REU 2007 · Discrete Mathematics · Lecture 1

Instructor: László Babai
Scribe: Sundeep Balaji

July 18, 2007. Revised by instructor. Last updated July 19 at 3:30 p.m.

1.1 Graphs

Refer to Section 6.1 in the **Discrete Mathematics Lecture Notes** (DMLN) handed out in class (also available online on this website). The concepts of graphs, subgraphs, degree of a vertex, isomorphism between graphs, girth of a graph, Hamilton cycle, independence number $\alpha(X)$, legal coloring, k-colorability, chromatic number $\chi(X)$, complement of graphs were introduced. Unless specified otherwise, n always denotes the number of vertices of the graph $X = (V, E)$.

The maximum number of edges in a graph with n vertices is $\binom{n}{2}$.

Exercise 1.1.1. Prove that the Petersen graph has no Hamilton cycle. (In contrast to most exercises which have elegant solutions, this one does not appear to.)

Question 1.1.2. Are the graphs Figure 6.8 and Figure 6.9 in DMLN isomorphic?

Let C_n denote the cycle of length n. Then its independence number, $\alpha(C_n) = \lfloor \frac{n}{2} \rfloor$.

Exercise 1.1.3. Find the independence number of the 5×5 toroidal grid. (In this graph, every vertex has degree 4.)

For the Rook's graph on an 8×8 chessboard, $\alpha = 8$ and the number of independent sets of maximum size is 8!. - Examples of self-complemantary graphs ($X \cong \overline{X}$): the graph with one vertex (K_1), the path of length 3 (P_4), cycle of length 5 (C_5).

Exercise 1.1.4. If $X \cong \overline{X}$, then $n \equiv 0, 1 \pmod 4$.

For a graph X, the clique number is $\omega(X) = \alpha(\overline{X}) \leq \chi(X)$.

Exercise 1.1.5. Construct a triangle-free graph with $\chi = 4$. (Hint: 11 vertices and 5-fold symmetry. This graph is known as Grötzsch's graph.)

Exercise 1.1.6. Prove $(\forall k)(\exists$ triangle-free graph $X)(\chi(X) \geq k)$.

Exercise 1.1.7. Prove: if X is triangle-free then $\chi(X) \leq 2\sqrt{n} + 1$.

Note that $\chi(X) = n \Leftrightarrow X \cong K_n$, where K_n is the n-*clique* (complete graph on n vertices).

Exercise* 1.1.8. Prove $(\forall k, \ell)(\exists X)$ ((a) X has no *odd* cycle of length $\leq \ell$ (b) $\chi(X) \geq k$).

Exercise 1.1.9 (Erdős 1959).** Prove $(\forall k, \ell)(\exists X)$ ((a) X has no cycle of length $\leq \ell$ (b) $\chi(X) \geq k$).

The following is a preview from weeks 5–8 and provides an explanation of the difficulty of proving 1.1.9.

Theorem 1.1.10 (Erdős-Hajnal). *(1) For any infinite cardinal k and any integer ℓ, 1.1.8 above is true. (2) For infinite chromatic numbers, 1.1.9 above fails badly: If X has no cycle of length 4 then $\chi(X)$ is countable.*

1.2 Groups

Look up the definition of a group and a commutative group (also called abelian group) in Wikipedia.

Example 1.2.1. $(\mathbb{Z}, +), (\mathbb{Z}_n, +)$, the general linear group $\mathrm{GL}_2(p)$ (2×2 matrices over $\mathbb{Z}_p$ with nonzero determinant (nonzero mod p)), the special linear group $\mathrm{SL}_2(p)$ (the subgroup of $\mathrm{GL}_2(p)$ consisting of those matrices with determinant $= 1 \pmod{p}$)

Exercise 1.2.2. If p is a prime $(\mathbb{Z}_p^\times, \cdot)$ is a group. Here $\mathbb{Z}_p^\times$ is the set of non-zero integers modulo p.

Definition 1.2.3. Let G be a group. $S \subset G$ is said to be **product-free** is $(\forall x, y, z \in S)(xy \neq z)$. Let $\alpha(G) =$ largest size of a product free set in G.

Exercise 1.2.4. Prove (a) $\alpha(\mathbb{Z}_n) \geq \frac{n-1}{3}$ (b) $\alpha(\mathbb{Z}_n) \geq \frac{2n}{7}$ $(n \geq 2)$

Question 1.2.5. (Babai–Sós, 1982) $(\exists c > 0)(\forall \text{finite } G, |G| \geq 2)(\alpha(G) \geq c|G|)$?

