Department of
Computer Science and Engineering
计算机科学与工程系

CS215 DISCRETE MATH

Dr. Qi Wang

Department of Computer Science and Engineering
Office: Room413, CoE South Tower
Email: wangqi@sustech.edu.cn

k-Element Permutations of a Set

- In how many ways can we choose **an ordered triple** of distinct elements from $\{1, 2, \ldots, n\}$?

k-Element Permutations of a Set

- In how many ways can we choose **an ordered triple** of distinct elements from $\{1, 2, \ldots, n\}$?

  More generally, in how many ways can we choose a list of k distinct elements from $\{1, 2, \ldots, n\}$?

k-Element Permutations of a Set

- In how many ways can we choose **an ordered triple** of distinct elements from $\{1, 2, \ldots, n\}$?

  More generally, in how many ways can we choose a list of k distinct elements from $\{1, 2, \ldots, n\}$?

  A list of k *distinct* elements chosen from a set N is called a **k-element permutation of N**

k-Element Permutations of a Set

- In how many ways can we choose **an ordered triple** of distinct elements from $\{1, 2, \ldots, n\}$?

  More generally, in how many ways can we choose a list of k distinct elements from $\{1, 2, \ldots, n\}$?

  A list of k *distinct* elements chosen from a set N is called a **k-element permutation of N**

  Note that the case of $k = n$ is special;
  An n-element permutation of a set N of size $|N| = n$ is what we earlier simply called a permutation.

k-Element Permutations of a Set

- How many three-element permutations of $\{1, 2, \ldots, n\}$ are there?

k-Element Permutations of a Set

- How many three-element permutations of $\{1, 2, \ldots, n\}$ are there?

  n choices for first number

k-Element Permutations of a Set

- How many three-element permutations of $\{1, 2, \ldots, n\}$ are there?

  n choices for first number

  For each way of choosing first number there are $n - 1$ choices for the second

k-Element Permutations of a Set

- How many three-element permutations of $\{1, 2, \ldots, n\}$ are there?

  n choices for first number

  For each way of choosing first number there are $n-1$ choices for the second

  For each way of choosing first two numbers,there are $n-2$ choices for the third number

k-Element Permutations of a Set

- How many three-element permutations of $\{1, 2, \ldots, n\}$ are there?

  n choices for first number

  For each way of choosing first number there are $n - 1$ choices for the second

  For each way of choosing first two numbers,there are $n - 2$ choices for the third number

  By product rule, there are $n(n-1)(n-2)$ ways to choose the permutation

An Example

- By product rule, there are $n(n-1)(n-2)$ ways to choose the permutation

An Example

- By product rule, there are $n(n-1)(n-2)$ ways to choose the permutation

Ex: When $n = 4$, there are $4 \times 3 \times 2 = 24$ 3 -element permutations of $\{1, 2, 3, 4\}$

$$L = \{123, 124, 132, 134, 142, 143, 213, 214, 231, 234, 241, 243$$
$$312, 314, 321, 324, 341, 342, 412, 413, 421, 423, 431, 432\}.$$

An Example

- By product rule, there are $n(n-1)(n-2)$ ways to choose the permutation

Ex: When $n = 4$, there are $4 \times 3 \times 2 = 24$ 3 -element permutations of $\{1, 2, 3, 4\}$

$$L = \{123, 124, 132, 134, 142, 143, 213, 214, 231, 234, 241, 243$$
$$312, 314, 321, 324, 341, 342, 412, 413, 421, 423, 431, 432\}.$$

Note: This type of "dictionary" ordering of tuples (assuming that we treat numbers the same as letters) is called a *lexicographic ordering* and is used quite often.

k-Element Permutations of a Set

- **Theorem** If N is a positive integer and k is an integer with $1 \le k \le n$, then there are
  $P(n,k) = n(n-1)(n-2)\cdots(n-k+1)$
  k-element permutations with n distinct elements.

k-Element Permutations of a Set

- **Theorem** If N is a positive integer and k is an integer with $1 \leq k \leq n$, then there are
  $P(n, k) = n(n-1)(n-2)\cdots(n-k+1)$
  k-element permutations with n distinct elements.

  How does this help us solve our original problem(from triangle program) of counting $\#$ of 3-element subsets?

k-Element Permutations of a Set

- **Theorem** If N is a positive integer and k is an integer with $1 \leq k \leq n$, then there are
  $P(n,k) = n(n-1)(n-2)\cdots(n-k+1)$
  k-element permutations with n distinct elements.

  How does this help us solve our original problem(from triangle program) of counting $\#$ of 3-element subsets?

  Note that every 3-element subset $\{i, j, k\}$ can be made into exactly 6 3-element perms

k-Element Permutations of a Set

- **Theorem** If N is a positive integer and k is an integer with $1 \leq k \leq n$, then there are
  $P(n,k) = n(n-1)(n-2)\cdots(n-k+1)$
  k-element permutations with n distinct elements.

  How does this help us solve our original problem(from triangle program) of counting $\#$ of 3-element subsets?

  Note that every 3-element subset $\{i, j, k\}$ can be made into exactly 6 3-element perms

  $(\#$ 3-element perms$) = 6 \times (\#$ 3-element subsets$)$

k-Element Permutations of a Set

- **Theorem** If N is a positive integer and k is an integer with $1 \leq k \leq n$, then there are $P(n, k) = n(n-1)(n-2)\cdots(n-k+1)$ k-element permutations with n distinct elements.

How does this help us solve our original problem(from triangle program) of counting $\#$ of 3-element subsets?

Note that every 3-element subset $\{i, j, k\}$ can be made into exactly 6 3-element perms

$$(\#\ \text{3-element perms}) = 6 \times (\#\ \text{3-element subsets})$$

$$P(n, 3) = 3! \cdot C(n, 3)$$

Binomial Coefficient

- **Theorem** For integers n and k with $0 \leq k \leq n$, the number of k-element subsets of an n-element set is

$$\binom{n}{k} = C(n,k) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k)!}.$$

This is the number of k-combinations of a set with n elements.

Some Properties of Binomial Coefficients

- $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is the number of k-element subsets of an n-element set.

$\binom{n}{0} = 1$ only one set of size 0.

$\binom{n}{n} = 1$ only one set of size n.

$\binom{n}{k} = \binom{n}{n-k}$ Obvious from equation. Can you think of a simple bijection that explains this?

Some Properties of Binomial Coefficients (cont.)

- $$\boxed{\sum_{i=0}^{n} \binom{n}{i} = 2^n}$$

Some Properties of Binomial Coefficients (cont.)

