REU 2007 - Apprentice program

Linear Algebra Puzzles. Discussion: Mon July 9, 1:30 - 2:30

Instructor: László Babai e-mail: laci@cs.uchicago.edu

1. **(Greatest common divisors)** Consider the $n \times n$ matrix $D = (d_{ij})$ where $d_{ij} = \gcd(i, j)$. Prove: $\det(D) = \prod_{i=1}^{n} \varphi(i)$ where φ denotes Euler's φ function.

2. **(Balancing numbers)** Suppose we have 13 real numbers with the following property: if we remove any one of the numbers, the remaining 12 can be split into two sets of 6 numbers each with equal sum. Prove: all the 13 numbers are equal. (Hint: first assume all the numbers are integers.)

3. **(Commuting matrices)** Let $A_1, \dots, A_m$ and $B_1, \dots, B_m$ be $n \times n$ matrices over a field F such that $A_i B_j = B_j A_i$ if and only if $i \neq j$. Prove: $m \leq n^2$. (Hint: prove that the matrices $A_1, \dots, A_m$ are linearly independent.) (Problem by Miklós Abért.)

4. **(Polynomials)** Prove: every polynomial $f(x) \neq 0$ has a multiple $g(x) = f(x)h(x) \neq 0$ in which every exponent is prime. (So $g(x)$ has the form $\sum_p a_p x^p$ where the summation is over primes.)

5. **(Pirates' secret)** In the sand on a deserted island, explorers find a brittle yellowing sheet of paper telling them that the pirates' secret is hidden in the roots of the polynomial $f(x) = x^{17} + 5x^{16} + 13x^{15} + \dots$. The rest of the sheet is torn off and could not be found. Prove: not all the roots of f are real.

6. **(Rational functions)** Prove that the rational functions $\{1/(x - \alpha) : \alpha \in \mathbb{R}\}$ are linearly independent over $\mathbb{R}$. (This will show that the space of rational functions has uncountable dimension.)

7. **(Hilbert matrix)** Let $a_1, \dots, a_n, b_1, \dots, b_n$ be $2n$ distinct elements of a field F. Prove that the $n \times n$ matrix $H = (h_{ij})$ is nonsingular, where $h_{ij} = 1/(a_i - b_j)$.

8. **(Dimension invariance)** (a) Prove: if the additive groups $(\mathbb{Z}^k, +)$ and $(\mathbb{Z}^m, +)$ are isomorphic then $k = m$. (b) The same is false for $\mathbb{R}$; in fact, the additive group $(\mathbb{R}^k, +)$ is isomorphic to $(\mathbb{R}, +)$ for every k.

9. **(Rank invariance under field extension)** Let $\mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{Q}^n$ be linearly independent over $\mathbb{Q}$. Prove: the same vectors are linearly independent over $\mathbb{C}$ (so even if we permit complex coefficients, there will be no notrivial linear relation among the vectors).

10. **(Cauchy's functional equation)** Find $\mathbb{R} \to \mathbb{R}$ functions f which satisfy the equation $f(x + y) = f(x) + f(y)$ for all $x, y \in \mathbb{R}$. The trivial solutions are the linear functions $f(x) = ax$. (a) Prove: nontrivial solutions exist. (b) A nontrivial solution cannot be (b1) continuous; (b2) continuous at a point; (b3) bounded in an interval; (b4) measurable.

11. **(Intersection matrix)** Let $A_1, \dots, A_{2^n}$ be the 2^n subsets of $[n] = \{1, 2, \dots, n\}$. Consider the $2^n \times 2^n$ matrix $M = (m_{ij})$ where $m_{ij} = |A_i \cap A_j|$. Prove: $\mathrm{rk}(M) = n$. (This is a huge matrix of small rank.)

12. **(Finite fields)** For which primes p do the "mod p complex numbers" $\mathbb{F}_p[i] = \{a + bi : a, b \in \mathbb{F}_p\}$ form a field (where $i^2 = -1$)?

13. **(Chebyshev polynomials)** Define the polynomial $U_n(x)$ by the identity $U_n(cos\alpha) = \sin((n+1)\alpha)/\sin(\alpha)$. So $U_0(x) = 1$, $U_1(x) = 2x$, $U_2(x) = 4x^2 - 1$, $U_3(x) = 8x^3 - 4x$, $U_4(x) = 16x^4 - 12x^2 + 1$, etc. (a) Show that $U_n(x)$ is a polynomial of degree n with integer coefficients. (These are "Chebyshev's polynomials of the second kind.") (b) Prove that all the n roots of U_n are real. (c) Let $T = (t_{ij})$ be the $n \times n$ tridiagonal matrix with $t_{ii} = 2x$ in the diagonal, and $t_{i-1,i} = 1$ and $t_{i,i-1} = 1$ (1s immediately above and below the diagonal), and zero everywhere else. Prove: $\det(T) = U(x)$. (d) Prove: $\sum_{n=0}^{\infty} U_n(x)t^n = 1/(1 - 2xt + t^2)$. (e) Prove: $(-i)^n U_n(i/2)$ is the n-th Fibonacci number (where $i = \sqrt{-1}$). (f) Prove: the U_n are orthogonal in $C[-1, 1]$ with respect to the weight function $\sqrt{1 - x^2}$.

14. **(Oddtown Theorem)** In Oddtown, there are n citizens and m clubs satisfying the rules that each club has an odd number of members and each pair of clubs shares an even number of members. (a) Prove: $m \leq n$. (Hint: prove that the incidence vectors of the clubs are linearly independent over $\mathbb{F}_2$.) (b) Show that it is possible to have n clubs in Oddtown. (c) Show that if n is even, there are more than $2^{n^2/8}/(n!)^2$ nonisomorphic Oddtown club systems with n clubs. (d) Show that for every n, there are *maximal* clubs systems with at most two clubs in Oddtown. (A club system is *maximal* if no more club can be added without violating the constraints.)

15. **(Maximal Eventown systems)** In Eventown, each club has an even number of members, each pair of clubs shares an even number of members, and no two clubs have identical membership. We proved in class that there are at most $2^{\lfloor n/2 \rfloor}$ clubs in Eventown. (a) Prove: every *maximal* Eventown club system is *maximum.* In other words, if there are fewer than $2^{\lfloor n/2 \rfloor}$ clubs in Eventown, one can add a club. (Note the contrast with Oddtown.) (b) Prove: for all sufficiently large n, there exist maximum Eventown club systems that are not isomorphic to the "married couples" system. (In the "married couples" system, there are $\lfloor n/2 \rfloor$ couples; the couples join clubs together; if n is odd, the one unmarried citizen is banned from all clubs.) (c) Prove that for all sufficiently large odd n there exist maximum Eventown club systems in which all citizens belong to at least one club. (d) Research question: if n is odd, are there maximum systems in which each citizen participates in (d1) exactly (d2) approximately the same number of clubs?

16. **(Committee sharing a secret key)** The president sets up an emergency committee of 7 members. A 25-digit secret number gives access to a safe. The president wants to ensure that if any 4 members of the committee get together then they can open the safe, but if only 3 of them join forces, they will never have the faintest idea of the secret number.

    A mathematician advises the president to make up a polynomial over a finite field, of which the constant term is the secret number. Find the specifics of the mathematician's advice (what degree polynomial, over what field, how to generate the coefficients, what info to give each member of the committee).