

Discrete Math, 10th day, Friday 7/9/04
REU 2004. Info:
<http://people.cs.uchicago.edu/~laci/reu04>.

Instructor: László Babai
Scribe: Ivona Bezáková

1 Cauchy-Hilbert Matrix

The **Hilbert matrix** is defined as:

$$\begin{bmatrix} \frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \cdots & \frac{1}{n+1} \\ \vdots & & & & \vdots \\ \frac{1}{n} & \frac{1}{n+1} & \frac{1}{n+2} & \cdots & \frac{1}{2n-1} \end{bmatrix}$$

The Hilbert matrix is a special case of a **Cauchy matrix**:

$$\begin{bmatrix} \frac{1}{\alpha_1 - \beta_1} & \frac{1}{\alpha_1 - \beta_2} & \frac{1}{\alpha_1 - \beta_3} & \cdots & \frac{1}{\alpha_1 - \beta_n} \\ \frac{1}{\alpha_2 - \beta_1} & \frac{1}{\alpha_2 - \beta_2} & \frac{1}{\alpha_2 - \beta_3} & \cdots & \frac{1}{\alpha_2 - \beta_n} \\ \vdots & & & & \vdots \\ \frac{1}{\alpha_n - \beta_1} & \frac{1}{\alpha_n - \beta_2} & \frac{1}{\alpha_n - \beta_3} & \cdots & \frac{1}{\alpha_n - \beta_n} \end{bmatrix}$$

Exercise 10.1. Prove: If all α_i, β_i are distinct then the Cauchy-Hilbert matrix has full rank.

2 Cauchy's Functional Equation

Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be a real function.

Definition 10.2. Cauchy's functional equation specifies:

$$(\forall x, y)(f(x + y) = f(x) + f(y)).$$

Which functions are solutions to Cauchy's functional equation (CFE)? Clearly, $f(x) = cx$ is a solution.

We will make several observations: if f satisfies CFE then

1. $f(0) = 0$. (Why?)
2. Let $c := f(1)$. Then $(\forall x \in \mathbb{Z})(f(x) = cx)$.
3. $f(p/q) = c \cdot p/q$ for $p, q \in \mathbb{Z}$. (Why?)

Therefore $(\forall x \in \mathbb{Q})(f(x) = cx)$.

Exercise 10.3. If f is continuous then $(\forall x)(f(x) = cx)$.

Exercise 10.4. If f is a solution of CFE and it is bounded in an interval then $(\forall x)(f(x) = cx)$.

This is a known fact from linear algebra:

Definition 10.5. Let \mathbb{F} be a field and U, W vector spaces over \mathbb{F} . A function $\varphi : V \rightarrow W$ is called **linear** if $(\forall x, y \in V)(\varphi(x + y) = \varphi(x) + \varphi(y))$ and $(\forall x \in V)(\forall \alpha \in \mathbb{F})(\varphi(\alpha x) = \alpha\varphi(x))$.

Lemma 10.6. Let \mathbb{F} be a field and V, W be two vector spaces over \mathbb{F} . Suppose $B \subseteq V$ be a basis and $\varphi : B \rightarrow W$ be an arbitrary function. Then φ can be uniquely extended to a linear function $\varphi : V \rightarrow W$.

Hamel basis H is a basis of \mathbb{R} over \mathbb{Q} (its existence is implied by Zorn's Lemma). Its cardinality is **continuum**, denoted as \mathfrak{c} . CFE translates to finding all \mathbb{Q} -linear (linear over \mathbb{Q}) functions $f : \mathbb{R} \rightarrow \mathbb{R}$. Using previous lemma we can define the function f by assigning a value $f(h)$ to every vector h in the Hamel basis.

Corollary 10.7. There are solutions to CFE not of the form $f(x) = cx$. In fact in $\alpha_1, \alpha_2, \dots$ are linearly independent over \mathbb{Q} then $f(\alpha_1), f(\alpha_2), \dots$ can be independently prescribed.

3 Number Theory

Exercise 10.8. Pick two positive integers x, y at random, what is the probability that x, y are relatively prime? (HINT. What does "integer chosen at random" mean? We want all integers to be chosen with the same probability. First make sense out of the problem statement. You will define the probability as a limit. Assume the limit exists. Then use $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.)

A little diversion: $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$ was stated by Fermat and proved by Leonhard Euler. Other examples of Fermat's theorems that Euler worked on include Fermat's Last Theorem stating that $x^n + y^n = z^n$, $n \geq 3$ implies $xyz = 0$ (recently proved by Andrew Wiles), and the following remarkable result:

Exercise 10.9. Let $p > 2$ be a prime. Prove that $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod{4}$.

Exercise 10.10. Prove that $\mathbb{F}_p[\sqrt{-1}] = \{a + bi \mid a, b \in \mathbb{F}_p\}$ (“complex numbers mod p ”) is a field if and only if $p \equiv -1 \pmod{4}$.

Exercise 10.11. Let $\{a_i\}_{i=0}^\infty$ be defined as $a_0 = 1$, $a_{n+1} = \sqrt{2^{a_n}}$. Prove that $(\forall n)(a_n < 2)$.

Exercise 10.12. Prove that $a_n \rightarrow 2$ for the a_i from the previous exercise.

Exercise 10.13. Find the maximum r s.t. $r^{r^{r^{\dots}}}$ is bounded.

Exercise 10.14. Find two infinite sets $A, B \subseteq \mathbb{N} = \{0, 1, 2, \dots\}$ such that for every $n \in \mathbb{N}$ there exist unique $a \in A$ and $b \in B$ such that $a + b = n$. (HINT. Look at the digits of the integers. Recall Hales-Jewett’s implies the Van der Waerden’s Theorem.)

4 Ramsey Theory

By Erdős-Szekeres $N = \binom{k+\ell-2}{k-1} \rightarrow (k, \ell)$, i.e. if G is a graph with N vertices then G contains a K_k or \overline{G} contains a K_ℓ . Turán’s example, a graph of n^2 vertices consisting of n independent copies of K_n , shows that $n^2 \not\rightarrow (n+1, n+1)$. The following theorem states a much stronger result.

Theorem 10.15 (Erdős). $2^{n/2} \not\rightarrow (n+1, n+1)$

In other words, $N \not\rightarrow (2 \log_2 N + 1, 2 \log_2 N + 1)$. The proof is based on the “probabilistic method.”

Corollary 10.16. If $2 \binom{n}{k} \leq 2 \binom{k}{2}$ then $n \not\rightarrow (k, k)$.

Exercise 10.17. Prove: $\binom{n}{k} \leq \frac{n^k}{k!}$.

We know that $4^n \rightarrow (n+1, n+1)$ (why?), i.e. $N \rightarrow (1/2 \log N, 1/2 \log N)$. By the above $N \not\rightarrow (2 \log N + 1, 2 \log N + 1)$. There is a multiplicative gap of 4 between the lower bound and the upper bound.

Open problems.

- (1) Shrink this gap: either prove $N \rightarrow ((\frac{1}{2} + \varepsilon) N, (\frac{1}{2} + \varepsilon) N)$ or prove $N \not\rightarrow ((2 - \varepsilon) N, (2 - \varepsilon) N)$.
- (2) Prove: $(\exists c)(\forall \varepsilon > 0)(\exists n_0)(\forall n > n_0)(n \rightarrow ((c - \varepsilon) n, (c - \varepsilon) n)$ and $n \not\rightarrow ((c + \varepsilon) n, (c + \varepsilon) n)$)