- $$\boxed{\sum_{i=0}^{n} \binom{n}{i} = 2^n}$$

Use Sum Rule

Let P = set of all subsets of $\{1,2,\ldots,n\}$

S_i = set of all i-subsets of $\{1,2,\ldots,n\}$

Some Properties of Binomial Coefficients (cont.)

- $$\boxed{\sum_{i=0}^{n} \binom{n}{i} = 2^n}$$

  Use Sum Rule

  Let P = set of all subsets of $\{1,2,\ldots,n\}$

  S_i = set of all i-subsets of $\{1,2,\ldots,n\}$

  $$\Rightarrow |P| = \sum_{i=0}^{n} |S_i| = \sum_{i=0}^{n} \binom{n}{i}$$

Some Properties of Binomial Coefficients (cont.)

- Let $L = L_1 L_2 \ldots L_n$ be a list of size n from $\{0, 1\}$

  If $\mathcal{L} = \text{set of all such lists} \Rightarrow \ |\mathcal{L}| = 2^n$

  There is a *bijection* between $\mathcal{L}$ and P so
  $|P| = 2^n$ and we are done.

Some Properties of Binomial Coefficients (cont.)

- Let $L = L_1 L_2 \ldots L_n$ be a list of size n from $\{0, 1\}$

  If $\mathcal{L} =$ set of all such lists $\Rightarrow$ $|\mathcal{L}| = 2^n$

  There is a *bijection* between $\mathcal{L}$ and P so
  $|P| = 2^n$ and we are done.

  Define the following function $f : \mathcal{L} \to P$

  If $L \in \mathcal{L}$ then $f(L)$ is the set $S \subseteq \{1, 2, \ldots, n\}$ defined by

$$i \in S \;\Leftrightarrow\; L_i = 1$$

Some Properties of Binomial Coefficients (cont.)

- Let $L = L_1 L_2 \ldots L_n$ be a list of size n from $\{0, 1\}$

  If $\mathcal{L}$ = set of all such lists $\Rightarrow \ |\mathcal{L}| = 2^n$

  There is a *bijection* between $\mathcal{L}$ and P so
  $|P| = 2^n$ and we are done.

  Define the following function $f : \mathcal{L} \to P$

  If $L \in \mathcal{L}$ then $f(L)$ is the set $S \subseteq \{1, 2, \ldots, n\}$ defined by

  $$i \in S \ \Leftrightarrow \ L_i = 1$$

  f is a *bijection* between $\mathcal{L}$ and P (why?) so $|\mathcal{L}| = |P|$

Some Properties of Binomial Coefficients (cont.)

- Let $L = L_1 L_2 \ldots L_n$ be a list of size n from $\{0, 1\}$

  If $\mathcal{L}$ = set of all such lists $\Rightarrow$ $|\mathcal{L}| = 2^n$

  There is a *bijection* between $\mathcal{L}$ and P so
  $|P| = 2^n$ and we are done.

  Define the following function $f : \mathcal{L} \to P$

  If $L \in \mathcal{L}$ then $f(L)$ is the set $S \subseteq \{1, 2, \ldots, n\}$ defined by
  $$i \in S \;\Leftrightarrow\; L_i = 1$$

  f is a *bijection* between $\mathcal{L}$ and P (why?) so $|\mathcal{L}| = |P|$

Ex: $n = 5$

$$f(10101) = \{1, 3, 5\},\; f(11101) = \{1, 2, 3, 5\},\; f(00000) = \emptyset$$

Binomial Coefficients

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Binomial Coefficients

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Each row begins with a 1 because $\binom{n}{0} = 1$

Binomial Coefficients

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Each row begins with a 1 because $\binom{n}{0} = 1$

Each row ends with a 1 because $\binom{n}{n} = 1$.

Binomial Coefficients

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Each row begins with a 1 because $\binom{n}{0} = 1$

Each row ends with a 1 because $\binom{n}{n} = 1$.

Each row increases at first then decreases.

Binomial Coefficients

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Each row begins with a 1 because $\binom{n}{0} = 1$

Each row ends with a 1 because $\binom{n}{n} = 1$.

Each row increases at first then decreases.

Second half of each row is the reverse of the first half.

Binomial Coefficients

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Each row begins with a 1 because $\binom{n}{0} = 1$

Each row ends with a 1 because $\binom{n}{n} = 1$.

Each row increases at first then decreases.

Second half of each row is the reverse of the first half.

Sum of items on n-th row is 2^n

Pascal's Triangle

Take the table

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Pascal's Triangle

Take the table

n \ k	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

and shift each row slightly so that middle element is in middle

```
            1
          1   1
        1   2   1
      1   3   3   1
    1   4   6   4   1
  1   5  10  10   5   1
1   6  15  20  15   6   1
```

Pascal's Triangle

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

Pascal's Triangle

						1						
					1		1					
				1		2		1				
			1		3		3		1			
		1		4		6		4		1		
	1		5		10		10		5		1	
1		6		15		20		15		6		1

What is the next row in the table?

Pascal's Triangle

							1							
						1		1						
					1		2		1					
				1		3		3		1				
			1		4		6		4		1			
		1		5		10		10		5		1		
	1		6		15		20		15		6		1	
1		7		21		35		35		21		7		1

							1							
						1		1						
					1		2		1					
				1		3		3		1				
			1		4		6		4		1			
		1		5		10		10		5		1		
	1		6		15		20		15		6		1	
1		7		21		35		35		21		7		1

Pascal identity

Each (non-1) entry in Pascal's Triangle is the sum of the two entries directly above it (to left and to right).

Pascal's Triangle

							1							
						1		1						
					1		2		1					
				1		3		3		1				
			1		4		6		4		1			
		1		5		10		10		5		1		
	1		6		15		20		15		6		1	
1		7		21		35		35		21		7		1

$$\boxed{\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}}$$

Pascal identity

Each (non-1) entry in Pascal's Triangle is the sum of the two entries directly above it (to left and to right).

Pascal's Identity

- $$\boxed{\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}}$$

Pascal's Identity

- $$\boxed{\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}}$$

  A purely *algebraic* proof (manipulating formulas) is possible.

Pascal's Identity

- $$\boxed{\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}}$$

  A purely *algebraic* proof (manipulating formulas) is possible.

  We will use a combinatorial proof.

A Combinatorial Proof

- $\binom{n}{k}$ is the number of k-element subsets of an n-element set.

A Combinatorial Proof

- $\binom{n}{k}$ is the number of k-element subsets of an n-element set.

$$\boxed{\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}}$$

Therefore, each term (left and right) represents the number of subsets of a particular size chosen from an appropriately sized set.

A Combinatorial Proof

- $$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

A Combinatorial Proof

- $$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

  Number of k-subsets of an n-element set.

