Designs and Codes
Martin Aigner

So 2017
Shagnik Das

# Exercise Sheet 6

**Due date: 12:30, Jul 12th, at the beginning of the exercise class.**
**Late submitters will be asked to update the course's lecture notes.**

You should try to solve all of the exercises below, and submit three solutions to be graded — each problem is worth 10 points. We encourage you to submit in pairs, but please remember to indicate the author of each individual solution.

**Exercise 1** In this exercise you will fill in some of the missing details from the proof of the Assmus–Mattson theorem we saw in lecture.

(a) In Step 2 of the proof, we used the fact that the (binary) Krawtchouk polynomial

$$P_{\ell,n}(x) = \sum_{j=0}^{\ell} (-1)^j \binom{x}{j} \binom{n-x}{\ell-j}$$

has degree $\ell$. Verify this by computing the coefficient of $x^\ell$ exactly and showing that it is non-zero.

(b) Complete Step 4: given that the weight sequence $(\alpha_0, \alpha_1, \ldots, \alpha_{n-t})$ of the punctured code $C_0$ is independent of the $t$-set $T$ of removed coordinates, prove that the words of weight $w$ in the original code $C$ form a $t$-design.

[Hint at `http://discretemath.imp.fu-berlin.de/DMIII-2017/hints/S6.html`.]

**Exercise 2** Recall that the extended ternary Golay code $G_{12}$ has the generator matrix

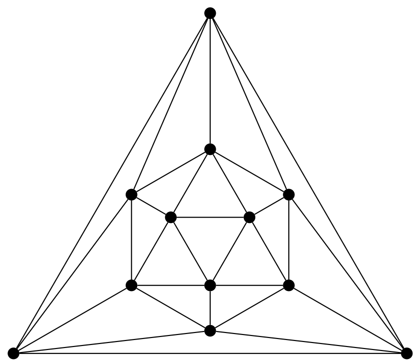
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & -1 & -1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & -1 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & -1 & -1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & -1 & -1 & 1 & 0 \end{pmatrix} \in \mathbb{F}_3^{6\times 12}.$$

(a) Show that $G_{12}$ is self-dual; that is, $(G_{12})^\perp = G_{12}$.

(b) Prove that $d(G_{12}) = 6$.

**Exercise 3**

In this exercise you will be introduced to the binary Golay codes. We start with the 5-regular 12-vertex icosahedron graph $\Gamma_{\text{ico}}$, pictured to the right.



Let $A$ be the adjacency matrix of $\Gamma_{\text{ico}}$, viewed as a matrix in $\mathbb{F}_2^{12\times 12}$. Let $J$ be the all-one matrix in $\mathbb{F}_2^{12\times 12}$, and set $B = J - A$. The *extended binary Golay code* $G_{24}$ is generated by the matrix $G = \left( \begin{array}{c|c} I_{12} & B \end{array} \right) \in \mathbb{F}_2^{12\times 24}$, and thus has parameters $n = 24$, $k = 12$ and $q = 2$.

(a) Show that $G_{24}$ is self-dual; that is, $(G_{24})^{\perp} = G_{24}$.

(b) Prove that $d(G_{24}) = 8$.

The *binary Golay code* $G_{23}$ is obtained by puncturing $G_{24}$ in any coordinate.

(c) Prove that $G_{23}$ is a 3-perfect binary code.

[Hint at `http://discretemath.imp.fu-berlin.de/DMIII-2017/hints/S6.html`.]

**Exercise 4**

(a) Suppose $C$ is a self-dual binary code with a basis $\{\vec{c}_1, \vec{c}_2, \ldots, \vec{c}_k\}$ such that the weight of each $\vec{c}_i$ is divisible by 4. Prove that the weight of every word $\vec{c} \in C$ is divisible by 4.

(b) Consider the code $G_{24}$ from Exercise 3. Deduce that, for every $w$, the supports of the codewords of weight $w$ form a 5-design.

(c) Show that when we take $w = 8$, we obtain a Steiner system. What are its parameters?

**Exercise 5** Number theorists have long known that the only natural numbers $x$ for which $x^2 + 7$ is a power of two are $x = 1, 3, 5, 11$ or $181$. Now that you also know this amazing fact, prove that (not necessarily linear) 2-perfect codes $C \subseteq \{0,1\}^n$ exist if and only if $n = 5$.

[Hint at `http://discretemath.imp.fu-berlin.de/DMIII-2017/hints/S6.html`.]

**Exercise 6** Let $A$ be an alphabet of size 6. Suppose $C \subseteq A^7$ is a (not necessarily linear) 1-perfect code.

(a) Show that every $(a_1, \ldots, a_5) \in A^5$ has a unique pair $(a_6, a_7)$ such that $(a_1, \ldots, a_7) \in C$.

(b) Deduce that such a code $C$ cannot, in fact, exist.

[Hint at `http://discretemath.imp.fu-berlin.de/DMIII-2017/hints/S6.html`.]