CompSci 230
Discrete Math for Computer Science

\[
\begin{bmatrix}
1 & 1 & 1 \\
-1 & 0 & 1 \\
1 & 1 & -1
\end{bmatrix} \begin{bmatrix}
J \\
M \\
S
\end{bmatrix} = \begin{bmatrix}
100 \\
40 \\
0
\end{bmatrix}
\]

Sep 26, 2013
Prof. Rodger

Slides modified from Rosen

Announcements

• Exam 1 is Tuesday, Oct. 1
• No class, Oct 3, No recitation Oct 4-7
• Prof. Rodger is out Sep 30-Oct 4
• There is Recitation: Sept 27-30.

Test 1

• Closed book, closed notes, closed neighbor
• There will be a handout of formulas supplied
• Topics:
  – Reading covers - Chap. 1, 2, and 13.3
  – Logic, Sets, Functions, Sequences, Cardinality, Matrices, DFA

Ways to Study

• Rework problems in lecture
• Rework problems from recitation
• Rework problems from old test
• Try examples using JFLAP
  – Write a DFA over \{a,b\} that has the number of b’s divisible by 3.
  – Write a DFA over \{a,b\} that accepts strings with “aa” and the number of b’s are divisible by 3
• Ask questions on piazza
  – Answer questions on piazza
Chap 2.5 Cardinality

How many elements? Can you list them in an ordered way so you don’t miss any of them?

- \( \{x \in \mathbb{Z} | x \mod 5 = 0, \text{ and } 0 < x \leq 100\} \)

- \( \{x \in \mathbb{Z} | x \mod 5 = 0\} \)

- All the subsets of \( \{x \in \mathbb{Z} | x \mod 5 = 0\} \)

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 (\( \mathbb{Z}^+ \)) is called *countable*. A set that is not countable is *uncountable*.

- \( \{x \in \mathbb{Z} | x \mod 5 = 0, \text{ and } 0 < x \leq 100\} \)
  - 20 elements: 5, 10, 15, … 100

- \( \{x \in \mathbb{Z} | x \mod 5 = 0\} \)
  - Infinite, you can list them out in an ordered way: 5, 10, 15, … “countable set”

- All the subsets of \( \{x \in \mathbb{Z} | x \mod 5 = 0\} \)
  - Infinite, you CANNOT list them all out in an ordered way “uncountable set”
Cardinality

- **Definition:** A set that is either finite or has the same cardinality as the set of positive integers ($\mathbb{Z}^+$) is called **countable.** A set that is not countable is **uncountable.**

- $\{x \in \mathbb{Z}|x \text{ mod } 5 = 0\}$ **countable**

- All subsets of $\{x \in \mathbb{Z}|x \text{ mod } 5 = 0\}$ **uncountable**

- A set that is not countable is **uncountable.**

- 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**

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.

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.
Showing that a Set is Countable

Example 1: Show that the set of positive even integers $E$ is a countable set.
Solution: Let $f(x) = 2x$.

\[
\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
\uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
2 & 4 & 6 & 8 & 10 & 12 \\
\end{array}
\]

Then $f$ is a bijection from $\mathbb{N}$ 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 $f(k) = t$.

Example 2: Show that the set of integers $\mathbb{Z}$ is countable.
Solution: Can list in a sequence:

\[0, 1, -1, 2, -2, 3, -3, \ldots\]

Or can define a bijection from $\mathbb{N}$ to $\mathbb{Z}$:
\- When $n$ is even: $f(n) = n/2$
\- When $n$ is odd: $f(n) = -(n-1)/2$

\[f(1) \text{ to } 0, f(2) \text{ to } 1, f(3) \text{ to } -1, f(4) \text{ to } 2, f(5) \text{ to } -2, \ldots\]

The Positive Rational Numbers are Countable

- Definition: A rational number can be expressed as the ratio of two integers $p$ and $q$ such that $q \neq 0$.
  \- $\frac{1}{4}$ 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:

\[r_1, r_2, r_3, \ldots\]
Does this work?

• For p/q
  – List all those numbers with q=1
    • 1/1, 2/1, 3/1, 4/1, 5/1, …
  – Then list all those numbers with q=2
    • 1/2, 2/2, 2/3, 2/4, 2/5, …
  – Then list all those numbers with q=3, etc

Does this work?

• For p/q
  – List all those numbers with q=1
    • 1/1, 2/1, 3/1, 4/1, 5/1, …
  – Then list all those numbers with q=2
    • 1/2, 2/2, 2/3, 2/4, 2/5, …
  – Then list all those numbers with q=3, etc

– Doesn’t work, infinite in too many directions!

Solution for listing out all p/q

• List all s.t.
  p+q=2
  1  2  3  4  5  ...

• Then all s.t.
  p+q=3
  1  2  3  4  5  ...

• Then all s.t.
  p+q=4
  1  2  3  4  5  ...

• Etc

• Why does this work?

Example - Strings

• Show that the set S of strings over the alphabet {0,1} is countable.

• What is S? Is S infinite?

• Solution:
Example - Strings

• Show that the set $S$ of strings over the alphabet \{0,1\} is countable.
• What is $S$? Is $S$ infinite?
  \[ S = \{010, 1101, ..., 11001010, ... \} \]
• **Solution:**
  • List out all the strings of length 0, then 1, then 2, etc. There are a finite number of each
  • $S = \{ \lambda, 0, 1, 00, 01, 10, 11, 000, ... \}$
  • $f(\lambda) = 1, f(0) = 2, f(1) = 3, f(00) = 4, ...$

Example: Is the set of all Java programs countable?