A Combinatorial Proof

- $$\boxed{\binom{n}{k}} = \boxed{\binom{n-1}{k-1}} + \binom{n-1}{k}$$

  Number of k-subsets of an n-element set.

  Number of $(k-1)$-subsets of an $(n-1)$-element set.

A Combinatorial Proof

- $$\boxed{\binom{n}{k}} = \boxed{\binom{n-1}{k-1}} + \boxed{\binom{n-1}{k}}$$

  Number of k-subsets of an n-element set.

  Number of $(k-1)$-subsets of an $(n-1)$-element set.

  Number of k-subsets of an $(n-1)$-element set.

A Combinatorial Proof

- $$\boxed{\binom{n}{k}} = \boxed{\binom{n-1}{k-1}} + \boxed{\binom{n-1}{k}}$$

  Number of k-subsets of an n-element set.

  Number of $(k-1)$-subsets of an $(n-1)$-element set.

  Number of k-subsets of an $(n-1)$-element set.

 Try to use sum principle to explain relationship among these three terms.

 Example: $n = 5$, $k = 2$

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}.$$

A Combinatorial Proof

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}.$$

A Combinatorial Proof

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}.$$

Consider $S = \{A, B, C, D, E\}$.

A Combinatorial Proof

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}.$$

Consider $S = \{A, B, C, D, E\}$.

Set S_1 of 2-subsets of S

$$S_1 = \{\{A, B\}, \{A, C\}, \{A, D\}, \{A, E\}, \{B, C\}, \\ \{B, D\}, \{B, E\}, \{C, D\}, \{C, E\}, \{D, E\}\}.$$

A Combinatorial Proof

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}.$$

Consider $S = \{A, B, C, D, E\}$.

Set S_1 of 2-subsets of S can be partitioned into 2 disjoint parts.

S_2 the 2-subsets that contain E and

S_3, the set of 2-subsets that do not contain E.

$$S_1 = \{\{A, B\}, \{A, C\}, \{A, D\}, \{A, E\}, \{B, C\}, \{B, D\}, \{B, E\}, \{C, D\}, \{C, E\}, \{D, E\}\}.$$

A Combinatorial Proof

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}.$$

Consider $S = \{A, B, C, D, E\}$.

Set S_1 of 2-subsets of S can be partitioned into 2 disjoint parts.

S_2 the 2-subsets that contain E and

S_3, the set of 2-subsets that do not contain E.

$$S_1 = \{\{A, B\}, \{A, C\}, \{A, D\}, \{A, E\}, \{B, C\}, \{B, D\}, \{B, E\}, \{C, D\}, \{C, E\}, \{D, E\}\}.$$

$$S_1 = \{\{A, B\}, \{A, C\}, \{A, D\}, \{A, E\}, \{B, C\}, \{B, D\}, \{B, E\}, \{C, D\}, \{C, E\}, \{D, E\}\}.$$

A Combinatorial Proof

- If n and k are integers satisfying $0 < k < n$, then

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

A Combinatorial Proof

- If n and k are integers satisfying $0 < k < n$, then

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Proof: Apply sum rule.

A Combinatorial Proof

- If n and k are integers satisfying $0 < k < n$, then

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Proof: Apply sum rule.

Let S_1 be set of all k-element subsets.

A Combinatorial Proof

- If n and k are integers satisfying $0 < k < n$, then

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Proof: Apply sum rule.

Let S_1 be set of all k-element subsets.

To apply sum rule, partition S_1 into S_2 and S_3.

Let S_2 be set of k-element subsets that contain x_n.

Let S_3 be set of k-element subsets that don't contain x_n.

Blaise Pascal

Born 1623; Died 1662

French Mathematician

A Founder of Probability Theory

Inventor of one of the first mechanical calculating machines

Pascal Programming Language named for him

The Binomial Theorem

$$(x+y) = \binom{1}{0}x + \binom{1}{1}y$$

The Binomial Theorem

$$(x+y) = \binom{1}{0}x + \binom{1}{1}y$$

$$(x+y)^2 = x^2 + 2xy + y^2 = \binom{2}{0}x^2 + \binom{2}{1}x^1y^1 + \binom{2}{2}y^2$$

The Binomial Theorem

$$(x+y) = \binom{1}{0}x + \binom{1}{1}y$$

$$(x+y)^2 = x^2 + 2xy + y^2 = \binom{2}{0}x^2 + \binom{2}{1}x^1y^1 + \binom{2}{2}y^2$$

$$\begin{aligned}(x+y)^3 &= x^3 + 3x^2y + 3xy^2 + y^3 \\ &= \binom{3}{0}x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + \binom{3}{3}y^3\end{aligned}$$

The Binomial Theorem

- Number of k-element subsets of an n-element set is called a **binomial coefficient** because of its role in the algebraic expansion of a binomial $(x + y)^n$.

The Binomial Theorem

- Number of k-element subsets of an n-element set is called a **binomial coefficient** because of its role in the algebraic expansion of a binomial $(x+y)^n$.

The Binomial Theorem For any integer $n \geq 0$,

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}$$

- Number of k-element subsets of an n-element set is called a **binomial coefficient** because of its role in the algebraic expansion of a binomial $(x+y)^n$.

  The Binomial Theorem For any integer $n \geq 0$,

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}$$

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i.$$

The Binomial Theorem

- Number of k-element subsets of an n-element set is called a **binomial coefficient** because of its role in the algebraic expansion of a binomial $(x+y)^n$.

The Binomial Theorem For any integer $n \geq 0$,

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}$$

$$(x+y)^n = \sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i.$$

Proof?

Application of the Binomial Theorem

- We may use the Binomial Theorem to prove

$$\boxed{\sum_{i=0}^{n} \binom{n}{i} = 2^n}$$

Labelling and Trinomial Coefficients

- Suppose we have k labels of one kind, e.g., red and $n - k$ labels of another, e.g., blue. In how many different ways can we apply these labels to n objects?

Labelling and Trinomial Coefficients

- Suppose we have k labels of one kind, e.g., red and $n-k$ labels of another, e.g., blue. In how many different ways can we apply these labels to n objects?

  Show that if we have k_1 labels of one kind, e.g., red, k_2 labels of a second kind, e.g., blue, and $k_3 = n - k_1 - k_2$ labels of a third kind, then there are $\frac{n!}{k_1!k_2!k_3!}$ ways to apply these labels to n objects

Labelling and Trinomial Coefficients

- Suppose we have k labels of one kind, e.g., red and $n-k$ labels of another, e.g., blue. In how many different ways can we apply these labels to n objects?

