CompSci 102
Discrete Math for Computer Science

$$\begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 1 & 3 \end{bmatrix}$$

February 7, 2012

Prof. Rodger

Slides modified from Rosen

Chap 2.5-2.6
Cardinality

Definition: The *cardinality* of a set A is equal to the cardinality of a set B, denoted

$$|A| = |B|,$$

if and only if there is a one-to-one correspondence (*i.e.*, a bijection) from A to B.

- If there is a one-to-one function (*i.e.*, an injection) from A to B, the cardinality of A is less than or the same as the cardinality of B and we write $|A| \leq |B|$.
- When $|A| \leq |B|$ and A and B have different cardinality, we say that the cardinality of A is less than the cardinality of B and write $|A| < |B|$.

Cardinality

- **Definition**: A set that is either finite or has the same cardinality as the set of positive integers ($\mathbf{Z}^+$) is called *countable*. A set that is not countable is *uncountable*.
- The set of real numbers $\mathbf{R}$ is an uncountable set.
- When an infinite set is countable (*countably infinite*) its cardinality is $\aleph_0$ (where $\aleph$ is aleph, the 1st letter of the Hebrew alphabet). We write $|S| = \aleph_0$ and say that S has cardinality "aleph null."

Showing that a Set is Countable

- An infinite set is countable if and only if it is possible to list the elements of the set in a sequence (indexed by the positive integers).
- The reason for this is that a one-to-one correspondence f from the set of positive integers to a set S can be expressed in terms of a sequence $a_1, a_2, \ldots, a_n, \ldots$ where $a_1 = f(1)$, $a_2 = f(2), \ldots, a_n = f(n), \ldots$

Hilbert's Grand Hotel

David Hilbert

The Grand Hotel (example due to David Hilbert) has countably infinite number of rooms, each occupied by a guest. We can always accommodate a new guest at this hotel. How is this possible?

Explanation: Because the rooms of Grand Hotel are countable, we can list them as Room 1, Room 2, Room 3, and so on. When a new guest arrives, we move the guest in Room 1 to Room 2, the guest in Room 2 to Room 3, and in general the guest in Room n to Room $n + 1$, for all positive integers n. This frees up Room 1, which we assign to the new guest, and all the current guests still have rooms.

Hilbert's Grand Hotel

Take room 1, everyone else move down one room

Manager   New guest
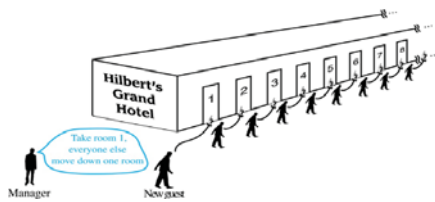
The hotel can also accommodate a countable number of new guests, all the guests on a countable number of buses where each bus contains a countable number of guests (see exercises).

Showing that a Set is Countable

Example 1: Show that the set of positive even integers E is a countable set.

Solution: Let $f(x) = 2x$.

$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \ .....$$

$$\updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow$$

$$2 \quad 4 \quad 6 \quad 8 \quad 10 \quad 12 \ ......$$

Then f is a bijection from $\mathbf{N}$ to E since f is both one-to-one and onto. To show that it is one-to-one, suppose that $f(n) = f(m)$. Then $2n = 2m$, and so $n = m$. To see that it is onto, suppose that t is an even positive integer. Then $t = 2k$ for some positive integer k and $f(k) = t$. ◀

Showing that a Set is Countable

Example 2: Show that the set of integers $\mathbf{Z}$ is countable. ◀

Showing that a Set is Countable

Example 2: Show that the set of integers $\mathbf{Z}$ is countable.

Solution: Can list in a sequence:

$$0, 1, -1, 2, -2, 3, -3, ...$$

Or can define a bijection from $\mathbf{N}$ to $\mathbf{Z}$:

– When n is even: $f(n) = n/2$

– When n is odd: $f(n) = -(n-1)/2$ ◀

The Positive Rational Numbers are Countable

- **Definition**: A *rational number* can be expressed as the ratio of two integers p and q such that $q \neq 0$.
  - ¾ is a rational number
  - $\sqrt{2}$ is not a rational number.

  Example 3: Show that the positive rational numbers are countable.

