

Heaven's light is our guide"

Rajshahi University of Engineering & Technology
Department of Computer Science & Engineering

Network Security

Course No. : 305

Chapter 5: Counting

Prepared By : Julia Rahman

5.1 The basics of counting

5.1 The basics of counting

 **Problem:** [# allowable passwds]

□ Properties on a passwd:

1. 6,7 or 8 chars in length
2. alphabet: $S = \{0, \dots, 9\} \cup \{A, B, \dots, Z\}$
3. contains at least one digit.

\Rightarrow How many passwds are there ?

Solution:

#passwd = #passwd of length 6 + ..7 +.. 8

#passwd of length $k = |S^k \setminus S^k \text{ w/o digit}|$
 $= |S^k| - |S^k \text{ w/o digit}| = |S|^k - (|S|-10)^k$

Hence #passwd = $(36^8 - 26^8) + (36^7 - 26^7) + (36^6 - 26^6)$.


□ Two basic counting principles:

- 1) The product rule and
- 2) The sum rule


5.1 The basics of counting

THE PRODUCT RULE:

- ✓ Suppose that a procedure can be broken down into a sequence of two tasks.
- ✓ If there are n_1 ways to do the first task and for each of these ways of doing the first task, there are n_2 ways to do the second task, then there are $n_1 n_2$ ways to do the procedure.


 **EXAMPLE 1:** A company with just two employees, Sanchez and Patel, rents a floor of a building with 12 offices. How many ways are there to assign different offices to these two employees?

Solution: Assigning offices to these two employees consists of assigning an office to Sanchez, which can be done in 12 ways, then assigning an office to Patel different from the office assigned to Sanchez, which can be done in 11 ways. By product rule, there are $12 \cdot 11 = 132$ ways to assign offices to these two employees.

 **EXAMPLE 2:** The chairs of an auditorium are to be labeled with a letter and a positive integer not exceeding 100. What is the largest number of chairs that can be labeled differently?

Solution: Labeling a chair consists of two tasks, assigning one of the 26 letters and then assigning one of the 100 possible integers to the seat. The product rule shows that there are $26 \cdot 100 = 2600$ different ways that a chair can be labeled.

5.1 The basics of counting

 **EXAMPLE 3:** There are 32 microcomputers in a computer center. Each microcomputer has 24 ports. How many different ports to a microcomputer in the center are there?

Solution: The procedure of choosing a port consists of two tasks, first picking a microcomputer and then picking a port on this microcomputer. Because there are 32 ways to choose the microcomputer and 24 ways to choose the port no matter which microcomputer has been selected, the product rule shows that there are $32 \cdot 24 = 768$ ports.

 **EXAMPLE 4:** How many different bit strings of length seven are there?

Solution: Each of the seven bits can be chosen in two ways, because each bit is either 0 or 1. Therefore, the product rule shows there are a total of $2^7 = 128$ different bit strings of length seven.

5.1 The basics of counting

✚ THE SUM RULE:

- ✓ If a task can be done either in one of n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.

✚ **EXAMPLE 11:** Suppose that either a member of the mathematics faculty or a student who is a mathematics major is chosen as a representative to a university committee. How many different choices are there for this representative if there are 37 members of the mathematics faculty and 83 mathematics majors and no one is both a faculty member and a student?

Solution: There are 37 ways to choose a member of the mathematics faculty and there are 83 ways to choose a student who is a mathematics major. Choosing a member of the mathematics faculty is never the same as choosing a student who is a mathematics major because no one is both a faculty member and a student. By the sum rule it follows that there are $37 + 83 = 120$ possible ways to pick this representative.

5.1 The basics of counting



EXAMPLE 12: A student can choose a computer project from one of three lists. The three lists contain 23, 15, and 19 possible projects, respectively. No project is on more than one list. How many possible projects are there to choose from?

Solution: The student can choose a project by selecting a project from the first list, the second list, or the third list. Because no project is on more than one list, by the sum rule there are $23 + 15 + 19 = 57$ ways to choose a project.


