CSC/MATH 870 – Computational Discrete Geometry

Lecture 2 (9/12/05)

1 Sets

Like the concepts of point and line in Euclidean geometry, in mathematics, the terms *set* and *set membership* are fundamental objects used to define other mathematical objects, and so are not themselves formally defined. However, informally, a set can be thought of as a well-defined collection of objects considered as a whole. The objects of a set are called *elements* or members. The elements of a set can be anything: numbers, people, letters of the alphabet, other sets, and so on. Two sets A and B are said to be *equal*, written $A = B$, if they have the same members. The set equality $A = B$ is equivalent to the two *subset* relations $A \subseteq B$ and $B \subseteq A$. Here

$$A \subseteq B \qquad \text{means that for all } x, \qquad x \in A \;\Rightarrow\; x \in B \;.$$

The symbol $\Rightarrow$ means "implies". "$\heartsuit \Rightarrow \clubsuit$" is equivalent to "if $\heartsuit$ then $\clubsuit$". The symbol $\supseteq$ is also used: $B \supseteq A$ means $A \subseteq B$. The *intersection* of A and B is

$$A \cap B := \{x : \; x \in A \text{ and } x \in B\} \;.$$

The *union* of A and B is

$$A \cup B := \{x : \; x \in A \text{ or } x \in B\} \;.$$

From two sets A and B, we obtain a new set

$$A \times B = \{(a, b) : \; a \in A \text{ and } b \in B\} \;.$$

A symbol of the form (a, b) is called an *ordered pair*. The set $A \times B$ is called the (*cartesian*) *product* of A and B.

Example. Here are some sets that we will encounter in the course.

- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$;
- $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, $\mathbb{R}^3$, $\mathbb{R}^4$, $\ldots$;
- the *(affine) halfspace* $\big\{x \in \mathbb{R}^d : \; a \cdot x \leq b\big\}$, for some $a \in \mathbb{R}^d, b \in \mathbb{R}$;
- the *(affine) hyperplane* $\big\{x \in \mathbb{R}^d : \; a \cdot x = b\big\}$, for some $a \in \mathbb{R}^d, b \in \mathbb{R}$;
- the *affine subspace* $\big\{x \in \mathbb{R}^d : \; A\,x = b\big\}$, for some matrix $A \in \mathbb{R}^{m \times d}$ and some $b \in \mathbb{R}^m$;
- the *linear subspace* $\big\{x \in \mathbb{R}^d : \; A\,x = 0\big\}$, for some matrix $A \in \mathbb{R}^{m \times d}$;
- the line segment $L := \big\{(x, y) \in \mathbb{R}^2 : \; x, y \geq 0,\, x + y = 1\big\}$, which can also be described as the intersection of the affine subspace $\big\{(x, y) \in \mathbb{R}^2 : \; x + y = 1\big\}$ with the nonnegative quadrant $\mathbb{R}^2_{\geq 0}$;

- $\{(0,1),(1,0)\} = L \cap \mathbb{Z}^2$.

The *empty set* is the set with no elements. It is denoted $\emptyset$ or $\{\}$. The empty set is "extreme" in that it is the smallest possible set. $S \neq \emptyset$ if and only if there is an x such that $x \in S$. One would like to go to the other extreme and define a set that contains "everything"; however, we know since at least the days of Bertrand Russell that such a set is hard to come by. (Consider the set $S = \{X : \ X \text{ is a set and } X \notin X\}$. Is the sentence $S \in S$ true or false?) For two sets A and B, we define the *set difference*

$$A - B = \{x : \ x \in A \text{ and } x \notin B\} \ .$$

Given a set $A \subseteq X$, we define the *complement* of A in X to be $X - A$.

Example. The even integers are the complement of the odd integers in $\mathbb{Z}$.

If the "universal set" X is clear from the context, we often write $\overline{A}$ or A^c for the complement of A (in X). The famous *DeMorgan laws* assert that for two subsets $A, B \subseteq X$,

$$(A \cup B)^c = A^c \cap B^c \qquad \text{and} \qquad (A \cap B)^c = A^c \cup B^c.$$

2 Relations and functions

A *relation* on a set A is a subset of $A \times A$. Given a relation $R \subseteq A \times A$, we often write $x \sim y$ instead of $(x, y) \in R$.

Example. Some familiar examples for relations $a \sim b$ in $\mathbb{Z}$ are:

- $a = b$
- $a < b$
- $a \leq b$
- $a|b$ (a divides b).