• $\Sigma = \text{the set of all symbols in Java programs}$
• $S = \text{the set of all strings over the alphabet}$

Example: Is the set of all Java programs countable?

• Yes
• **Solution:**
  • $\Sigma = \text{the set of all symbols in Java programs}$
    - $\Sigma = \{a, b, ..., z, 0, 1, 2, ..., 9, (, ), {, }, =, +, ...\}$
  - $\Sigma$ is finite
  • $S$ is the set of all strings over the alphabet
  • $J = \{ p \in S \mid p \text{ is a valid Java program} \}$
  • List out all the strings in $S$ and if they compile (then a valid Java program), put them in $J$

The Real numbers are uncountable

• Proof(sketch) by diagonalization
• Suppose we can list out all the real numbers without missing any of them.
• List out all real numbers
• Claim we missed one!
• There is a number whose $i$th digit is different from the $i$th digit in the $i$th number.

  1 $\leftrightarrow$ 0.397204817...
  2 $\leftrightarrow$ 0.526613809...
  3 $\leftrightarrow$ 0.498310123...
  4 $\leftrightarrow$ 0.275418331...
  5 $\leftrightarrow$ 0.002200025...
  6 $\leftrightarrow$ 0.999904681...
  ...

• List out all real numbers
• Claim we missed one!
• There is a number whose $i$th digit is different from the $i$th digit in the $i$th number.
• Contradiction!
• Thus real numbers are not countable

  1 $\leftrightarrow$ 0.597204817...
  2 $\leftrightarrow$ 0.526613809...
  3 $\leftrightarrow$ 0.498310123...
  4 $\leftrightarrow$ 0.275418331...
  5 $\leftrightarrow$ 0.002200025...
  6 $\leftrightarrow$ 0.999904681...
  ...

Matrices

• Examples:
  – Graph Theory - Express which vertices of a graph are connected by edges
  – Graphics
    • Represent a 3D object with a matrix
    • Project a 3D object onto a 2D screen
    • Optimal curve fitting
  – Transportation systems.
  – Communication networks
  – Economics and Game Theory
• For now, definition and basic operations

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.

  $3\times2$ matrix

\[
\begin{bmatrix}
  1 & 1 \\
  0 & 2 \\
  1 & 3
\end{bmatrix}
\]
Notation

• Let \( m \) and \( n \) be positive integers and let

\[
A = \begin{bmatrix}
  a_{11} & a_{12} & \cdots & a_{1n} \\
  a_{21} & a_{22} & \cdots & a_{2n} \\
  \vdots & \vdots & \ddots & \vdots \\
  a_{m1} & a_{m2} & \cdots & a_{mn}
\end{bmatrix}
\]

• The \( i \)th row of \( A \) is the \( 1 \times n \) matrix \([a_{i1}, a_{i2}, \ldots, a_{in}]\).

• The \( j \)th column of \( A \) is the \( m \times 1 \) matrix:

\[
\begin{bmatrix}
  a_{1j} \\
  a_{2j} \\
  \vdots \\
  a_{mj}
\end{bmatrix}
\]

• 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 \( a_{ij} \).

Matrix Arithmetic: Addition

Definition: Let \( A = [a_{ij}] \) and \( B = [b_{ij}] \) be \( m \times n \) matrices. The sum of \( A \) and \( B \), denoted by \( A + B \), is the \( m \times n \) 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 \( m \times k \) 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 \( i \)th row of \( A \) and the \( j \)th column of \( B \). In other words, if \( AB = [c_{ij}] \) then \( c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{ik}b_{kj} \).

Example:

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

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

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 \( i \)th row of \( A \) and the \( j \)th column of \( B \). In other words, if \( AB = [c_{ij}] \) then \( c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{ik}b_{kj} \).

Example:

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

undefined when number of columns in the first matrix is not the same as number of rows in the second.
Illustration of Matrix Multiplication

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

\[
A = \begin{bmatrix}
a_{11} & a_{12} & \cdots & a_{1k} \\
a_{21} & a_{22} & \cdots & a_{2k} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} & a_{m2} & \cdots & a_{mk}
\end{bmatrix}
\]

\[
B = \begin{bmatrix}
b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\
b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
b_{k1} & b_{k2} & \cdots & b_{kj} & \cdots & b_{kn}
\end{bmatrix}
\]

\[
AB = \begin{bmatrix}
c_{11} & c_{12} & \cdots & c_{1n} \\
c_{21} & c_{22} & \cdots & c_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
c_{m1} & c_{m2} & \cdots & c_{mn}
\end{bmatrix}
\]

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

Example use of Matrix Multiplication

- Solving set of linear equations

\[
\begin{align*}
J + M + S &= 100 \\
-J + S &= 40 \\
J + M - S &= 0
\end{align*}
\]

\[
\begin{bmatrix}
1 & 1 & 1 \\
-1 & 0 & 1 \\
1 & 1 & -1
\end{bmatrix}\begin{bmatrix}
J \\
M \\
S
\end{bmatrix} = \begin{bmatrix}
100 \\
40 \\
0
\end{bmatrix}
\]

Is Matrix Multiplication Commutative

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

Does $AB = BA$?

\[
AB = \begin{bmatrix} 3 & 2 \\ 5 & 3 \end{bmatrix} \quad BA = \begin{bmatrix} 4 & 3 \\ 3 & 2 \end{bmatrix}
\]

$AB \neq BA$
Identity Matrix and Powers of Matrices

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

$$I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

$$AI_n = I_mA = A$$

when $A$ is an $m \times n$ matrix.

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

$$A^0 = I_n \quad A^r = AAA\cdots A$$

$r$ times

Transposes of Matrices

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

If $A^t = [b_{ij}]$, 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 $\begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$. 