  Show that if we have k_1 labels of one kind, e.g., red, k_2 labels of a second kind, e.g., blue, and $k_3 = n - k_1 - k_2$ labels of a third kind, then there are $\frac{n!}{k_1!k_2!k_3!}$ ways to apply these labels to n objects

  What is the coefficient of $x^{k_1}y^{k_2}z^{k_3}$ in $(x+y+z)^n$?

Labelling and Trinomial Coefficients

- There are $\binom{n}{k_1}$ ways to choose the red items There are then $\binom{n-k_1}{k_2}$ ways to choose the blue items from the remaining $n-k_1$. The remaining k_3 items get labelled a third color.

Labelling and Trinomial Coefficients

- There are $\binom{n}{k_1}$ ways to choose the red items There are then $\binom{n-k_1}{k_2}$ ways to choose the blue items from the remaining $n-k_1$. The remaining k_3 items get labelled a third color.

  Using the *product rule* the total number of labellings is

$$
\begin{aligned}
\binom{n}{k_1}\binom{n-k_1}{k_2} &= \frac{n!}{k_1!(n-k_1)!}\frac{(n-k_1)!}{(k_2)!(n-k_1-k_2)!} \\
&= \frac{n!}{k_1!k_2!(n-k_1-k_2)!} = \frac{n!}{k_1!k_2!k_3!}
\end{aligned}
$$

Labelling and Trinomial Coefficients

- When $k_1 + k_2 + k_3 = n$, we call

$$\frac{n!}{k_1!k_2!k_3!}$$

a *trinomial coefficient* and denote it as

$$\binom{n}{k_1 \quad k_2 \quad k_3}$$

Labelling and Trinomial Coefficients

- When $k_1 + k_2 + k_3 = n$, we call

$$\frac{n!}{k_1!k_2!k_3!}$$

a *trinomial coefficient* and denote it as

$$\binom{n}{k_1 \quad k_2 \quad k_3}$$

What is the coefficient of $x^{k_1}y^{k_2}z^{k_3}$ in $(x+y+z)^n$?

- Suppose that 25 students are in a room. What is the probability that at least two of them share a birthday?

The Birthday Paradox

- Suppose that 25 students are in a room. What is the probability that at least two of them share a birthday?

  It's greater than $1/2$! (only need 23)

- Suppose that 25 students are in a room. What is the probability that at least two of them share a birthday?

  It's greater than $1/2$! (only need 23)

  A_n – "there are n students in a room and at least two of them share a birthday."

The Birthday Paradox

- Suppose that 25 students are in a room. What is the probability that at least two of them share a birthday?

  It's greater than 1/2! (only need 23)

  A_n – "there are n students in a room and at least two of them share a birthday."

  We may assume that a year has 365 days and there are no twins in the room.

The Birthday Paradox

- Suppose that 25 students are in a room. What is the probability that at least two of them share a birthday?

  It's greater than $1/2$! (only need 23)

  A_n – "there are n students in a room and at least two of them share a birthday."

  We may assume that a year has 365 days and there are no twins in the room.

  This will be very similar to the analysis of hashing n keys into a table of size 365.

The Birthday Paradox

- A_n – "there are n students in a room and at least two of them share a birthday."

  Sample space: $|S| = 365^n$

The Birthday Paradox

- A_n – "there are n students in a room and at least two of them share a birthday."

  Sample space: $|S| = 365^n$

  B_n – "there are n students in a room and none of them share a birthday."

The Birthday Paradox

- A_n – "there are n students in a room and at least two of them share a birthday."

  Sample space: $|S| = 365^n$

  B_n – "there are n students in a room and none of them share a birthday."

  $\#B_n = 365 \times 364 \times \cdots \times (365 - (n-1))$

The Birthday Paradox

- A_n – "there are n students in a room and at least two of them share a birthday."

  Sample space: $|S| = 365^n$

  B_n – "there are n students in a room and none of them share a birthday."

  $\#B_n = 365 \times 364 \times \cdots \times (365 - (n-1))$

  $\#A_n + \#B_n = 365^n$

The Birthday Paradox

n	A_n	B_n	n	A_n	B_n
1	0.00000000	1.00000000	16	0.28360400	0.71639599
2	0.00273972	0.99726027	17	0.31500766	0.68499233
3	0.00820416	0.99179583	18	0.34691141	0.65308858
4	0.01635591	0.98364408	19	0.37911852	0.62088147
5	0.02713557	0.97286442	20	0.41143838	0.58856161
6	0.04046248	0.95953751	21	0.44368833	0.55631166
7	0.05623570	0.94376429	22	0.47569530	0.52430469
8	0.07433529	0.92566470	23	0.50729723	0.49270276 ...
9	0.09462383	0.90537616	24	0.53834425	0.46165574
10	0.11694817	0.88305182	25	0.56869970	0.43130029
11	0.14114137	0.85885862	26	0.59824082	0.40175917
12	0.16702478	0.83297521	27	0.62685928	0.37314071
13	0.19441027	0.80558972	28	0.65446147	0.34553852
14	0.22310251	0.77689748	29	0.68096853	0.31903146
15	0.25290131	0.74709868	30	0.70631624	0.29368375

"Birthday" attacks

- Event A: at least two people in the room have the same birthday

  Event B: no two people in the room have the same birthday

  $\Pr[A] = 1 - \Pr[B]$

$$
\begin{aligned}
\Pr[B] &= \left(1 - \frac{1}{365}\right) \cdot \left(1 - \frac{2}{365}\right) \cdot \dots \cdot \left(1 - \frac{n-1}{365}\right) \\
&= \prod_{i=1}^{n-1} \left(1 - \frac{i}{365}\right).
\end{aligned}
$$

  $\Pr[A] = 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{365}\right)$

"Birthday" attacks

- Event A: at least two people in the room have the same birthday

  Event B: no two people in the room have the same birthday

  $\Pr[A] = 1 - \Pr[B]$

$$\begin{aligned}\Pr[B] &= \left(1 - \frac{1}{365}\right) \cdot \left(1 - \frac{2}{365}\right) \cdot \cdots \cdot \left(1 - \frac{n-1}{365}\right) \\ &= \prod_{i=1}^{n-1} \left(1 - \frac{i}{365}\right).\end{aligned}$$

  $\Pr[A] = 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{365}\right)$

  $p(n; H) := 1 - \prod_{i=1}^{n-1}(1 - \frac{i}{H})$

“Birthday” attacks

- Since $e^x = 1 + x + \frac{x^2}{2!} + \cdots$, for $|x| \ll 1$, $e^x \approx 1 + x$

“Birthday” attacks

- Since $e^x = 1 + x + \frac{x^2}{2!} + \cdots$, for $|x| \ll 1$, $e^x \approx 1 + x$

  Thus, we have $e^{-i/H} \approx 1 - \frac{i}{H}$.

