C&O 434/634

Assignment 3

1. Let $\mathcal{P}$ be a projective plane of order n. A *subplane* of $\mathcal{P}$ is a subset of the points and a subset of the lines of $\mathcal{P}$ that is itself a projective plane. Show that iff $\mathcal{P}$ has a subplane of order m then $n \geq m^2$. If equality holds prove that each line of $\mathcal{P}$ meets the subplane in 1 or $m+1$ points. [Subplanes of order $\sqrt{n}$ are known as *Baer subplanes*. A projective plane over a field of order q^2 contains a subplane of order q.]

2. Let $\mathcal{D}$ be a 2-(v, k, λ) design and let β be a block in $\mathcal{D}$. Let $f(z)$ be the polynomial $(z-a)^2$ and assume that exactly d blocks distinct from β meet it in at least one point. Show that the average value of f_β over the blocks of $\mathcal{D}$ is at least
$$\frac{(k-a)^2 + (b-1-d)a^2}{b}.$$
Next compute the average of f_β over Ω (the set of all k-subsets of $\{1, \ldots, v\}$) and hence show that the number of blocks that have at least one point in common with β is at least
$$\frac{k(r-1)^2}{(k-1)(\lambda-1)+r-1}.$$
If equality holds, show that $\mathcal{D}$ has degree two and determine its degree set.

3. Show that if there is an $n \times n$ Latin square that is symmetric and idempotent, then n is odd.

4. Let $\mathcal{D}$ be a Hadamard 2-design with point set V. Let $\mathcal{D}^1$ be the incidence structure with point set $V \cup \infty$ and block set consisting of the blocks of $\mathcal{D}$ extended by ∞, together with the complements in V of the blocks of $\mathcal{D}$. Show $\mathcal{D}^1$ is 3-design and determine its parameters.

5. Show that a 3-design on v points with $2v-2$ blocks is a Hadamard 3-design.

6. A design is *affine* it is resolvable and there is a constant c such that any two blocks in different classes intersect in exactly c points. Prove that 3-design is affine if and only if it is Hadamard 3-design.

7. Let L be a Latin square of order n. A *subsquare* of L is a submatrix that is itself a Latin square. Prove that if L has a subsquare of order m, then $n \geq 2m$.

8. Assume $q = 6t + 1$ is a prime power and let γ be a generator of the the multiplicative group of the field of order q (a primitive element). Show that the translates (under addition) of the sets

$$\{\gamma^i, \gamma^{2t+i}, \gamma^{4t}\}, \quad (0 \leq i < t)$$

form a Steiner triple system.

9. Show that if the are Steiner triple systems on v_1 points and on v_2 points, there is a Steiner triple system on $v_1 v_2 - v_2 + 1$ points.

10. Let G be a matrix over $\mathbb{Z}_2$. Show that if each row of G has even weight, then each word in $\text{row}(G)$ has even weight. Show further that if $GG^T = 0$ and the weight of any row of G is divisible by four, then each word in $\text{row}(G)$ has weight divisible by four.

11. Let $\mathcal{D}$ be a symmetric 2-$(v, k, 2)$ design with incidence matrix N and let G be the matrix

$$G = \begin{pmatrix} I & N \end{pmatrix}.$$

Prove that, if k is odd then $\text{row}(G)$ is an even self-dual binary code with minimum weight $k + 1$.

12. Let $\mathcal{D}$ be a symmetric 2-$(v, k, 2)$ design with k odd. If N is the incidence matrix of $\mathcal{D}$ and

$$G = \begin{pmatrix} I & N \end{pmatrix},$$

show that $\text{row}(G)$ is a self-dual even binary code. Hence show that we cannot have $k \equiv 7$ modulo eight.

13. Prove that the code in the previous problem has minimum weight $k + 1$.

14. Suppose we have an $OA(k, q)$ and a flat unitary matrix H of order $q \times q$. Our array can be viewed as an incidence structure with q^2 lines and kq points. Let M be the incidence matrix of the dual; this has order $q^2 \times kq$. Show that the kd^2 vectors

$$(\mathbf{1} \otimes He_i) \circ Me_j$$

form k mutually unbiased bases in $\mathbb{C}^{q^2}$. [If $q = 26$, then the product construction provides five mub's in $\mathbb{C}^{576}$. There is an $OA(26, 6)$, and so we obtain six mub's in $\mathbb{C}^{576}$.]

15. Let $v_1, \ldots, v_m$ be a set of flat unit vectors spanning a set of equiangular lines in $\mathbb{C}^d$ and let $e_1, \ldots, e_d$ be the standard basis for $\mathbb{C}^d$. Assume that $|v_i^* v_j| = \alpha^2$ if $i \neq j$ and let G be the Gram matrix of the projections

$$v_1 v_1^*, \ldots, v_m v_m^*, e_1 e_1^*, \ldots, e_d e_d^*.$$

Prove that if the relative bound is tight, $\mathrm{rk}(G) = m + d - 1$ and that otherwise $\mathrm{rk}(G) = m + d$. Deduce that $m \leq d^2 - d + 1$.