The relation $R \subseteq A \times A$ is an *equivalence relation* if it has the following three properties:

(i) $a \sim a$ for all $a \in A$ (reflexivity)

(ii) $a \sim b$ implies $b \sim a$ (symmetry)

(iii) $a \sim b$ and $b \sim c$ imply $a \sim c$ (transitivity).

Example. Of the above examples of relations $a \sim b$, only the one defined by $a = b$ is an equivalence relation.

The *equivalence class* of $a \in A$ is $[a] := \{b \in A : \ b \sim a\}$. Equivalence classes divide the underlying set A in the following sense:

(i) For $a_1, a_2 \in A$, either $[a_1] = [a_2]$ or $[a_1] \cap [a_2] = \emptyset$.

(ii) For every $a \in A$, there is an equivalence class containing a.

In mathematical terms, the equivalence classes (with respect to a given equivalence relation on A) form a *partition* of A.

Example. Given a fixed $n \in \mathbb{N}$, we define the relation $\equiv$ on $\mathbb{Z}$ by $x \equiv y$ if and only if $x - y$ is divisible by n. The relation $\equiv$ is an equivalence relation on $\mathbb{Z}$; it has exactly n distinct equivalence classes, namely $[0]$, $[1]$,...,$[n-1]$. This set of equivalence classes is called the *set of integers modulo* n, written $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$. One can define addition and multiplication operations on $\mathbb{Z}_n$ and see that these axioms satisfy many (but not all) of the axioms for integers.

A *function* f with *domain* A and *codomain* B is a rule which assigns to each $a \in A$ one and only one element $f(a)$ of B. We write $f : A \to B$. The *graph* of this function is

$$\Gamma(f) = \{(a, b) \in A \times B : \ b = f(a)\} \ .$$

The graph is a subset of $A \times B$ which has exactly one member with first entry a for each $a \in A$. The graph of a function $f : A \to A$ is a special case of a relation (for which there is only one $(x, y) \in R$ for every $x \in A$).

Example. Here's a sample of functions:

- $s : \mathbb{R} \to \mathbb{R}$ defined through $s(x) = x^2$;
- $s : \mathbb{R} \to \mathbb{R}_{\geq 0}$ defined through $s(x) = x^2$;
- $s : \mathbb{Z} \to \mathbb{Z}$ defined through $s(x) = x^2$;
- $p : \mathbb{R}^2 \to \mathbb{R}$ defined through $p(x, y) = x + y$;
- $f : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ defined through $f(0) = 0$, $f(1) = 1$, and $f(k+2) = f(k+1) + f(k)$ for $k \geq 0$.

3 Recursions and generating functions

The last example is an instance of a *recursive sequence*. It is the famous *Fibonacci sequence* $(f_k)_{k=0}^{\infty} = (0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \dots)$ defined through

$$f_0 = 0, \ f_1 = 1, \quad \text{and} \quad f_{k+2} = f_{k+1} + f_k \quad \text{for} \quad k \geq 0 \ .$$

My favorite way of dealing with recursive sequence is through *generating functions*. Let

$$F(x) = \sum_{k \geq 0} f_k \, x^k.$$

We embed both sides of the recursion identity into their generating functions:

$$\sum_{k \geq 0} f_{k+2} \, x^k = \sum_{k \geq 0} (f_{k+1} + f_k) \, x^k = \sum_{k \geq 0} f_{k+1} \, x^k + \sum_{k \geq 0} f_k \, x^k. \tag{1}$$

The left–hand side of (1) is

$$\sum_{k\geq 0} f_{k+2}\, x^k = \frac{1}{x^2} \sum_{k\geq 0} f_{k+2}\, x^{k+2} = \frac{1}{x^2} \sum_{k\geq 2} f_k\, x^k = \frac{1}{x^2}\,(F(x) - x)\,,$$

while the right–hand side of (1) is

$$\sum_{k\geq 0} f_{k+1}\, x^k + \sum_{k\geq 0} f_k\, x^k = \frac{1}{x} F(x) + F(x)\ .$$

So (1) can be restated as

$$\frac{1}{x^2}\,(F(x) - x) = \frac{1}{x} F(x) + F(x)$$

or

$$F(x) = \frac{x}{1 - x - x^2}\ .$$

It's fun to check (e.g., with a computer) that when we expand the function F into a power series, we indeed obtain the Fibonacci numbers as coefficients:

$$\frac{x}{1 - x - x^2} = x + x^2 + 2\,x^3 + 3\,x^4 + 5\,x^5 + 8\,x^6 + 13\,x^7 + 21\,x^8 + 34\,x^9 + \cdots\ .$$