"Birthday" attacks

- Since $e^x = 1 + x + \frac{x^2}{2!} + \cdots$, for $|x| \ll 1$, $e^x \approx 1 + x$

  Thus, we have $e^{-i/H} \approx 1 - \frac{i}{H}$.

  Recall that $p(n; H) := 1 - \prod_{i=1}^{n-1}(1 - \frac{i}{H})$

  This probability can be approximated as
  $$p(n; H) \approx 1 - e^{-n(n-1)/2H} \approx 1 - e^{-n^2/2H}.$$

"Birthday" attacks

- Since $e^x = 1 + x + \frac{x^2}{2!} + \cdots$, for $|x| \ll 1$, $e^x \approx 1 + x$

  Thus, we have $e^{-i/H} \approx 1 - \frac{i}{H}$.

  Recall that $p(n; H) := 1 - \prod_{i=1}^{n-1}(1 - \frac{i}{H})$

  This probability can be approximated as

  $$p(n; H) \approx 1 - e^{-n(n-1)/2H} \approx 1 - e^{-n^2/2H}.$$

  Let $n(p; H)$ be the smallest number of values we have to choose, such that the probability for finding a collision is at least p. By inverting the expression above, we have

  $$n(p; H) \approx \sqrt{2H \ln \frac{1}{1-p}}.$$

Euclidean Algorithm

- The Euclidean algorithm in pseudocode

ALGORITHM 1 The Euclidean Algorithm.

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return x\{gcd(a, b) is x\}

The number of divisions required to find $\gcd(a, b)$ is $O(\log b)$, where $a \geq b$. (this will be proved later.)

Euclidean Algorithm

- The Euclidean algorithm in pseudocode

ALGORITHM 1 The Euclidean Algorithm.

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return x\{gcd(a, b) is x\}

The number of divisions required to find $\gcd(a, b)$ is $O(\log b)$, where $a \geq b$. (this will be proved later.)

Why ?

Euclidean Algorithm

- Key steps in the Euclidean algorithm

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 & 0 \le r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 & 0 \le r_3 < r_2, \\
&\ \ \vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_{\mathrm{n}} & 0 \le r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n \, .
\end{aligned}
$$

- Key steps in the Euclidean algorithm

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 & 0 \le r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 & 0 \le r_3 < r_2, \\
&\;\;\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \le r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n \,.
\end{aligned}
$$

Observation:

$r_{i+2} = r_i \bmod r_{i+1}$

Euclidean Algorithm

- Key steps in the Euclidean algorithm

$$
\begin{array}{llr}
r_0 & = r_1 q_1 + r_2 & 0 \le r_2 < r_1, \\
r_1 & = r_2 q_2 + r_3 & 0 \le r_3 < r_2, \\
 & \quad \vdots & \\
r_{n-2} & = r_{n-1} q_{n-1} + r_n & 0 \le r_n < r_{n-1}, \\
r_{n-1} & = r_n q_n . &
\end{array}
$$

Observation:

$r_{i+2} = r_i \bmod r_{i+1}$

We claim that $r_{i+2} < \frac{1}{2} r_i$

Euclidean Algorithm

- Key steps in the Euclidean algorithm

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 & 0 \le r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 & 0 \le r_3 < r_2, \\
&\ \ \vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \le r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n .
\end{aligned}
$$

Observation:

$r_{i+2} = r_i \bmod r_{i+1}$

We claim that $r_{i+2} < \frac{1}{2} r_i$

Case (i): $r_{i+1} \le \frac{1}{2} r_i$: $r_{i+2} < r_{i+1} \le \frac{1}{2} r_i$.

Case (ii): $r_{i+1} > \frac{1}{2} r_i$: $r_{i+2} = r_i \bmod r_{i+1} = r_i - r_{i+1} < \frac{1}{2} r_i$.

Euclidean Algorithm

- Key steps in the Euclidean algorithm

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 \le r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 && 0 \le r_3 < r_2, \\
&\ \vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 \le r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n .
\end{aligned}
$$

See [Theorem 1 p. 347].

Observation:

$$r_{i+2} = r_i \bmod r_{i+1}$$

We claim that $r_{i+2} < \frac{1}{2} r_i$

Case (i): $r_{i+1} \le \frac{1}{2} r_i$: $r_{i+2} < r_{i+1} \le \frac{1}{2} r_i$.

Case (ii): $r_{i+1} > \frac{1}{2} r_i$: $r_{i+2} = r_i \bmod r_{i+1} = r_i - r_{i+1} < \frac{1}{2} r_i$.

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

Solving Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

  $$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

  where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

  ◇ linear: it is a linear combination of previous terms

Solving Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

◇ linear: it is a linear combination of previous terms

◇ homogeneous: all terms are multiples of a_j's

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

◇ linear: it is a linear combination of previous terms

◇ homogeneous: all terms are multiples of a_j's

◇ degree k: a_n is expressed by the previous k terms

Solving Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

◇ linear: it is a linear combination of previous terms

◇ homogeneous: all terms are multiples of a_j's

◇ degree k: a_n is expressed by the previous k terms

◇ constant coefficients: coefficients are constants

Solving Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

  $$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

  where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

  ◇ linear: it is a linear combination of previous terms

  ◇ homogeneous: all terms are multiples of a_j's

  ◇ degree k: a_n is expressed by the previous k terms

  ◇ constant coefficients: coefficients are constants

  By induction, such a recurrence relation is uniquely determined by this recurrence relation, and k initial conditions $a_0, a_1, \ldots, a_{k-1}$.

Examples of Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

Examples

$$P_n = (1.11)P_{n-1}$$

$$f_n = f_{n-1} + f_{n-2}$$

$$a_n = a_{n-1} + a_{n-2}^2$$

$$H_n = 2H_{n-1} + 1$$

$$B_n = nB_{n-1}$$

Examples of Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

Examples

$P_n = (1.11)P_{n-1}$ linear homogeneous recurrence relation of degree 1

$f_n = f_{n-1} + f_{n-2}$

$a_n = a_{n-1} + a_{n-2}^2$

$H_n = 2H_{n-1} + 1$

$B_n = nB_{n-1}$

Examples of Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

Examples

$P_n = (1.11) P_{n-1}$ linear homogeneous recurrence relation of degree 1

$f_n = f_{n-1} + f_{n-2}$ linear homogeneous recurrence relation of degree 2

$a_n = a_{n-1} + a_{n-2}^2$

$H_n = 2H_{n-1} + 1$

$B_n = nB_{n-1}$

Examples of Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

  $$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

  where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

  Examples

  $P_n = (1.11)P_{n-1}$ linear homogeneous recurrence relation of degree 1

  $f_n = f_{n-1} + f_{n-2}$ linear homogeneous recurrence relation of degree 2

  $a_n = a_{n-1} + a_{n-2}^2$ NOT linear

  $H_n = 2H_{n-1} + 1$

  $B_n = nB_{n-1}$

Examples of Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

Examples

$P_n = (1.11)P_{n-1}$	linear homogeneous recurrence relation of degree 1
$f_n = f_{n-1} + f_{n-2}$	linear homogeneous recurrence relation of degree 2
$a_n = a_{n-1} + a_{n-2}^2$	NOT linear
$H_n = 2H_{n-1} + 1$	NOT homogeneous
$B_n = nB_{n-1}$	