5.2 The Pigeonhole Principle


5.2 The Pigeonhole Principle


The pigeonhole principle:

If k is a positive integer and $k + 1$ or more objects are placed into k boxes, then there is at least one box containing two or more of the objects.

Proof: We will prove the pigeonhole principle using a proof by contraposition. Suppose that none of the k boxes contains more than one object. Then the total number of objects would be at most k . This is a contradiction, because there are at least $k + 1$ objects.

 **EXAMPLE 1:** Among any group of 367 people, there must be at least two with the same birthday, because there are only 366 possible birthdays.

 **EXAMPLE 2:** In any group of 27 English words, there must be at least two that begin with the same letter, because there are 26 letters in the English alphabet.

 **EXAMPLE 3:** How many students must be in a class to guarantee that at least two students receive the same score on the final exam, if the exam is graded on a scale from 0 to 100 points?

Solution: There are 101 possible scores on the final. The pigeonhole principle shows that among any 102 students there must be at least 2 students with the same score.

5.2 The Pigeonhole Principle

Generalized pigeonhole principle

✚ **Theorem 2:** If N objects are placed into k boxes, then there is at least one box containing at least $\lceil N / k \rceil$ objects.

Proof: We will use a proof by contradiction. Suppose that none of the boxes contains more than $\lceil N / k \rceil - 1$ objects. Then, the total number of objects is at most

$$k(\lceil \frac{N}{k} \rceil - 1) < k(\frac{N}{k} + 1 - 1) = N$$

where the inequality $\lceil N / k \rceil < (N / k) + 1$ has been used. This is a contradiction because there are a total of N objects.


✚ **EXAMPLE 5:** Among 100 people there are at least $\lceil 100/12 \rceil = 9$ who were born in the same month.


5.3 Permutations and Combinations

5.3 Permutations and Combinations

Permutation:

- ✓ A set of distinct objects is an ordered arrangement of these objects.
- ✓ An ordered arrangement of r elements of a set is called an r -permutation.

 **Example:** Let $S = \{ 1, 2, 3 \}$. The ordered arrangement 3, 1, 2 is a permutation of S . The ordered arrangement 3, 2 is a 2-permutation of S .

 **EXAMPLE 3:** Let $S = \{ a, b, c \}$. The 2-permutations of S are the ordered arrangements a, b ; a, c ; b, a ; b, c ; c, a and c, b . Consequently, there are six 2-permutations of this set with three elements. To see that there are always six 2-permutations of a set with three elements, note that there are three ways to choose the first element of the arrangement and two ways to choose the second element of the arrangement because it must be different from the first element. By the product rule, it follows that $P(3, 2) = 3 \cdot 2 = 6$.

5.3 Permutations and Combinations

THEOREM 1:

If n is a positive integer and r is an integer with $1 \leq r \leq n$, then there are

$$p(n, r) = n(n-1)(n-2)\cdots(n-r+1)$$

r -permutations of a set with n distinct elements.

Proof: Use the product rule, the first element can be chosen in n ways. There are $n-1$ ways to choose the 2nd element. Likewise, there are $n-2$ ways to choose 3rd element, and so on until there are exactly $n-(r-1)=n-r+1$ ways to choose the r -th element. Thus, there are $n \cdot (n-1) \cdot (n-2) \cdots (n-r+1)$ r -permutations of the set

- ❖ Note that $p(n,0)=1$ whenever n is a nonnegative integer as there is exactly one way to order zero element.

 **Corollary 1:** If n and r are integers with $0 \leq r \leq n$, then $P(n,r) = \frac{n!}{(n-r)!}$

Proof: When n and r are integers with $1 \leq r \leq n$, by Theorem 1 we have


$$P(n,r) = n(n-1)\cdots(n-r+1) = \frac{n!}{(n-r)!}$$

As $\frac{n!}{(n-0)!} = \frac{n!}{(n)!} = 1$ when n is a nonnegative integer, we have


$$P(n,r) = \frac{n!}{(n-r)!} \text{ also holds when } r=0$$

- ❖ By Theorem 1, we know that if n is a positive integer, then $P(n,n)=n!$

5.3 Permutations and Combinations

 **EXAMPLE 4:** How many ways are there to select a first-prize winner, a second-prize winner, and a third-prize winner from 100 different people who have entered a contest?

