Math 155: Designs and Groups

Homework Assignment #3 (10 February 2010):
Inclusion-Exclusion, designs, and a bit about regular graphs

This problem set is due Wednesday, Feb.17 in class, together with problems 6 and 7 of Homework #2.

1. Solve Problem #18 on p.27–28 of the textbook. For part (a) can you prove the identity using finite differences instead of the principle of inclusion and exclusion? [You may know part (b) already; some 15 years ago it also appeared on the Qualifying Exam for graduate students.]

2. Solve Problem #16 on p.27 (this involves arguments similar to those we'll use in analyzing arcs and ovals).

3. Let k be the finite field of q elements where $q \equiv 3 \bmod 4$, and let G be the group of $(q^2-q)/2$ permutations of k of the form $x \mapsto a^2x + b$ where $a, b \in k$ and $a \neq 0$. Prove that while G is not doubly transitive, G does act transitively (indeed simply transitively) on *unordered* pairs of elements of k. Use this to give an alternative verification of Paley's construction of a Hadamard 2-design.

4. Let F be a perfect (but not necessarily finite) field[1] of characteristic 2, and $C \subset \mathbf{P}^2(F)$ the conic $xz = y^2$, i.e. $(x : y : z) = (r^2 : rs : s^2)$ for $(r : s) \in \mathbf{P}^1(F)$.[2] Determine for each point on C the tangent through C, and find the point $P \in \mathbf{P}^2(F)$ at which all the tangents meet. Check algebraically that any point $P' \neq P$ in the projective plane lies on a unique tangent. [Our combinatorial techniques don't apply when F is infinite.]

5. Now let F be a finite field of 2^n elements, and let d be an integer relatively prime to n. Prove that the subset of $\mathbf{P}^2(F)$ consisting of $(1:0:0)$, $(0:1:0)$, and all points of the form $(x : y : z) = (a^{2^d} : a : 1)$ $(a \in F)$ is a hyperoval, and is an extended conic (a conic together with its center) if and only if $d \equiv \pm 1 \bmod n$. Conclude that if $n = 5$ or $n > 6$ then $\mathbf{P}^2(F)$ contains hyperovals that are not extended conics.

6. Recall that the "girth" of a graph is the length of its shortest cycle. Prove that a regular graph of degree d and girth 6 has at least $2(d^2 - d + 1)$ vertices, with equality possible if and only if there is a finite projective plane of order $d-1$. For instance there is up to isomorphism a unique cubic graph[3] of girth 6 on 14 vertices (the "Heawood graph"); what is its automorphism group? Show that this is also the graph obtained by tiling the torus with seven pairwise adjacent hexagons.

---

[1] Recall that a field k called is *perfect* if every finite extension of k. This condition is automatic if k has characteristic zero, while in characteristic p it is equivalent to the condition that $k = k^p$, i.e. every field element is of the form c^p for some $c \in k$ (unique because $c^p - c'^p = (c - c')^p$. This is automatic for finite fields but may fail in general, e.g. $\mathbf{F}_p(X)$ is not perfect since X is not a p-th power.

[2] Remember that the notation $(x : y : z) = (r^2 : rs : s^2)$ means that there exists $c \in k^*$ such that $(x, y, z) = c(r^2, rs, s^2)$; in general we cannot assume that $(x, y, z) = (r^2, rs, s^2)$ (with $c = 1$).

[3] "cubic graph" is standard graph theory lingo for "regular graph of degree 3".