Advanced Combinatorics
Math 295, Spring 2007
Class Summary and Homework Questions: Week 3, Lectures 9 and 10.

Note: the **final exam** on Friday will be closed-book, except that you will be permitted to refer to these printed Class Summaries (for Week 3 only, not for weeks 1 and 2) because of the more advanced nature of the 3rd week material. Hard copies will be distributed at the exam; you cannot use your previously received copy.

Proofread by instructor, April 12, 6 am. The Lecture 9 material contains updates compared to the preliminary version distributed by the TA.

Lecture 9 - April 10

The Homework below is due on Thursday 12th March.

A *basis* for a vector space V is a linearly independent set of vectors which span V. Every vector space has a basis.
Theorem. The following are equivalent:
(a) B is a basis for V.
(b) B is a maximal linearly independent set for V.
(c) B is a minimal set that spans V.
(d) B is a linearly independent set and $|B| = \dim V$.
(e) B spans V and $|B| = \dim V$.
Do: (a) Prove every linearly independent set in a vector space V can be extended to a basis for V.
(b) Prove every set in V that spans V contains subset that is a basis for V.
Theorem. If $\{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$ is a basis for a vector space V, then every $\mathbf{v} \in V$ can be written uniquely as $\mathbf{v} = \beta_1\mathbf{b}_1 + \cdots + \beta_n\mathbf{b}_n$.
The $\beta_1, \ldots, \beta_n$ are called the *coordinates* of $\mathbf{v}$ with respect to the basis $\{\mathbf{b}_1, \cdots, \mathbf{b}_n\}$. This gives a bijection from V to F^n. An *isomorphism* $f\colon V \to W$ is a bijection such that $f(\mathbf{x} + \mathbf{y}) = f(\mathbf{x}) + f(\mathbf{y})$ and $f(\alpha\mathbf{x}) = \alpha f(\mathbf{x})$ for all $\mathbf{x}, \mathbf{y} \in V$ and $\alpha \in F$. If there exists an isomorphism we say the two vector spaces are isomorphic, $V \cong W$. If $\dim_F V = n$ then $V \cong F^n$.
Do: Prove if $V \cong W$, then $\dim V = \dim W$.
Corollary. If V is an n-dimensional vector space over $\mathbb{F}_p$ then $|V| = p^n$.
Note that this in particular applies to the n-dimensional subspaces of $\mathbb{F}_p^N$ for any N: each n-dimensional subspace consists of p^n vectors. We used this in the proof of Eventown Theorem.
For a field F consider the vector space $F[x]$ of polynomials over F. (The "vectors" in $F[x]$ are the polynomials in the variable x. Note that linear combinations of polynomials can be taken in the obvious manner.)
The countably infinite set $\{1, x, x^2, \ldots\}$ is a basis for $F[x]$.
Puzzle: Prove that all vector spaces have bases, including those containing uncountably large linearly independent sets. (Requires Zorn's Lemma.)
Puzzle: (Cauchy's Functional Equation) Consider a function $f\colon \mathbb{R} \to \mathbb{R}$ which satisfies $f(x + y) = f(x) + f(y)$ for all $x, y \in \mathbb{R}$.
(I) Show that if any one of the following holds, then $f(x) = cx$.
(a) f is continuous.