  Solution: The positive rational numbers are countable since they can be arranged in a sequence:
  $$r_1, r_2, r_3, \ldots$$
  The next slide shows how this is done. →

◄

The Positive Rational Numbers are Countable

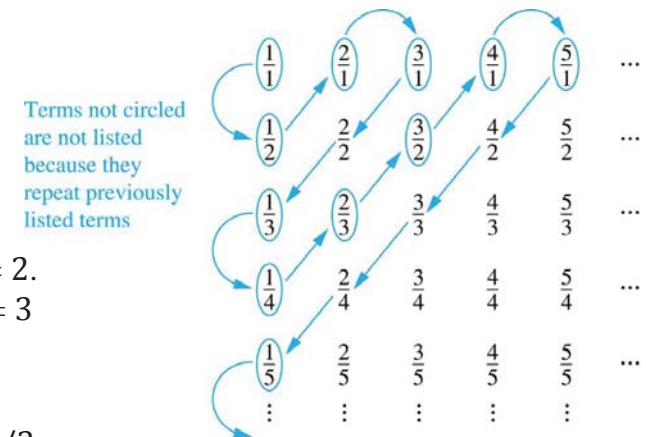First row $q = 1$.
Second row $q = 2$.
etc.

Constructing the List

First list p/q with $p + q = 2$.
Next list p/q with $p + q = 3$

And so on.

1, ½, 2, 3, 1/3, 1/4, 2/3, ...

Terms not circled are not listed because they repeat previously listed terms

◄

Strings

Example 4: Show that the set of finite strings S over a finite alphabet A is countably infinite.

Assume an alphabetical ordering of symbols in A

◄

Strings

Example 4: Show that the set of finite strings S over a finite alphabet A is countably infinite.

Assume an alphabetical ordering of symbols in A

Solution: Show that the strings can be listed in a sequence. First list

1. All the strings of length 0 in alphabetical order.
2. Then all the strings of length 1 in lexicographic (as in a dictionary) order.
3. Then all the strings of length 2 in lexicographic order.
4. And so on.

This implies a bijection from **N** to S and hence it is a countably infinite set.

◄

The set of all Java programs is countable.

Example 5: Show that the set of all Java programs is countable.

◀

Solution: Let S be the set of strings constructed from the characters which can appear in a Java program. Use the ordering from the previous example. Take each string in turn:

- Feed the string into a Java compiler. (A Java compiler will determine if the input program is a syntactically correct Java program.)
- If the compiler says YES, this is a syntactically correct Java program, we add the program to the list.
- We move on to the next string.

◀

In this way we construct an implied bijection from **N** to the set of Java programs. Hence, the set of Java programs is countable.

The Real Numbers are Uncountable

Georg Cantor
(1845-1918)

Example: Show that the set of real numbers is uncountable.

Solution: The method is called the Cantor diagonalization argument, and is a proof by contradiction.

1. Suppose **R** is countable. Then the real numbers between 0 and 1 are also countable (any subset of a countable set is countable)
2. The real numbers between 0 and 1 can be listed in order r_1, r_2, r_3,… .
3. Let the decimal representation of this listing be

$$r_1 = 0.d_{11}d_{12}d_{13}d_{14}d_{15}d_{16}\cdots$$
$$r_2 = 0.d_{21}d_{22}d_{23}d_{24}d_{25}d_{26}\cdots$$
$$r_3 = 0.d_{31}d_{32}d_{33}d_{34}d_{35}d_{36}\cdots$$
$$\vdots$$

4. Form a new real number with the decimal expansion

where $r_i = 3$ if $d_{ii} \neq 3$ and $r_i = 4$ if $d_{ii} = 3$

$$r = .r_1r_2r_3r_4\cdots$$

5. r is not equal to any of the r_1, r_2, r_3,… Because it differs from r_i in its ith position after the decimal point. Therefore there is a real number between 0 and 1 that is not on the list since every real number has a unique decimal expansion. Hence, all the real numbers between 0 and 1 cannot be listed, so the set of real numbers between 0 and 1 is uncountable.
6. Since a set with an uncountable subset is uncountable (an exercise), the ◀ set of real numbers is uncountable.

Matrices

- Matrices are useful discrete structures that can be used in many ways. For example, they are used to:
  - describe certain types of functions known as linear transformations.
  - Express which vertices of a graph are connected by edges (see Chapter 10).
- In later chapters, we will see matrices used to build models of:
  - Transportation systems.
  - Communication networks.
- Algorithms based on matrix models will be presented in later chapters.
- Here we cover the aspect of matrix arithmetic that will be needed later.