Examples of Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

Examples

$P_n = (1.11)P_{n-1}$	linear homogeneous recurrence relation of degree 1
$f_n = f_{n-1} + f_{n-2}$	linear homogeneous recurrence relation of degree 2
$a_n = a_{n-1} + a_{n-2}^2$	NOT linear
$H_n = 2H_{n-1} + 1$	NOT homogeneous
$B_n = nB_{n-1}$	coefficients are not constants

Solving Linear Recurrence Relations

- **Example** Consider the recurrence relation

  $a_n = 2a_{n-1} - a_{n-2}$,

  Which of the following are solutions?

  - $a_n = 3n$:

  - $a_n = 2^n$:

  - $a_n = 5$:

- **Example** Consider the recurrence relation

  $$a_n = 2a_{n-1} - a_{n-2},$$

  Which of the following are solutions?

  - $a_n = 3n$: YES
  - $a_n = 2^n$: NO
  - $a_n = 5$: YES

Solving Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

Solving Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

Fact: Assume that the sequences a_n and a'_n both satisfy the recurrence, then $b_n = a_n + a'_n$, $d_n = \alpha a_n$ also satisfy the recurrence, where α is a constant.

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

Fact: Assume that the sequences a_n and a'_n both satisfy the recurrence, then $b_n = a_n + a'_n$, $d_n = \alpha a_n$ also satisfy the recurrence, where α is a constant.

This means: If we find some solutions to a linear homogeneous recurrence, then any linear combination of them will also be a solution.

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

Fact: Assume that the sequences a_n and a'_n both satisfy the recurrence, then $b_n = a_n + a'_n$, $d_n = \alpha a_n$ also satisfy the recurrence, where α is a constant.

This means: If we find some solutions to a linear homogeneous recurrence, then any linear combination of them will also be a solution.

So, try to find any solution of the form $a_n = r^n$ that satisfies the recurrence.

Solving Linear Recurrence Relations

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

  $$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

  where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

  Basic idea: Look for solutions of the form $a_n = r^n$, where r is a constant.

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

  $$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

  where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

  Basic idea: Look for solutions of the form $a_n = r^n$, where r is a constant.

  ◇ Bring $a_n = r^n$ back to the recurrence relation:

  $$r^n = c_1 r^{n-1} + c_2 r^{n-2} + \cdots + c_k r^{n-k},$$

  i.e.,

  $$r^{n-k}(r^k - c_1 r^{k-1} - \cdots - c_k) = 0$$

- **Definition** A *linear homogeneous relation of degree k* with constant coefficients is a recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers, and $c_k \neq 0$.

Basic idea: Look for solutions of the form $a_n = r^n$, where r is a constant.

◇ Bring $a_n = r^n$ back to the recurrence relation:

$$r^n = c_1 r^{n-1} + c_2 r^{n-2} + \cdots + c_k r^{n-k},$$

i.e.,

$$r^{n-k}(r^k - c_1 r^{k-1} - \cdots - c_k) = 0$$

◇ The solutions to the *characteristic equation* can yield an explicit formula for the sequence.

$$(r^k - c_1 r^{k-1} - \cdots - c_k) = 0$$

Recall: Problem IV

- **Fibonacci number**

  $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$

Recall: Problem IV

- **Fibonacci number**

  $F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$

  ◇ What is the closed-form expression of F_n?

Recall: Problem IV

- **Fibonacci number**

  $F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$

  ◇ What is the closed-form expression of F_n?

  Consider $x^n = x^{n-1} + x^{n-2}$, with $x \neq 0$. There are two different roots

  $$\phi = \frac{1+\sqrt{5}}{2}, \quad \psi = \frac{1-\sqrt{5}}{2}$$

  Then F_n can be the form of $a\phi^n + b\psi^n$. By $F_0 = 0$ and $F_1 = 1$, we have $a + b = 0$ and $\phi a + \psi b = 1$, leading to $a = \frac{1}{\sqrt{5}}$, $b = -a$. Therefore,

  $$F_n = \frac{\phi^n - \psi^n}{\sqrt{5}}$$

Solving Linear Recurrence Relations of degree 2

- Consider an arbitrary linear homogeneous relation of degree 2 with constant coefficients:

  $a_n = c_1 a_{n-1} + c_2 a_{n-2}$.

Solving Linear Recurrence Relations of degree 2

- Consider an arbitrary linear homogeneous relation of degree 2 with constant coefficients:

  $$a_n = c_1 a_{n-1} + c_2 a_{n-2}.$$

  The characteristic equation (CE) is:

  $$r^2 - c_1 r - c_2 = 0.$$

Solving Linear Recurrence Relations of degree 2

- Consider an arbitrary linear homogeneous relation of degree 2 with constant coefficients:

  $$a_n = c_1 a_{n-1} + c_2 a_{n-2}.$$

  The characteristic equation (CE) is:

  $$r^2 - c_1 r - c_2 = 0.$$

  Theorem If this CE has 2 roots $r_1 \neq r_2$, then the sequence $\{a_n\}$ is a solution of the recurrence relation if and only if $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for $n \geq 0$ and constants α_1, α_2.

Solving Linear Recurrence Relations of degree 2

- Consider an arbitrary linear homogeneous relation of degree 2 with constant coefficients:

  $$a_n = c_1 a_{n-1} + c_2 a_{n-2}.$$

  The characteristic equation (CE) is:

  $$r^2 - c_1 r - c_2 = 0.$$

  Theorem If this CE has 2 roots $r_1 \neq r_2$, then the sequence $\{a_n\}$ is a solution of the recurrence relation if and only if $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for $n \geq 0$ and constants α_1, α_2.

  Proof?

Solving Linear Recurrence Relations of degree 2

- Consider an arbitrary linear homogeneous relation of degree 2 with constant coefficients:

  $a_n = c_1 a_{n-1} + c_2 a_{n-2}$.

  The characteristic equation (CE) is:

  $r^2 - c_1 r - c_2 = 0$.

  Theorem If this CE has 2 roots $r_1 \neq r_2$, then the sequence $\{a_n\}$ is a solution of the recurrence relation if and only if $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ for $n \geq 0$ and constants α_1, α_2.