(b) f is continuous at a point.
(c) f is bounded in an interval.
(d) f is measurable in an interval.
(II) Prove that there exists a solution which is not linear. Hint: $\mathbb{R}$ is a vector space over $\mathbb{Q}$. (A basis of this space is called a "Hamel basis.")
Notation: $F[x_1, \ldots, x_k]_n$ is the space of polynomials of degree $\le n$ in the k variables $x_1, \ldots, x_k$. The degree of the *monomial* $\prod_{i=1}^k x_i^{k_i}$ is $\sum_{i=1}^k r_i$. The degree of a polynomial is the largest degree of its monomials when fully expanded. For example, if $f(x, y) = x^5y^7 + 100x^6y^6 + 7x^{10}$, then $\deg(f) = 12$. The degree of the zero polynomial is $-\infty$.
Homework 9.1: Prove: $\dim F[x_1, x_2, \ldots, x_k]_n = \binom{n+k}{k}$. Hint: A basis for this space is $\{\prod_{i=1}^k x_i^{j_i} \mid j_i \ge 0, \sum_{i=1}^k j_i \le n\}$. Therefore the dimension of the space is the number of solutions to the inequality $\sum_{i=1}^k j_i \le n$ in nonnegative integers $j_1, \ldots, j_k$.
Fisher's Inequality: Suppose $A_1, \ldots, A_m \subseteq \{1, 2, \ldots, n\}$ are distinct subsets, and $|A_i \cap A_j| = k$ for $i \ne j$ and a fixed $k > 0$. Then $m \le n$.
This is actually a generalization of R. A. Fisher's 1940 inequality which imposed two additional uniformity constraints: all the A_i have equal size, and all elements belong to the same number of sets A_i. In a seminal 1949 note, R. C. Bose eliminated the second uniformity constraint and more importantly, introduced the "linear algebra method" into the theory of extremal set systems. The full result was proved by K. N. Majumdar (1953) by a slight extension of Bose's method. The proof, outlined below and discussed in full in class, can be found in the blue text, Theorem 4.1, p.78.
Def. (Erdős - Rado, 1960) A *sunflower* is a set system $A_1, \ldots, A_m$ such that for every $i \ne j$ we have $A_i \cap A_j = \bigcap_{h=1}^m A_h$. The set $C = \bigcap_{h=1}^m A_h$ is called the *kernel* of the sunflower; the sets $A_i \setminus C$ are the *petals*. The petals are disjoint from each other as well as from the kernel.
Do: Assuming $A_1, \ldots, A_m$ are distinct, nonempty, and form a sunflower, show that their incidence vectors are linearly independent.
Quadratic forms: $q(\mathbf{x}) = \mathbf{x}^T A \mathbf{x}$, positive definite and positive semi-definite quadratic forms and matrices over $\mathbb{R}$.
Do: Show: $q(\mathbf{x}) = \sum_{i=1}^n \sum_{j=1}^n \alpha_{ij} x_i x_j$, where $A = (\alpha_{ij})$ and
$\mathbf{x} = (x_1, \ldots, x_n)^T \in \mathbb{R}^n$.
Do: Prove: if A is positive definite and B is positive semi-definite then $A + B$ is positive definite.
Theorem. If A is positive definite then A is non-singular.
Do: (R.C. Bose) Compute

$$\det \begin{pmatrix} \ell & k & \cdots & k \\ k & \ell & & \vdots \\ \vdots & & \ddots & k \\ k & \cdots & k & \ell \end{pmatrix}$$

as a product of obviously non-zero factors ($\ell > k > 0$).
(Bose's proof of Fisher's inequality for the uniform case (all sets have the same size ℓ) relied on the fact that this matrix is nonsingular, a fact he established by computing its determinant.)

Do: (Majumdar) Compute

$$\det \begin{pmatrix} \ell_1 & k & \cdots & k \\ k & \ell_2 & & \vdots \\ \vdots & & \ddots & k \\ k & \cdots & k & \ell_n \end{pmatrix}$$

as a product of obviously non-zero factors ($\ell_i > k > 0$).
(Majumdar's proof of the most general version of Fisher's inequality, stated above, relied on the fact that this matrix is nonsingular, a fact he established by computing its determinant. Note that using positive definiteness, we have obtained a simpler proof of the nonsingularity of this matrix.)
Do: Show that the diagonal matrix $\text{diag}(\delta_1, \ldots, \delta_n)$ is positive definite if and only if all δ_i are positive.
Zsigmond Nagy's constructive proof (1972) that $\binom{k}{3} \not\to (k+1, k+1)$. (See the blue text, Thm. 4.6 (p. 83))
Puzzle: Prove if k is large enough ($k \geq 9$) and we have a homogeneous red set of size m in Nagy's coloring then $m \leq (k-1)/2$.
Homework 9.2: For $\mathbf{v}_1, \ldots, \mathbf{v}_m \in F^n$ let $\alpha_{ij} = \mathbf{v}_i \cdot \mathbf{v}_j$ and $A = (\alpha_{ij})_{m \times m}$. Prove that if $\det A \neq 0$ then $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent.
Homework 9.3: Find 7 subsets $A_1, \ldots, A_7 \subset \{1, 2, \ldots, 7\}$ such that $|A_i| = 3$ and $|A_i \cap A_j| = 1$ for all $i \neq j$.
Homework 9.4: Count the 3-dimensional subspaces of $\mathbb{F}_p^n$. (Find a closed form expression.)

Lecture 10 - April 11

The Homework below is due on Friday, March 13.