Now we use our favorite method of handling rational functions from Calculus: a *partial-fractions expansion*. In our case, the denominator factors as $1 - x - x^2 = \left(1 - \frac{1+\sqrt{5}}{2}\, x\right)\left(1 - \frac{1-\sqrt{5}}{2}\, x\right)$, and the partial-fractions expansion is

$$F(x) = \frac{x}{1 - x - x^2} = \frac{1/\sqrt{5}}{1 - \frac{1+\sqrt{5}}{2}\, x} - \frac{1/\sqrt{5}}{1 - \frac{1-\sqrt{5}}{2}\, x}\ .$$

The two terms suggest the use of the *geometric series*

$$\sum_{k\geq 0} z^k = \frac{1}{1 - z}$$

with $z = \frac{1+\sqrt{5}}{2}\, x$ and $z = \frac{1-\sqrt{5}}{2}\, x$, respectively:

$$\begin{aligned} F(x) = \frac{x}{1 - x - x^2} &= \frac{1}{\sqrt{5}} \sum_{k\geq 0} \left(\frac{1+\sqrt{5}}{2}\, x\right)^k - \frac{1}{\sqrt{5}} \sum_{k\geq 0} \left(\frac{1-\sqrt{5}}{2}\, x\right)^k \\ &= \sum_{k\geq 0} \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right) x^k\ . \end{aligned}$$

Comparing the coefficients of x^k in the definition of $F(x) = \sum_{k\geq 0} f_k\, x^k$ and the new expression above for $F(x)$, we discover the closed form expression for the Fibonacci sequence

$$f_k = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right).$$

4 Graphs and trees

A *(simple) graph* $G = (V, E)$ is composed of two objects: a finite set V (the *vertices* or *nodes* of G) and a set E of pairs of distinct vertices (the *edges* of G). The number of vertices $|V|$ is the *order* of G. If $e = \{a, b\} \in E$ then we say that e *joins* a and b, and that a and b are *adjacent*. We also say that a and e (as well as b and e) are *incident*. While a graph is by definition an abstract entity, we typically represent it with a diagram in the plane, which shows the vertices as points and simple curves between adjacent vertices. A graph is *planar* if it can be represented by such a diagram, in which none of the edge curves cross. The *degree* (or *valence*) of $v \in V$ is the number of edges incident with v. The degrees of all the vertices of G, listed in nonincreasing order, is the *degree sequence* of G.

Example. The *complete graph* K_n is a graph of order n for which each pair of distinct vertices forms an edge. The graphic representations of K_1, K_2, K_3 are a point, a line segment, and a triangle, respectively. K_n is planar precisely for $1 \leq n \leq 4$. The degree sequence of K_n is $(n-1, n-1, \ldots, n-1)$.

A famous theorem, which is as old as graph theory itself, asserts that the sum of the degrees of all the vertices of G is even. Consequently, the number of vertices of G with odd degree is even. Leonard Euler came up with this theorem in 1736 when he solved the *Königsberg bridge problem*.

An alternative description of a graph $G = (V, E)$ is through its *adjacency matrix*. One orders the vertices $v_1, v_2, \ldots, v_n \in V$ and forms an $n \times n$ matrix with entries

$$a_{jk} = \begin{cases} 1 & \text{if } \{v_j, v_k\} \in E, \\ 0 & \text{if } \{v_j, v_k\} \notin E. \end{cases}$$

Note that $a_{jk} = a_{kj}$ (i.e., the adjacency matrix is symmetric) and $a_{jj} = 0$.

A sequence of m edges of the form $\{v_0, v_1\}, \{v_1, v_2\}, \ldots, \{v_{m-1}, v_m\}$ is a *walk* of length m, and this walk *joins* the vertices v_0 and v_m. This walk is *closed* if $v_0 = v_m$. A walk that does not repeat edges is a *trail*. A trail that has distinct vertices (except possibly $v_0 = v_m$) is a *path*. A closed path is a *cycle*. A trail of G is *Eulerian* if it contains every edge in G. A cycle in a graph G of order n is *Hamiltonian* if it has length n. A path in G is *Hamiltonian* if has length $n-1$ and joins distinct vertices.