  Proof?

  See [Theorem 1 p. 515].

- **Example 1** $a_n = a_{n-1} + 2a_{n-2}$, with $a_0 = 2$, $a_1 = 7$

- **Example 1** $a_n = a_{n-1} + 2a_{n-2}$, with $a_0 = 2$, $a_1 = 7$

  The *characteristic equation* is

  $r^2 - r - 2 = 0$.

Solving Linear Recurrence Relations of degree 2

- **Example 1** $a_n = a_{n-1} + 2a_{n-2}$, with $a_0 = 2$, $a_1 = 7$

  The *characteristic equation* is

  $$r^2 - r - 2 = 0.$$

  Two roots are 2 and -1. So, assume that

  $$a_n = \alpha_1 2^n + \alpha_2 (-1)^n.$$

- **Example 1** $a_n = a_{n-1} + 2a_{n-2}$, with $a_0 = 2$, $a_1 = 7$

  The *characteristic equation* is

  $r^2 - r - 2 = 0.$

  Two roots are 2 and -1. So, assume that

  $a_n = \alpha_1 2^n + \alpha_2(-1)^n.$

  By the two initial conditions, we have

  $a_0 = \alpha_1 + \alpha_2 = 2$

  $a_1 = 2\alpha_1 - \alpha_2 = 7$

Solving Linear Recurrence Relations of degree 2

- **Example 1** $a_n = a_{n-1} + 2a_{n-2}$, with $a_0 = 2$, $a_1 = 7$

  The *characteristic equation* is

  $r^2 - r - 2 = 0.$

  Two roots are 2 and -1. So, assume that

  $a_n = \alpha_1 2^n + \alpha_2(-1)^n$.

  By the two initial conditions, we have

  $a_0 = \alpha_1 + \alpha_2 = 2$
  $a_1 = 2\alpha_1 - \alpha_2 = 7$

  We get $\alpha_1 = 3$ and $\alpha_2 = -1$. Thus,

  $a_n = 3 \cdot 2^n - (-1)^n$

- **Example 2** $a_n = 7a_{n-1} - 10a_{n-2}$, with $a_0 = 2$, $a_1 = 1$

- **Example 2** $a_n = 7a_{n-1} - 10a_{n-2}$, with $a_0 = 2$, $a_1 = 1$

  The *characteristic equation* is

  $r^2 - 7r + 10 = 0$.

- **Example 2** $a_n = 7a_{n-1} - 10a_{n-2}$, with $a_0 = 2$, $a_1 = 1$

  The *characteristic equation* is

  $r^2 - 7r + 10 = 0.$

  Two roots are 2 and 5. So, assume that

  $a_n = \alpha_1 2^n + \alpha_2 5^n.$

- **Example 2** $a_n = 7a_{n-1} - 10a_{n-2}$, with $a_0 = 2$, $a_1 = 1$

  The *characteristic equation* is

  $r^2 - 7r + 10 = 0.$

  Two roots are 2 and 5. So, assume that

  $a_n = \alpha_1 2^n + \alpha_2 5^n.$

  By the two initial conditions, we have

  $a_0 = \alpha_1 + \alpha_2 = 2$

  $a_1 = 2\alpha_1 + 5\alpha_2 = 1$

Solving Linear Recurrence Relations of degree 2

- **Example 2** $a_n = 7a_{n-1} - 10a_{n-2}$, with $a_0 = 2$, $a_1 = 1$

  The *characteristic equation* is

  $$r^2 - 7r + 10 = 0.$$

  Two roots are 2 and 5. So, assume that

  $$a_n = \alpha_1 2^n + \alpha_2 5^n.$$

  By the two initial conditions, we have

  $$a_0 = \alpha_1 + \alpha_2 = 2$$
  $$a_1 = 2\alpha_1 + 5\alpha_2 = 1$$

  We get $\alpha_1 = 3$ and $\alpha_2 = -1$. Thus,

  $$a_n = 3 \cdot 2^n - 5^n$$

Solving Linear Recurrence Relations of degree k

- Consider an arbitrary linear homogeneous relation of degree k with constant coefficients:

  $a_n = \sum_{i=1}^{k} c_i a_{n-i}$.

Solving Linear Recurrence Relations of degree k

- Consider an arbitrary linear homogeneous relation of degree k with constant coefficients:

  $$a_n = \sum_{i=1}^{k} c_i a_{n-i}.$$

  The characteristic equation (CE) is:

  $$r^k - \sum_{i=1}^{k} c_i r^{k-i} = 0.$$

Solving Linear Recurrence Relations of degree k

- Consider an arbitrary linear homogeneous relation of degree k with constant coefficients:

  $$a_n = \sum_{i=1}^{k} c_i a_{n-i}.$$

  The characteristic equation (CE) is:

  $$r^k - \sum_{i=1}^{k} c_i r^{k-i} = 0.$$

  Theorem If this CE has k distinct roots r_i, then the solutions to the recurrence are of the form

  $$a_n = \sum_{i=1}^{k} \alpha_i r_i^n$$

  for all $n \geq 0$, where the α_i's are constants.

Solving Linear Recurrence Relations of degree k

- Consider an arbitrary linear homogeneous relation of degree k with constant coefficients:

  $$a_n = \sum_{i=1}^{k} c_i a_{n-i}.$$

  The characteristic equation (CE) is:

  $$r^k - \sum_{i=1}^{k} c_i r^{k-i} = 0.$$

  Theorem If this CE has k distinct roots r_i, then the solutions to the recurrence are of the form

  $$a_n = \sum_{i=1}^{k} \alpha_i r_i^n$$

  for all $n \geq 0$, where the α_i's are constants.

  Example $a_n = 2a_{n-1} + 5a_{n-2} - 6a_{n-3}$

The Case of Degenerate Roots

- **Theorem** If the CE $r^2 - c_1 r - c_2 = 0$ has only 1 root r_0, then

  $$a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n,$$

  for all $n \geq 0$ and two constants α_1 and α_2.

The Case of Degenerate Roots

- **Theorem** If the CE $r^2 - c_1 r - c_2 = 0$ has only 1 root r_0, then

$$a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n,$$

for all $n \geq 0$ and two constants α_1 and α_2.

Proof?

- **Theorem** If the CE $r^2 - c_1 r - c_2 = 0$ has only 1 root r_0, then

$$a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n,$$

for all $n \geq 0$ and two constants α_1 and α_2.

Proof?

Exercise.

