Designs and Codes — So 2017
Martin Aigner — Shagnik Das

Practice Sheet

This sheet is not for submission.
No due date ⇒ no late submission ⇒ no dire warning

This additional problems are provided to allow you some further practice ahead of the exams. We will not be discussing their solutions in class, but you should write to us if you have any questions concerning these exercises.

Exercise 1 Let $\mathcal{D}$ be a t-(v,k,λ) design over the ground set X, and let $x \in X$.

(a) Let $\mathcal{D}_x = \{B \setminus \{x\} : B \in \mathcal{D}, x \in B\}$ be defined over the ground set $X \setminus \{x\}$. Show that $\mathcal{D}_x$ is a $(t-1)$-design, and compute its parameters.

(b) Let $\mathcal{D}^x = \{B : B \in \mathcal{D}, x \notin B\}$ be defined over the ground set $X \setminus \{x\}$. Show that $\mathcal{D}^x$ is also a $(t-1)$-design, and compute its parameters.

(c) A design $\mathcal{D}$ is called *extendable* if there is some design $\mathcal{E}$ such that the ground sets satisfy $X(\mathcal{D}) = X(\mathcal{E}) \setminus \{x\}$ for some x, and $\mathcal{D} \cong \mathcal{E}_x$. If $\mathcal{D}$ is an extendable 2-(v,k,λ) design, how many blocks does its extension $\mathcal{E}$ have?

Exercise 2 Let $\mathcal{P}$ be a projective plane of order q. Three points that do not lie on a common line are said to form a *triangle*. How many triangles does $\mathcal{P}$ have?

Exercise 3 Show that the Fano plane is the unique projective plane of order 2 (up to isomorphism). What is the size of its automorphism group?[1]

Exercise 4 Show that if a projective plane $\mathcal{P}$ of order q is extendable (see Exercise 1), then $q \in \{2, 4, 10\}$. Show that the Fano plane is indeed extendable by constructing its extension.

Exercise 5 Consider an m-set X and all 2^m subsets. Order the subsets $C_1, C_2, \ldots, C_{2^m}$ arbitrarily. Show that the $2^m \times 2^m$ matrix $H = (h_{i,j})$ defined by $h_{i,j} = (-1)^{|C_i \cap C_j|}$ is a Hadamard matrix.

[1] An automorphism of a design $\mathcal{D}$ is a bijection $\varphi : X \to X$ such that a block $B \in \mathcal{D}$ if and only if its image $\varphi(B) \in \mathcal{D}$.

Exercise 6 An $n \times n$ Latin square L is *reduced* if $L_{1,i} = L_{i,1} = i$ for $1 \leq i \leq n$. Let r_n denote the number of reduced Latin squares of order n. Compute r_n for $n \leq 4$. How many isomorphism types exist?[2] Which have orthogonal mates?

Exercise 7 Consider

$$L = \begin{pmatrix} 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Find an orthogonal mate for L and construct a semi-magic square on $\{1, 2, \ldots, 16\}$.[3]

Exercise 8

(a) Use $\mathbb{F}_4$ to construct three mutually orthogonal Latin squares of order four.

(b) Use two orthogonal Latin squares of order three to construct a projective plane of order three.

Exercise 9 A *linear space* $LS(X, \mathcal{B})$ is a set of points X together with a family $\mathcal{B}$ of blocks such that

(i) $|B| \geq 3$ for all $B \in \mathcal{B}$

(ii) for every pair $x \neq x' \in X$, there is a unique block $B \in \mathcal{B}$ with $x, x' \in B$.

It is a fact that the existence of a linear space $LS(X, \mathcal{B})$ with $|X| = n$ and block sizes $|B| \in \{k_1, k_2, \ldots, k_r, k_{r+1}, \ldots, k_m\}$ such that no two blocks $B, B' \in \mathcal{B}$ with $|B|, |B'| \in \{k_1, \ldots, k_r\}$ intersect, implies $N(n) \geq \min\{N(k_1), \ldots, N(k_r), N(k_{r+1}) - 1, \ldots, N(k_m) - 1\}$.

By starting with a projective plane $\mathcal{P}$ of order $q \geq 4$, construct an appropriate linear space $LS(X, \mathcal{B})$ on a ground set of size $q^2 + q - 2$, and deduce that $N(18) \geq 2$ and $N(70) \geq 6$.

Exercise 10 We know that the Hamming code $H_{3,2}$ is a $[7, 4, 3; 2]$-code, while its extension $\hat{H}_{3,2}$ is an $[8, 4, 4; 2]$-code. Show that these codes are the unique linear codes (up to reordering the coordinates) for their respective parameters.

[2] Two Latin squares are isomorphic if one can be obtain from the other by permuting rows, columns and symbols. An isomorphism type is an equivalence class under isomorphism.

[3] Recall that this is a 4×4 matrix with distinct entries from $\{1, 2, \ldots, 16\}$ such that all row and column sums are the same.

Exercise 11 Let $n \geq 2R+2$, and let $C \subseteq \{0,1\}^n$ be an R-perfect code (not necessarily linear) with the weight sequence $(a_0, a_1, \ldots, a_n)$, and suppose further that $a_0 = 1$.

(a) By considering words of weight $R+1$, show that $a_{2R+1}\binom{2R+1}{R+1} = \binom{n}{R+1}$.

(b) By now considering words of weight $R+2$, show that $a_{2R+2}\binom{2R+2}{R+2} = \binom{n}{R+2} - a_{2R+1}\binom{2R+1}{R+2}$.

(c) Show that all R-perfect codes over $\{0,1\}^n$ containing $\vec{0}$ have the same weight sequence.

Exercise 12 Let H be a normalised Hadamard matrix of order $n \geq 4$. Construct codes A, B and C, where:

(a) $A \subseteq \{0,1\}^{n-1}$, $|A| = n$, $d(A) = n/2$.

(b) $B \subseteq \{0,1\}^{n-1}$, $|B| = 2n$, $d(B) = n/2 - 1$.

(c) $C \subseteq \{0,1\}^n$, $|C| = 2n$, $d(C) = n/2$.