Example. The complete graph K_n, for $n \geq 3$, has a Hamiltonian cycle; in fact, it has $(n-1)!$ distinct Hamiltonian cycles, corresponding to circular permutations. K_n has $n!$ distinct Hamiltonian paths.

To continue our discussion of Euler's first theorem in graph theory, we mention a second result from the same paper: If a graph G has a closed Eulerian trail then the degree of each vertex in G is even. Further more, if G is connected, then this evenness condition suffices to ensure the existence of a closed Eulerian trail. Many theorems in graph theory are proved *algorithmically*, that is, one proves the existence of an algorithm that produces what the theorem asserts. As an example, you may try to prove that if the degree of each vertex in G is even, then each edge of G belongs to a closed trail (and hence to a cycle). As similar as closed Eulerian trails and Hamiltonian cycles

may look, there are no results analogous to the above for Hamiltonian cycles: we don't know of any such characterization for graphs with Hamiltonian cycles, nor is there a satisfactory algorithm for constructing a Hamiltonian cycle, should one exist (this algorithmic problem is a weak version of the infamous *traveling salesperson problem*).

The graph G is *connected* if for each pair of vertices a and b, there is a walk joining a and b; otherwise G is *disconnected*. In a connected graph, the *distance* between $a, b \in V$ is the shortest length of a walk (which will be a path) joining a and b.

A *tree* is a connected graph that becomes disconnected upon the removal of any edge. The following are equivalent characterizations for a connected graph G to be a tree:

- G has exactly $|V| - 1$ edges.
- G has no cycles.
- Every pair of distinct vertices is joined by a unique path.

Let $G = (V, E)$, $U \subseteq V$, and $F \subseteq E$, such that the vertices of each edge in F belong to U. Then $G' = (U, F)$ is also graph, a *subgraph* of G. If F consists of all edges of G that join vertices in U, then G' is an *induced* subgraph of G. If $U = V$ then G' is called *spanning*. Another nice example for a theorem that can be proved algorithmically is the result that every connected graph has a spanning tree.

For a lot of applications, simple graphs are not sufficient. If we allow *multiple edges* (an edge can appear more than once in E, i.e., E is a multiset) and *loops* (an edge of the form $\{a, a\}$ for some vertex a), we call G a *multigraph* or a *general graph*. For a lot of further applications, one wants the edges in a graph to be oriented one way or other (i.e., an edge is not specified by a two-element subset of V but by an ordered pair of vertices), which leads to *directed graphs* or *digraphs*.

5 Lattices

The relation $R \subseteq A \times A$ is a *partial order* if it has the following three properties:

(i) $a \sim a$ for all $a \in A$ (reflexivity)

(ii) $a \sim b$ and $a \neq b$ imply $b \not\sim a$ (antisymmetry)

(iii) $a \sim b$ and $b \sim c$ imply $a \sim c$ (transitivity)

A *partially ordered set* (often simply called *poset*) is a set A on which a partial order is defined.

Example. Let $A = \{1, 2, 3\}$.

- We define the relation $\sim$ on A through $a \sim b$ if $a \leq b$. This poset is completely described by $1 \leq 2 \leq 3$.

- We define the relation $\sim$ on A through $a \sim b$ if $a|b$ (a divides b). This poset is completely described by $1|2$ and $1|3$ (there are no other relations).

Our first relation gives a *total order* on A: any two elements of A are comparable. This is not true for the second relation, for which 2 and 3 are incomparable.

Let A be a poset with the partial order $\preceq$, and let $a, b \in A$. The *least upper bound* or *join* of a and b is the minimal $c \in A$ (in terms of the partial order $\leq$) such that $a \preceq c$ and $b \preceq c$; it is denoted by $a \vee b$. The *greatest lower bound* or *meet* of a and b is the maximal $c \in A$ such that $c \preceq a$ and $c \preceq b$; it is denoted by $a \wedge b$. Least upper bounds and greatest lower bounds do not generally exist in every poset. If they do (for all $a, b \in A$) then the poset is a *lattice*. A lattice necessarily has a maximal and a minimal element.

Example. Here's a short sample of lattices:

- Any set with a total order is a lattice.
- The subsets of a fixed set form a lattice with the partial order $\subseteq$. If the fixed set is finite, this lattice is a *Boolean lattice*.
- Given a finite set of hyperplanes in $\mathbb{R}^d$, consider all possible intersections of hyperplanes (including $\mathbb{R}^d$ itself, which is the empty intersection). These intersections form a lattice with the partial order $\supseteq$, the *intersection lattice* of the hyperplane arrangement.