Homework 10.1: Prove: if $A_1, \ldots, A_m$ are distinct k-sets and $m > k!(s-1)^k$ then there is a sunflower with s petals among the A_i. (Hint: induction on k. Note that a set of disjoint sets is a sunflower (with empty kernel).)
Theorem. (Skew Oddtown) Consider the sets $A_1, \ldots, A_m \subseteq \{1, 2, \ldots, n\}$ and $B_1, \ldots, B_m \subseteq \{1, 2, \ldots, n\}$, and the conditions
(1) $|A_i \cap B_i|$ is odd for all i,
(2) $|A_i \cap B_j|$ is even for $i > j$, and
(2') $|A_i \cap B_j|$ is even for $i \neq j$.
Then not only does (1) and (2') imply $m \leq n$ but so does (1) and (2).
The Ray-Chaudhuri – Wilson Theorem (1975) If $A_1, \ldots, A_m \subseteq X$ are distinct, $|X| = n$, $|A_i| = k$ for all i, and $|A_i \cap A_j| \in \{\ell_1, \ldots, \ell_s\}$ for all $i \neq j$, then $m \leq \binom{n}{s}$.
This result is a milestone in the theory of extremal set systems. Its proof was based on higher incidence matrices ("inclusion matrix," blue text Chapter 7.1) and represented a significant extension of Bose's linear algebra method. (See blue text, p87, Theorem 4.10 (statement of result), and p119 (Sec. 5.11, accessible proof via spaces of polynomials).)
The following variations of this fundamental result appear in a seminal paper by Frankl and Wilson (1981).
Non-Uniform version of the Ray-Chaudhuri – Wilson Theorem (Frankl – Wilson, 1981) Fix a prime p. If $A_1, \ldots, A_m \subseteq \{1, 2, \ldots, n\}$ are distinct and

$|A_i \cap A_j| \in \{\ell_1, \dots, \ell_s\}$ for all $i \neq j$, then $m \leq \sum_{i=0}^{s} \binom{n}{i}$.

The original proof of this result, like that of the Ray-Chaudhuri – Wilson Theorem, used higher incidence matrices. The accessible proof via spaces of multivariate polynomials, found by the instructor in 1988 and discussed in full in class, is described in the blue text, Thm 5.17, Sec. 5.10, p117.
Definition of congruence modulo m:
$a \equiv b \pmod{m}$ if $m \mid a - b$. Example: $5 \equiv 54 \pmod{7}$.
We say that $k \in \{\ell_1, \dots, \ell_s\} \pmod{p}$ if $(\exists i)(k \equiv \ell_i \pmod{p})$.
Modular version of the Ray-Chaudhuri – Wilson Theorem (Frankl – Wilson, 1981) Let p be a prime. If $A_1, \dots, A_m \subseteq \{1, 2, \dots, n\}$ are distinct, $|A_i| = k$,

$$|A_i \cap A_j| \in \{\ell_1, \dots, \ell_s\} \pmod{p}$$

for all $i \neq j$ and

$$k \notin \{\ell_1, \dots, \ell_s\} \pmod{p},$$

then $m \leq \binom{n}{s}$. (See blue text, p120.)
This last version is particularly significant because of its wide range of applications, one of which follows.
Explicit Ramsey construction (Frankl and Wilson, 1981): Fix a prime p and let $n > p^2$. Label the $\binom{n}{p^2-1}$ nodes by the (p^2-1)-subsets of an n-set. A line between two nodes labelled A and B is colored red if $|A \cap B| \equiv -1 \pmod{p}$ and colored blue otherwise.
Homework 10.2: Use this explicit construction to prove

$$\binom{n}{p^2-1} \nrightarrow \left(\binom{n}{p-1} + 1, \binom{n}{p-1} + 1 \right).$$

Hint. You need to show that if $A_1, \dots, A_m \subseteq \{1, \dots, n\}$, $|A_i| = p^2 - 1$, and these m sets form a homogeneous subset for the given coloring then $m \leq \binom{n}{p-1}$. On the one hand use the Ray-Chaudhuri – Wilson Theorem, and on the other use Frankl and Wilson's modular version of the Ray-Chaudhuri – Wilson Theorem.
Do: Prove that if $\binom{n}{p^2-1} \nrightarrow (\binom{n}{p-1} + 1, \binom{n}{p-1} + 1)$ then for every C there exists an $N_0 \in \mathbb{N}$ such that for all $N > N_0$ we have $N^C \nrightarrow (N, N)$.