The Case of Degenerate Roots

- **Example** $a_n = 4a_{n-1} - 4a_{n-2}$, with $a_0 = 1$, $a_1 = 0$

The Case of Degenerate Roots

- **Example** $a_n = 4a_{n-1} - 4a_{n-2}$, with $a_0 = 1$, $a_1 = 0$

  The *characteristic equation* is

  $$r^2 - 4r + 4 = 0.$$

The Case of Degenerate Roots

- **Example** $a_n = 4a_{n-1} - 4a_{n-2}$, with $a_0 = 1$, $a_1 = 0$

  The *characteristic equation* is

  $$r^2 - 4r + 4 = 0.$$

  The only root is 2. So, assume that

  $$a_n = \alpha_1 2^n + \alpha_2 n 2^n.$$

The Case of Degenerate Roots

- **Example** $a_n = 4a_{n-1} - 4a_{n-2}$, with $a_0 = 1$, $a_1 = 0$

  The *characteristic equation* is

  $$r^2 - 4r + 4 = 0.$$

  The only root is 2. So, assume that

  $$a_n = \alpha_1 2^n + \alpha_2 n 2^n.$$

  By the two initial conditions, we have

  $$a_0 = \alpha_1 = 1$$
  $$a_1 = 2\alpha_1 + 2\alpha_2 = 0$$

The Case of Degenerate Roots

- **Example** $a_n = 4a_{n-1} - 4a_{n-2}$, with $a_0 = 1$, $a_1 = 0$

  The *characteristic equation* is

  $$r^2 - 4r + 4 = 0.$$

  The only root is 2. So, assume that

  $$a_n = \alpha_1 2^n + \alpha_2 n 2^n.$$

  By the two initial conditions, we have

  $$a_0 = \alpha_1 = 1$$
  $$a_1 = 2\alpha_1 + 2\alpha_2 = 0$$

  We get $\alpha_1 = 1$ and $\alpha_2 = -1$. Thus,

  $$a_n = 2^n - n2^n$$

The Case of Degenerate Roots in General

- **Theorem** [Theorem 4, p.519] Suppose that there are t roots $r_1, \ldots, r_t$ with multiplicities $m_1, \ldots, m_t$. Then

$$a_n = \sum_{i=1}^{t} \left(\sum_{j=0}^{m_i - 1} \alpha_{i,j} n^j \right) r_i^n,$$

for all $n \geq 0$ and constants $\alpha_{i,j}$.

- **Theorem** [Theorem 4, p.519] Suppose that there are t roots $r_1, \ldots, r_t$ with multiplicities $m_1, \ldots, m_t$. Then

  $$a_n = \sum_{i=1}^{t} \left(\sum_{j=0}^{m_i - 1} \alpha_{i,j} n^j \right) r_i^n,$$

  for all $n \geq 0$ and constants $\alpha_{i,j}$.

  Example

  $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$ with $a_0 = 1$, $a_1 = -2$, $a_2 = -1$

- **Definition** A *linear nonhomogeneous relation* with constant coefficients may contain some terms $F(n)$ that depend only on n

  $$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n).$$

  The recurrence relation

  $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$ is called the *associated homogeneous recurrence relation*.

Linear Nonhomogeneous Recurrence Relations

- **Definition** A *linear nonhomogeneous relation* with constant coefficients may contain some terms $F(n)$ that depend only on n

  $$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n).$$

  The recurrence relation

  $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$ is called the *associated homogeneous recurrence relation*.

  Fact: Assume that the sequence b_n satisfies the recurrence. Then another sequece a_n satisfies the non-homogeneous recurrence if and only if $h_n = a_n - b_n$ is a sequence that satisfies the associated homogeneous recurrence.

Linear Nonhomogeneous Recurrence Relations

- **Definition** A *linear nonhomogeneous relation* with constant coefficients may contain some terms $F(n)$ that depend only on n

  $$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n).$$

  The recurrence relation

  $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$ is called the *associated homogeneous recurrence relation*.

  Fact: Assume that the sequence b_n satisfies the recurrence. Then another sequece a_n satisfies the non-homogeneous recurrence if and only if $h_n = a_n - b_n$ is a sequence that satisfies the associated homogeneous recurrence.

  Idea: We already know how to find h_n. For many common $f(n)$, a solution b_n to the non-homogeneous recurrence is similar to $f(n)$. We then need find $a_n = b_n + h_n$ to the non-homogeneous recurrence that satisfies both recurrence and initial conditions.

- **Theorem** If $a_n = p(n)$ is any particular solution to the linear nonhomogeneous relation with constant coefficients,

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n),$$

Then all its solutions are of the form

$$a_n = p(n) + h(n),$$

where $a_n = h(n)$ is any solution to the associated homogeneous recurrence relation

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}.$$

Solving Linear Nonhomogeneous Recurrence Relations

- **Example** $a_n = 3a_{n-1} + 2n$. Which solution has $a_1 = 3$?

- **Example** $a_n = 3a_{n-1} + 2n$. Which solution has $a_1 = 3$?

  The *characteristic equation* of the associated linear homogeneous recurrence relation is $r^2 - 3r = 0$. Thus, the solution to the original problem are all of the form $a_n = \alpha 3^n + p(n)$.

- **Example** $a_n = 3a_{n-1} + 2n$. Which solution has $a_1 = 3$?

  The *characteristic equation* of the associated linear homogeneous recurrence relation is $r^2 - 3r = 0$. Thus, the solution to the original problem are all of the form $a_n = \alpha 3^n + p(n)$.

  We try a degree-t polynomial as the particular solution $p(n)$.

- **Example** $a_n = 3a_{n-1} + 2n$. Which solution has $a_1 = 3$?

  The *characteristic equation* of the associated linear homogeneous recurrence relation is $r^2 - 3r = 0$. Thus, the solution to the original problem are all of the form
  $a_n = \alpha 3^n + p(n)$.

  We try a degree-t polynomial as the particular solution $p(n)$.

  Let $p(n) = cn + d$, then
  $cn + d = 3(c(n-1) + d) + 2n$, which means
  $(2c + 2)n + (2d - 3c) = 0$.

Solving Linear Nonhomogeneous Recurrence Relations

- **Example** $a_n = 3a_{n-1} + 2n$. Which solution has $a_1 = 3$?

  The *characteristic equation* of the associated linear homogeneous recurrence relation is $r^2 - 3r = 0$. Thus, the solution to the original problem are all of the form $a_n = \alpha 3^n + p(n)$.

  We try a degree-t polynomial as the particular solution $p(n)$.

  Let $p(n) = cn + d$, then
  $cn + d = 3(c(n-1) + d) + 2n$, which means
  $(2c + 2)n + (2d - 3c) = 0$.

  We get $c = -1$ and $d = -3/2$. Thus,
  $$p(n) = -n - 3/2$$

Next Lecture

- generating function, relation ...