REU Apprentice program

László Babai

Jun 28, 2019

FINITE PROBABILITY SPACES

Reading: Chapter 7 of instructor's online notes,
http://people.cs.uchicago.edu/∼laci/06dm/lecturenotes.pdf

Exercise 1. A club with 2000 members distributes membership cards numbered 1 through 2000 to its members at random; each of the 2000! permutations of the cards is equally likely. Members whose card number coincides with their year of birth receive a prize ("lucky member"). The club legally serves vodka to all of its members. Determine the expected number of lucky members. What is the size of the sample space for this experiment? Indicate how you use the vodka assumption.

In the exercises below, (Ω, P) is a finite probility space. The size of the sample space is $|\Omega| = n$.

Exercise 2. Construct a probability space and 3 events in it that are pairwise but not fully independent. Make your sample space as small as possible.

Exercise 3. Suppose there exist k independent non-trivial events in (Ω, P). Prove: $n \geq 2^k$.

Exercise 4. Suppose there exist k pairwise independent non-trivial events in (Ω, P). Prove: $n \geq k + 1$.

Exercise 5. Show that the inequality in the preceding exercise is tight: for every $k \geq 3$, construct a finite probability space such that $n = k+1$ and there exist k pairwise independent non-trivial events in the space.

Exercise 6. For every $k \geq 2$, construct a finite probability space such that $n \leq 2k$ and there exist k pairwise independent events with probabiliy $1/2$ each in the space.

Exercise 7. For every $k \geq 3$, construct a finite probability space such that $n \leq 4k$ and there exist k triplewise independent events with probabiliy $1/2$ each in the space.

Exercise 8. Suppose there exist k 4-wise independent non-trivial events in (Ω, P). Prove: $n \geq \binom{k+1}{2}$. (Or prove any lower bound that is quadratic in k.)

TOURNAMENTS

DEF. Recall that a **tournament** is an orientation of the complete graph. We call the vertices "players" and the arrow $a \to b$ indicates that player a beat player b. We say that player x **dominates** the set A of players if $(\forall a \in A)(x \to a)$. We say that the tournament is **k-paradoxical** if every set of k players is dominated by some player.

Exercise 9. Construct a 2-paradoxical tournament.

Exercise 10. Prove that for every fixed k, almost all tournaments are k-paradoxical. This means the following. Let $p(n,k)$ denote the probebility that a random tournament with n players is k-paradoxical. Prove that for every k,

$$\lim_{n\to\infty} p(n,k) = 1.$$

Exercise 11. Use the probabilistic method to prove that if $n > 3k^2 2^k$ then there exists a k-paradoxical tournament of n vertices.

QUADRATIC RESIDUES, PALEY TOURNAMENT, WEIL'S CHARACTER SUM ESTIMATE

DEF Let p be a prime and $\mathbb{F}_p$ the finite field of order p (the numbers $0, 1, \dots, p-1$ with modulo p operations). We say that $a \in \mathbb{F}_p$ is a *quadratic residue mod p* if $a \neq 0$ and there exists $x \in \mathbb{F}_p$ such that $a \equiv x^2 \pmod{p}$. a is a quadratic non-residue mod p if no such x exists. We define the *quadratic character* $\chi : \mathbb{F}_p \to \{0, 1, -1\}$ by setting $\chi(0) = 0$, and for $a \neq 0$ we set $\chi(a) = 1$ if a is a quadratic residue and $\chi(a) = -1$ if a is a quadratic non-residue.

Exercise 12. Prove: (a) The number of quadratic residues is $(p-1)/2$.
(b) Prove: $\sum_{a\in\mathbb{F}_p} \chi(a) = 0$.

Exercise 13. Prove: $\chi(a) \equiv a^{(p-1)/2} \pmod{p}$.

Exercise 14 (Multiplicativity)**.** Prove: $\chi(ab) = \chi(a)\chi(b)$.

Exercise 15. Prove: $\left|\sum_{a\in\mathbb{F}_p} \chi(a)\chi(a-1)\right| = 1$.

DEF Let p be a prime, $p \equiv -1 \pmod{4}$. The **Paley tournament** $P(p)$ is defined as follows. The vertices of $P(p)$ are the elements of the field $\mathbb{F}_p$. We draw the arrow $i \to j$ if $j - i$ is a quadratic residue mod p.

Exercise 16. Show that this definition is sound: it indeed defines a tournament. You need to show that every edge is oriented exactly one way. Show where you use the assumption that $p \equiv -1 \pmod{p}$.

Exercise 17. Show that the Paley tournament $P(7)$ is 2-paradoxical.

THEOREM 1 (André Weil's character sum estimate)**.** *Let g be a polynomial of degree d over $\mathbb{F}_p$. Assume g is not of the form $c \cdot h^2$ where $c \in \mathbb{F}_p$ and h is a polynomial over $\mathbb{F}_p$. Then*

$$\left| \sum_{a \in \mathbb{F}_p} \chi(g(a)) \right| \leq (d-1)\sqrt{p}\,.$$

This inequality shows that most terms of the sum on the left-hand side cancel out; the rate of cancellation is essentially the same as if the terms were randomly chosen from $\{1, -1\}$. Indeed, this theorem is a powerful *derandomization tool.*

Exercise 18. Use Weil's character sum estimate to prove that if p is a prime, $p \equiv -1 \pmod 4$, and $p > (k+1)^2 4^k$ then the Paley tournament $P(p)$ is k-paradoxical.

Hint. Let $A \subset \mathbb{F}_p$, $A = \{a_1, \dots, a_k\}$. For $x \in \mathbb{F}_p$ let $f(x) = \prod_{i=1}^{k} (\chi(x - a_i) + 1)$. Show:

- If x dominates A then $f(x) = 2^k$.
- If x lost against one of the a_i then $f(x) = 0$.
- At most one element x_0 is not convered by the two previous bullet points; if there is such an element, then $x_0 \in A$, x_0 dominates $A \setminus \{x_0\}$, and $f(x_0) = 2^{k-1}$.

Now proceed as follows.

(a) For $I \subseteq \{1, \dots, k\}$ let $g_I(x) = \prod_{i \in I} (x - a_i)$. Show that $f(x) = \sum_I \chi(g_I(x))$.

(b) Let N denote the number of players x that dominate A. Consider the sum $S = \sum_{x \in \mathbb{F}_p} f(x)$. Show that $S \leq 2^k N + 2^{k-1}$.

(c) Observe that $S = \sum_I \sum_x \chi(g_I(x))$ where the summation is over all $I \subseteq \{1, \dots, k\}$ and all $x \in \mathbb{F}_p$.

(d) Notice that the term corresponding to $I = \emptyset$ is p. So $S = p + R$ where R is an "error term." Therefore $2^k N \geq p + R - 2^{k-1}$.

(e) Estimate R via Weil's theorem: prove that $|R| < k \cdot 2^k \cdot \sqrt{p}$.

(f) Combine the last two items to show that if $p > (k+1)^2 4^k$ then $N > 0$.

(g) This shows that A is dominated by some x. Since this is true for every $A \subseteq \mathbb{F}_p$ of size $|A| = k$, we conclude that $P(p)$ is k-paradoxical.