Not Proofread

CMSC 27400-1/37200-1 Combinatorics and Probability **Spring 2005**

Lecture 21: May 18, 2005

Instructor: László Babai *Scribe: Raghav Kulkarni*

NOTE: Change in Monday's TA schedule; no change Tuesday and Thursday.
TA SCHEDULE: TA sessions are held in Ryerson-255, Monday 7:30-8:30,
Tuesday and Thursday 5:30–6:30pm.
INSTRUCTOR'S EMAIL: laci@cs.uchicago.edu
TA's EMAIL: hari@cs.uchicago.edu, raghav@cs.uchicago.edu

Pairwise Independent Random Variables

Homework Problem: If $\exists X_1, \ldots, X_m$ non-constant independent random variables then $|\Omega| \geq 2^m$.
Solution: Consider $(e_1, e_2, \ldots, e_m) \in \{+1, -1\}^m$ i.e., $(\forall i)(e_i \in \{+1, -1\})$.
Let A_i be the event that $X_i = x_i$, where x_i is such that $0 < P(X_i = x_i) < 1$.
$0 < P(A_i) < 1$. For every $(e_1, \ldots, e_m)$, events $\{A_i{}^{e_i} : i = 1, \ldots, m\}$ are independent. where $A_i^1 := A_i$ and $A_i^{-1} = \overline{A_i}$ (complement of A_i).
Consider the event $B(e_1, \ldots, e_m) := \bigcap_{i=1}^m A_i^{e_i}$.
$P(B(e_1, \ldots, e_m)) = \Pi_{i=1}^m P(A_i^{e_i})$ hence nonzero. Therefore, we have 2^m nonempty events $\{B(e_1, \ldots, e_m) : e_i \in \{+1, -1\}\ for\ i = 1, \ldots, m\}$.

Exercise 21.1 *Show that* $\{B(e_1, \ldots, e_m) : e_i \in \{+1, -1\}\ for\ i = 1, \ldots, m\}$ *are* 2^m *disjoint events.*

This shows that $|\Omega| \geq 2^m$.
Problem: If $X_1, \ldots, X_m$ are pairwise independent non-constant random variables then $|\Omega| \geq m + 1$.
Solution: Let $X_0 = 1$ be a constant random variable.

Exercise 21.2 $X_0, X_1, \ldots, X_m$ *are still pairwise independent.*

Claim: $X_0, X_1, \ldots, X_m$ are linearly independent in the space $\mathbb{R}^{|\Omega|}$.
$\dim(\mathbb{R}^{|\Omega|}) = \dim(\mathbb{R}^n) = n = |\Omega|$. Therefore, $n \geq m + 1$.
Proof of the Claim: WLOG $E(X_i) = 0$ for $i = 1, \ldots, m$. (Otherwise replace X_i by $X_i - E(X_i)X_0$.)

Exercise 21.3 *Show that the events are still pairwise independent.*

Define the innner product of random variables X and Y such that $\langle X, Y\rangle = E(XY)$.
Notice that for $i \neq j \quad E(X_iX_j) = E(X_i)E(X_j) = 0$. (independence)
for $i = j \quad E(X_i^2) > 0$. (X_i are non-constant for $i \geq 1$ and $E(X_0^2) = 1$.) Now we prove the linear independence of $\{X_i\}_{i=0}^m$.
Suppose that $\sum_{i=0}^m a_1X_i = 0$.
$0 = E(X_j(\sum_{i=0}^m a_1X_i)) = \sum_{i=1}^m a_iE(X_iX_j) = a_jE(X_j^2)$. But $E(X_j^2) \neq 0$. Therefore, $a_j = 0$ for $j = 0, \ldots, m$.

Exercise 21.4 *Show that this inequality is tight for $n = 2^k$, i.e., on $|\Omega| = 2^k$, we can define $2^k - 1$ pairwise independent non-constant random variables.*

Let $\mathbb{F}$ be a field.
Examples of field: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$.
$\mathbb{F}_p$: integers modulo p where p is a prime.

Exercise 21.5 *Integers mod m is not a field unless m is a prime, (Hint: If m is not a prime then $(\exists x, y \neq 0)(xy = 0)$.)*

Definition: The *order* of a field is the number of elements that it contains.

Theorem 21.6 (Galois) *A finite field of order q exists iff q is a power of a prime. Moreover, for q prime power, $\mathbb{F}_q$ is unique (up to isomorphism).*

Example: An *n-dimensional vector space over* $\mathbb{F} = \mathbb{F}_q$ is defined as $\mathbb{F}^n := \{(a_1, \ldots, a_n) : a_i \in \mathbb{F}\}$.
Definition: A *line* in $\mathbb{F}^n$ is $\{v_0 + tv \ : \ v_0, v \in \mathbb{F}^n, t \in \mathbb{F}\}$.
The number of points in $\mathbb{F}^n$ is q^n.
The number of lines in $\mathbb{F}^n$ is $\frac{q^n(q^n-1)}{q(q-1)}$. (Why?)

Exercise 21.7 $(\forall x \neq y \in \mathbb{F}^n)(\exists$ *a unique line through* $x, y)$.

CORRECTION: (for lecture 21) A3d (third axiom for possibly degenerate projective planes) : $\exists$ 3 points not on a line.
Proposition:
For a possibly degenerate projective plane $\mathcal{G} = (P, L, I)$, $|P| = |L|$.
Proof of the Proposition: $|P| \leq |L|$ (Fisher's inequality) $|L| \leq |P|$ (duality)
Definition: $\mathbb{F}_q^2$ with the lines defined as above and with the natural incidence relation is called the *affine plane over* $\mathbb{F}_q$.
Constructing the projective plane over $\mathbb{F}_q$

An affine plane has q^2 points and $q^2 + q$ lines. The number of lines in each parallel class is q. For each parallel class add a *point at infinity*. The number of new points added is $q+1$. Add a new line which consists of all the new points at infinity. This will give a projective plane of order q. (Why?) We just proved that for every prime power q, there exists a projective plane of order q.