In 2006, Fields medalist Tim Gowers proved that if $n = |\mathrm{SL}_2(p)|$ then $\alpha(\mathrm{SL}_2(p)) < cn^{8/9}$. Hence the answer to the question is no. His proof uses "algebraic graph theory" (graph theory plus linear algebra) and "representation theory" (group theory plus linear algebra). We shall hopefully see the complete proof by the end of week 4.

Exercise 1.2.6. Calculate $|\mathrm{SL}_2(p)|$. (Give a very simple exact formula.)

1.3 Linear Algebra

Definition 1.3.1. A **vector space** V over a field F of scalars (think of real numbers) is an abelian group where we can multiply by scalars such that $(\forall \alpha, \beta \in F, v, w \in V)((\alpha\beta)v = \alpha(\beta v), (\alpha + \beta)v = \alpha v + \beta v, \alpha(v + w) = \alpha v + \alpha w, 1 \cdot v = v)$.

Example 1.3.2. $C[0, 1] =$ continuous real-valued functions on $[0, 1]$, $\mathbb{R}^n = n \times 1$ column vectors with real entries.

Definition 1.3.3. $v_1, \ldots, v_k$ are said to be **linearly independent over** F if $(\forall \alpha_1, \ldots, \alpha_k \in F)(\sum_{i=1}^{k} \alpha_i v_i = 0 \;\Rightarrow\; \alpha_1 = \ldots = \alpha_k = 0)$.

Exercise 1.3.4. Find a curve in $\mathbb{R}^n$ such that any n points are linearly independent (give a simple explicit formula).

Exercise 1.3.5. $\mathbb{R}$ is a vector space over $\mathbb{Q}$. Prove that $1, \sqrt{2}, \sqrt{3}$ and more generally the square roots of all square-free positive integers (integers not divisible by the square of any prime) are linearly independent over $\mathbb{Q}$.

Definition 1.3.6. **Span**$(v_1, \ldots, v_k) = \{\sum \alpha_i v_i \mid \alpha_i \in \text{ scalars}\}$. $v_1, \ldots, v_k$ generake V if their span is V. A **basis** of V is a linearly independent set of generators.

Example 1.3.7. $\mathbb{R}[x] = \{\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \mid a_i \in \mathbb{R}, n \in \mathbb{N}\}$ = the space of polynomials with real coefficients. An $\mathbb{R}$-basis is $\{1, x, x^2, x^3, \ldots\}$.

Exercise 1.3.8. If $f_0, f_1, \ldots \in \mathbb{R}[x]$ and $\deg(f_i) = i$, then $f_0, f_1, \ldots$ form an $\mathbb{R}$-basis of $\mathbb{R}[x]$.

Exercise 1.3.9. Every linearly independent set can be extended to a basis and every set of generators contains a basis.

Exercise 1.3.10. Any two basis of the same vector space have the same cardinality which is called the dimension. Equivalently, if L is a linearly independent set and G is a set of generators then $|L| \leq |G|$.

Exercise 1.3.11. $v_1, v_2, \ldots, v_k$ is a basis if and only if every vector is a unique linear combination of the v_i.

If $v_1, \ldots, v_k$ is a basis and $w = \alpha_1 v_1 + \cdots + \alpha_k v_k$ then $\alpha_1, \ldots, \alpha_k$ are the **coordinates** of w with respect to this basis. Arranging the coordinates as a $k \times 1$ column vector, we get a bijection between V and F^k which preserves linear combinations (such a bijection is called an **isomorphism**); therefore $V \cong F^k$. Hence a vector space is characterized, up to isomorphism, by its dimension and the field of scalars.

Exercise 1.3.12. If $F = \mathbb{F}_p$ and V is a k-dimensional vector space over F, then $|V| = p^k$.

1.4 Combinatorics

Exercise 1.4.1. $\binom{n}{n/2}/2^n > 1/n$. In fact, $\binom{n}{n/2}/2^n \sim \frac{c}{\sqrt{n}}$ where $c = \sqrt{2/\pi}$. (**READ** about **asymptotic equality** $(\sim)$ from Section 2.2 in DMLN.)

Exercise 1.4.2. If there are n people, and they can form clubs such that (a) no two clubs have the exact same set of members; (b) every club has an even number of members; and (c) any two clubs have an even number of members in common ("Eventown Rules") then prove that the maximum number of clubs that can be formed is $2^{\lfloor \frac{n}{2} \rfloor}$. (Hint: Linear algebra modulo 2)