Matrix

Definition: A *matrix* is a rectangular array of numbers. A matrix with m rows and n columns is called an $m \times n$ matrix.

- The plural of matrix is *matrices*.
- A matrix with the same number of rows as columns is called *square*.
- Two matrices are *equal* if they have the same number of rows and the same number of columns and the corresponding entries in every position are equal.

3×2 matrix
$$\begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 1 & 3 \end{bmatrix}$$

Notation

- Let m and n be positive integers and let

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

- The ith row of A is the $1 \times n$ matrix $[a_{i1}, a_{i2}, \ldots, a_{in}]$. The jth column of A is the $m \times 1$ *matrix*:

- The (i,j)th *element* or *entry* of A is the element a_{ij}. We can use $A = [a_{ij}]$ to denote the matrix with its (i,j)th element equal to a_{ij}.

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ \cdot \\ \cdot \\ a_{mj} \end{bmatrix}$$

Matrix Arithmetic: Addition

Defintion: Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be m n matrices. The sum of A and B, denoted by $A + B$, is the m n matrix that has $a_{ij} + b_{ij}$ as its (i,j)th element. In other words, $A + B = [a_{ij} + b_{ij}]$.

Example:

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 2 & -3 \\ 3 & 4 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 4 & -1 \\ 1 & -3 & 0 \\ -1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 & -2 \\ 3 & -1 & -3 \\ 2 & 5 & 2 \end{bmatrix}$$

Note that matrices of different sizes can NOT be added.

Matrix Multiplication

Definition: Let A be an $n \times k$ matrix and B be a $k \times n$ matrix. The *product* of A and B, denoted by AB, is the $m \times n$ matrix that has its (i,j)th element equal to the sum of the products of the corresponding elements from the ith row of A and the jth column of B. In other words, if $AB = [c_{ij}]$ then $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{kj}b_{2j}$.

Example:

$$\begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 1 & 1 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 14 & 4 \\ 8 & 9 \\ 7 & 13 \\ 8 & 2 \end{bmatrix}$$

The product of two matrices is undefined when the number of columns in the first matrix is not the same as the number of rows in the second.

Illustration of Matrix Multiplication

- The Product of $\mathbf{A} = [a_{ij}]$ and $\mathbf{B} = [b_{ij}]$

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{i1} & a_{i2} & \cdots & a_{ik} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{m1} & a_{m2} & \cdots & a_{mk} \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} b_{11} & a_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ b_{k1} & b_{k2} & \cdots & b_{kj} & \cdots & b_{kn} \end{bmatrix}$$

$$\mathbf{AB} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & c_{ij} & \cdot \\ \cdot & \cdot & & \cdot \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix}$$

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj}$$

Is Matrix Multiplication Commutative

Example: Let
$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \qquad \mathbf{B} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

Does $\mathbf{AB} = \mathbf{BA}$?

Is Matrix Multiplication Commutative

Example: Let
$$\mathbf{A} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \qquad \mathbf{B} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

Does $\mathbf{AB} = \mathbf{BA}$?

Solution:
$$\mathbf{AB} = \begin{bmatrix} 2 & 2 \\ 5 & 3 \end{bmatrix} \qquad \mathbf{BA} = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}$$

$$\mathbf{AB} \neq \mathbf{BA}$$

Identity Matrix and Powers of Matrices

Definition: The *identity matrix of order n* is the $m \times n$ matrix $\mathbf{I}_n = [\delta_{ij}]$, where $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$.

$$\mathbf{I_n} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

$$\mathbf{AI}_n = \mathbf{I}_m\mathbf{A} = \mathbf{A}$$
when $\mathbf{A}$ is an $m \times n$ matrix

Powers of square matrices can be defined. When A is an $n \times n$ matrix, we have:

$$\mathbf{A}^0 = \mathbf{I}_n \qquad \mathbf{A}^r = \underbrace{\mathbf{AAA}\cdots\mathbf{A}}_{r \text{ times}}$$

Transposes of Matrices

Definition: Let $\mathbf{A} = [a_{ij}]$ be an $m \times n$ matrix. The *transpose* of $\mathbf{A}$, denoted by $\mathbf{A}^t$, is the $n \times m$ matrix obtained by interchanging the rows and columns of $\mathbf{A}$.

If $\mathbf{A}^t = [b_{ij}]$, then $b_{ij} = a_{ji}$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$.

The transpose of the matrix $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ is the matrix $\begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$.