2015 Chicago Math REU Apprentice Program Exercises
Monday, July 6

Instructor: László Babai
Notes by Yiguang Zhang

11.1 Permutations

Exercise 11.1. Prove: (a) the transpositions generate $S_n$. (b) The transpositions of the form $(i, i + 1)$ ("neighbor-swaps") generate $S_n$.

Exercise 11.2. Recall that two permutations $\pi, \sigma$ are conjugate if there exists a permutation $\tau$ such that $\pi = \tau^{-1}\sigma\tau$. Prove: two permutations are conjugate if and only if they have the same cycle structure.

Exercise 11.3. For a permutation $\pi$, define $\text{sgn}(\pi) = \begin{cases} +1 & \text{if } \pi \text{ is even} \\ -1 & \text{if } \pi \text{ is odd} \end{cases}$. Prove: for any permutations $\sigma$ and $\pi$, it holds that $\text{sgn}(\sigma\pi) = \text{sgn}(\sigma)\text{sgn}(\pi)$.

Exercise 11.4. Two permutations $\pi$ and $\tau$ are said to commute if $\pi\tau = \tau\pi$. The support of a permutation $\tau$ is the set $\text{Supp}(\tau) := \{i \in [n] : \tau(i) \neq i\}$ of elements actually moved by $\tau$. Show the following:

1. If $\text{Supp}(\pi) \cap \text{Supp}(\tau) = \emptyset$, then $\pi$ and $\tau$ commute.
2. It is not necessarily true that if $\pi$ and $\tau$ commute, then $\text{Supp}(\pi) \cap \text{Supp}(\tau) = \emptyset$.

Exercise 11.5. Let $m_n$ be the maximum order of a permutation in $S_n$. Estimate $\log(m_n)$ within a constant factor. (Hint. Use the Prime Number Theorem: $\pi(x) \sim x/\ln x$ where $\pi(x)$ denotes the number of primes $\leq x$.)

Exercise 11.6. Let $c_1(\pi)$ denote the length of the cycle passing through the number 1 in the permutation $\pi$. Prove: for any $i = 1, \ldots, n$, for a random permutation $\pi$ selected uniformly from $S_n$, we have $\mathbb{P}_{\pi \in S_n}[c_1(\pi) = i] = \frac{1}{n}$.

11.2 Finite Probability Spaces

Exercise 11.7. Study finite probability spaces from the instructor’s Discrete Mathematics Lecture Notes (Chap. 7).
Exercise 11.8. For an event $A \subseteq \Omega$, define the indicator variable $\vartheta_A(x)$ to be the random variable such that

$$\vartheta_A(x) = \begin{cases} 1 & \text{if } x \in A; \\ 0 & \text{otherwise.} \end{cases}$$

Prove that $\mathbb{E}(\vartheta_A) = \mathbb{P}(A)$.

Exercise 11.9. Let $X, Y : \Omega \to \mathbb{R}$ be two random variables. Prove that

$$\mathbb{E}(X + Y) = \mathbb{E}(X) + \mathbb{E}(Y).$$

Exercise 11.10. Read “How to be alien” by George Mikes.

Exercise 11.11. Prove using the Binomial Theorem that

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

Exercise 11.12. Prove that

$$\sum_{k=0}^{\infty} \binom{n}{2k} = 2^{n-1}.$$

Exercise 11.13. Prove that

$$\left| \sum_{k=0}^{\infty} \binom{n}{3k} \frac{2^n}{3} \right| < 1.$$

Exercise 11.14. Let $S(n, d) = \sum_{k=0}^{\infty} \binom{n}{kd}$.

1. Find the values of $n$ for which $S(n, 4) = 2^{n-2}$.

2. * Find a closed-form expression for $S(n, k)$ for every $k$ and estimate $|S(n, k) - \frac{2^n}{k}|$.
   (Hint: use the binomial theorem).

Exercise 11.15. We count fixed points of a permutation as a cycle. Prove:

$$\mathbb{E}_{\pi \in S_n}[\text{number of cycles in } \pi] \sim \ln n.$$

11.3 Linear Algebra

Let $V$ and $W$ denote vector spaces.

Exercise 11.16. Prove: $S \subseteq V$ is a basis for $V$ if and only if, for any $v \in V$, $v$ can be written uniquely as a linear combination of elements in $S$.

Exercise 11.17. Prove: if $\text{dim}(V) = n$, then $V \cong \mathbb{R}^n$.

Exercise 11.18. Prove: $\mathbb{R}^n \cong \mathbb{R}^m$ if and only if $n = m$.

Exercise 11.19. Let $f : V \to W$ be a homomorphism. Prove: if $S \subseteq V$ is linearly dependent, then $f(S)$ is linearly dependent.
Exercise 11.20. Let \( f : V \to W \) be a homomorphism. Let \( 0_V \) denote the zero element of \( V \). Prove that \( f(0_V) = 0_W \).

Exercise 11.21. Prove: if \( e_1, \ldots, e_n \in V \) is a basis in \( V \) and \( w_1, \ldots, w_n \) are arbitrary vectors in \( W \) then there exists a unique homomorphism \( f : V \to W \) such that \( f(e_i) = w_i \) for all \( i \).

Exercise 11.22. Prove: if \( A = \{f_0, f_1, \ldots, f_n\} \subseteq \mathbb{R}[x] \) satisfies \( \deg(f_i) = i \), then \( A \) is a basis of \( \mathbb{R}^{\leq n}[x] \). Recall that \( \mathbb{R}[x] \) denotes the vector space of polynomials over the reals, and \( \mathbb{R}^{\leq n}[x] \) denotes the subspace consisting of the polynomials of degree at most \( n \).

Exercise 11.23. Let \( f : V \to W \) be a homomorphism. Prove that

1. \( \ker(f) \leq V \).
2. \( \text{im}(f) \leq W \).
3. \( \dim[\ker(f)] + \dim[\text{im}(f)] = \dim(V) \).

Exercise 11.24. The circulant matrix generated by the sequence \( (a_0, \ldots, a_{n-1}) \) is defined as

\[
C(a_0, \ldots, a_{n-1}) = \begin{pmatrix}
a_0 & a_1 & a_2 & \cdots & a_{n-1} \\
a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
a_1 & a_2 & a_3 & \cdots & a_0
\end{pmatrix},
\]

where \( a_0, \ldots a_{n-1} \) can be any complex number.

1. Prove: the determinant of the circulant is a product of linear forms of the \( a_j \), so that one can write

\[
\det(C(a_0, \ldots, a_{n-1})) = \prod_{i=0}^{n-1} L_i(a_0, \ldots, a_{n-1}),
\]

where \( L_i \) denotes a linear expression. Hint: \( L_0(a_0, \ldots, a_{n-1}) = \sum_{j=1}^{n} a_j \).

2. Find an eigenbasis for \( C(a_0, \ldots, a_{n-1}) \) in \( \mathbb{C}^n \) – it will be the same eigenbasis for any choice of \( (a_0 \ldots a_{n-1}) \). (An eigenbasis of the matrix \( A \) in \( \mathbb{C}^n \) is a basis of \( \mathbb{C}^n \) consisting of eigenvectors of \( A \).)