane of order n i.e., an $(n^2+n+1, n+1, 1)$ design;*
- *existence of $n-1$ mutually orthogonal Latin squares.*

Hadamard matrices and $(4n-1, 2n-1, n-1)$ designs I

Definition

An $m \times m$ matrix $(m \geq 2)$ $\mathbf{H}$ with entries from the set $\{+1, -1\}$ is called Hadamard matrix if $\mathbf{H}^T\mathbf{H} = m\mathbf{I}$.

Examples: (for powers of 2)

$$\mathbf{H}_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}, \quad \mathbf{H}_{2m} = \begin{bmatrix} +\mathbf{H}_m & +\mathbf{H}_m \\ +\mathbf{H}_m & -\mathbf{H}_m \end{bmatrix}, \quad \mathbf{H}_{mn} = \mathbf{H}_m \otimes \mathbf{H}_n$$

Theorem

If $\mathbf{H}$ *is an Hadamard matrix of order* m *then either* $m = 2$ *or* m *is divisible by* 4.

Conjecture: There exist $\mathbf{H}_{4k}$ for any $k \in \mathbb{N}_+$.

Theorem

$\exists \mathbf{H}_{4n}$ *matrix* $\iff \exists$ *Hadamard* $(4n-1, 2n-1, n-1)$ *design.*

Hadamard matrices and $(4n-1, 2n-1, n-1)$ designs II

Proof.

- By multiplying the rows and columns by -1 transform the entries of the first row and first column of $\mathbf{H}_{4n}$ to 1's.
- Omit the first row and column, that gives the incidence matrix of the design.

□

Contents

Probabilistic interpretation of 2-designs I

Let $\mathcal{D} = \{S_1, S_2 \dots S_b\}$ be a (classical) (v, k, λ) design with base set S, and let μ be the uniform probability measure on S. Let $E_i : S \to \mathbb{R}$ be the characteristic function of S_i.

Interpretation:

- S: set of elementary events
- $\mathcal{D}$: set of selected events

Properties:

- $|S_i| = k \iff \mu(E_i) = \int_S E_i \, \mathrm{d}\mu = \frac{\mathrm{k}}{\mathrm{v}}$
- Points are covered by r blocks $\iff \sum_{i=1}^{b} E_i = r$

Probabilistic interpretation of 2-designs II

- Pairs are covered by λ blocks

$\iff$ $\sum_{i=1}^{b} E_i(x)E_i(y) = \lambda = \text{constant} \quad \forall x, y \in S, \quad x \neq y$

$\iff$ $\forall \phi$ permutation of S

$$\sum_{i=1}^{b} E_i\big(\phi(x)\big)E_i\big(\phi(y)\big) = \sum_{i=1}^{b} E_i(x)E_i(y)$$

$\iff$ $\sum_{i=1}^{b} (E_i \circ \Phi) \otimes (E_i \circ \Phi) = \sum_{i=1}^{b} E_i \otimes E_i$

Quantum designs

Definition

The family $\mathcal{D} = \{P_1, P_2 \dots P_b\}$ of orthogonal projections (events) of the Hilbert space $\mathbb{C}^v$ is called a quantum design.

- $\mathcal{D}$ is regular if $\operatorname{Tr} P_i = \frac{k}{v}$ for every i;
- $\mathcal{D}$ is coherent if $\sum_{i=1}^{b} P_i = rI$;
- $\mathcal{D}$ is t-coherent (w.r.t. the unitary group), if $\forall U$ unitary, $\forall 1 \leq s \leq t$:

$$\sum_{i=1}^{b} P_i^{\otimes s} = \sum_{i=1}^{b} (UP_iU)^{\otimes s};$$

- the degree of $\mathcal{D}$ is the cardinality of the set

$$\left\{ \operatorname{Tr}(P_iP_j) \mid i,j \in \{1,2 \dots b\},\ i \neq j \right\}$$

- An affine quantum design is a quantum design of degree 2.

Special quantum designs

Theorem

- *A maximal system of MUB (mutually unbiased bases) is a regular, 2-coherent affine quantum design.*
- *A SIC-POVM (symmetric, informationally complete positive operator valued measure) is a regular, 2-coherent quantum design of degree 1.*

Summary

- Classical block design theory is a well developed, powerful tool to design events on a finite, classical event space with a rich symmetric structure.
- Similar methods can/should be used to design sets of quantum events with high symmetry on a quantum event lattice.
- Known quantum designs nicely fit into the framework of the quantum design theory.

Thank You for the attention!