Winter 2018, Math 148: Week 8 Problem Set
Due: Wednesday, March 7th, 2018
Constructing More and More t-designs

Discussion problems. The problems below should be completed in class.

(D1) *Designs from difference sets.* A subset $A \subset \mathbb{Z}_n$ is a *difference set* if each nonzero element of $\mathbb{Z}_n$ occurs the same number of times as $x - y$ for distinct $x, y \in A$.

(a) Determine whether each of the following is a difference set. You may find it useful to divide the work here!

$$\{0, 2, 3, 4, 8\} \subset \mathbb{Z}_{11} \qquad \{0, 1, 3, 11\} \subset \mathbb{Z}_{12}$$

(b) For each set $A \subset \mathbb{Z}_n$ in part (a) above, determine for which t the collection of sets $A + i = \{i + x : x \in A\}$ for $i \in \mathbb{Z}_n$ form a t-design.

(c) Our goal for this discussion problem is to prove the following theorem.

Theorem. *Given a difference set $A \subset \mathbb{Z}_n$, the sets $A + i$ for $i \in \mathbb{Z}_n$ form a 2-design.*

Assuming the theorem holds, find the parameters v, k, and r_1 (i.e. the number of blocks each $j \in \mathbb{Z}_n$ appears in), each in terms of $|A|$ and n. Using general facts about 2-designs, find b and r_2 (i.e. the number of blocks in which each pair $j, j' \in \mathbb{Z}_n$ appear together) in terms of $|A|$ and n. Can you find a difference set that produces a 2-design with parameters $(v, k, r_2) = (7, 3, 2)$? What about $(v, k, r_2) = (7, 3, 1)$?

(d) Argue that each block $A + i$ is distinct. Prove that each $j \in \mathbb{Z}_n$ occurs in r_1 blocks.

(e) Given distinct $j, j' \in \mathbb{Z}_n$, argue that $j - j' = x - y$ has r_2 solutions (x, y) for distinct $x, y \in A$. For each solution (x, y), find a value of i so that $j, j' \in A + i$.

(f) Conclude that the above theorem holds.

(g) If we replace $\mathbb{Z}_n$ in both the definition of difference set and the theorem above with $\mathbb{F}_q$ for q a prime power, does the theorem still hold? In particular, does your proof break, and if so, can you amend your argument to avoid this?

(D2) *The projective plane over a finite field.* The goal of this problem is to construct spaces in which any 2 distinct lines intersect in exactly 1 point.

(a) (i) Draw the affine plane $\mathbb{F}_2^2$. List all of the lines in $\mathbb{F}_2^2$.
(ii) For each pair L_1, L_2 of parallel lines, draw a new point "off the edge of the plane" and extend L_1 and L_2 to contain the new point. They might not be "straight"!
(iii) How many points does your space have? How many points does each line have?
(iv) Does every pair of distinct points still determine a line? Is there an easy way to fix this while preserving your answers in part (c)?
(v) Using t-designs, what can you conclude about the lines in the resulting space?

(b) (i) Draw the affine plane $\mathbb{F}_3^2$. What is the maximum number of non-parallel lines?
(ii) As in problem (D1), for each triple L_1, L_2, L_3 of parallel lines, draw a new point "off the edge of the plane" and extend each line to contain the new point.
(iii) How many lines do you need to add in order to ensure every 2 points determine a line? Do all of your lines contain the same number of points?
(iv) Using t-designs, what can you conclude about the lines in the resulting space?

(c) Pick a representation for $\mathbb{F}_4$ using polynomials. Repeat the construction from parts (a) and (b) using the affine plane $\mathbb{F}_4^2$. Do the set of lines form a t-design?

(d) Conjecture a general construction for the projective plane of $\mathbb{F}_q$. Viewing the set of lines in this space as blocks in a 2-design, what will the parameters (v, k, r) be?

Required problems. As the name suggests, you must submit *all* required problem with this homework set in order to receive full credit.

(R1) Describe how to construct the following designs using methods we have seen. You are *not* required to explicitly give the resulting design, only describe how you would construct it.

(a) A 2-design with $(v, k, r) = (31, 6, 1)$
(b) A 1-design with $(v, k, r) = (11, 5, 5)$
(c) A 2-design with $(v, k, r) = (7, 7, 1)$
(d) A 2-design with $(v, k, r) = (49, 7, 1)$
(e) A 2-design with $(v, k, r) = (11, 5, 2)$
(f) A 1-design with $(v, k, r) = (16, 4, 5)$

(R2) Verify that the set $A = \{b^2 : b \in \mathbb{Z}_{11}\}$ of perfect squares in $\mathbb{Z}_{11}$ is a difference set.

(R3) Prove that if $A \subset \mathbb{Z}_n$ is a difference set, then so is $A + i$ for each $i \in \mathbb{Z}_n$. (Your proof can be short!) Conclude that when searching for difference sets, it suffices to assume $0, 1 \in A$.

(R4) A *quadrangle* is a set of 4 points, no 3 of which lie on a line together (i.e. no 3 are colinear). How many quadrangles are there in the projective plane over $\mathbb{F}_2$? How are the quadrangles related to the lines in the projective plane? Does this also hold for quadrangles in the projective plane over $\mathbb{F}_3$?

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) An *oval* in the projective plane over $\mathbb{F}_q$ is a set of $q+2$ points of which no three are colinear. Prove that the intersection of an oval and a line has either 0 points or 2 points.

(C2) Find all ovals in the projective plane over $\mathbb{F}_3$, and prove that your list is complete.

(C3) Suppose p is prime and $p = 4n+3$ for some $n \geq 1$. Prove that the set $A = \{b^2 : b \in \mathbb{Z}_p\}$ of perfect squares in $\mathbb{Z}_p$ is a difference set. Does the same hold if p is prime and $p = 4n + 1$ for some $n \geq 1$?