Solution: Because it matters which person wins which prize, the number of ways to pick the three prize winners is the number of ordered selections of three elements from a set of 100 elements, that is, the number of 3-permutations of a set of 100 elements. Consequently, the answer is $P(100, 3) = 100 \cdot 99 \cdot 98 = 970,200$.

 **EXAMPLE 5:** Suppose that there are eight runners in a race. The winner receives a gold medal, the second place finisher receives a silver medal, and the third-place finisher receives a bronze medal. How many different ways are there to award these medals, if all possible outcomes of the race can occur and there are no ties?

Solution: The number of different ways to award the medals is the number of 3-permutations of a set with eight elements. Hence, there are $P(8, 3) = 8 \cdot 7 \cdot 6 = 336$ possible ways to award the medals.

5.3 Permutations and Combinations

Combinations

✚ **EXAMPLE 8:** How many different committees of three students can be formed from a group of four students?

Solution:

- ✓ We need only find the number of subsets with three elements from the set containing the four students.
- ✓ We see that there are four such subsets, one for each of the four students, because choosing four students is the same as choosing one of the four students to leave out of the group.
- ✓ This means that there are four ways to choose the three students for the committee, where the order in which these students are chosen does not matter.

✚ An ***r-combination*** of elements of a set is an unordered selection of r elements from the set.

✚ An r -combination is simply a subset of the set with r elements.

✚ Denote by $C(n,r)$. Note that $C(n,r)$ is also denoted by $\binom{n}{r}$ and is called a binomial coefficient.

5.3 Permutations and Combinations

✚ **Example 9:** Let S be the set $\{1, 2, 3, 4\}$. Then $\{1, 3, 4\}$ is a 3-combination from S .

✚ **Example 10:** We see that $C(4, 2) = 6$, because the 2-combinations of $\{a, b, c, d\}$ are the six subsets $\{a, b\}$, $\{a, c\}$, $\{a, d\}$, $\{b, c\}$, $\{b, d\}$, and $\{c, d\}$.

✚ **r-combination:**

- ✓ We can determine the number of r -combinations of a set with n elements using the formula for the number of r -permutations of a set
- ✓ Note that the r -permutations of a set can be obtained by first forming r -combinations and then ordering the elements in these combinations

✓ **THEOREM 2:**

The number of r -combinations of a set with n elements, where n is a nonnegative integer and r is an integer with $0 \leq r \leq n$ equals

$$C(n, r) = \frac{n!}{r!(n-r)!}$$

Proof: The r -permutations of the set can be obtained by forming the $C(n, r)$ r -combinations and then ordering the elements in each r -permutation which can be done in $P(r, r)$ ways

$$P(n, r) = C(n, r) * P(r, r).$$

$$\text{This implies that } C(n, r) = \frac{P(n, r)}{P(r, r)} = \frac{n! / (n - r)!}{r! / (r - r)!} = \frac{n!}{r!(n - r)!}$$

5.3 Permutations and Combinations

✓ When computing r-combination

$$C(n, r) = \frac{n!}{r!(n-r)!} = \frac{P(n, r)}{r!} = \frac{n(n-1)\cdots(n-r+1)}{r!}$$

thus canceling out all the terms in the larger factorial

 **Corollary 2:**

Let n and r be nonnegative integers with $r \leq n$. Then $C(n, r) = C(n, n-r)$

Proof:

$$C(n, r) = \frac{n!}{r!(n-r)!}$$

$$C(n, n-r) = \frac{n!}{(n-r)!(n-(n-r))!} = \frac{n!}{(n-r)!r!}$$

 **Combinatorial proof:**

A combinatorial proof of an identity is a proof that uses counting arguments to prove that both sides of the identity count the same objects but in different ways.

Proof: Suppose that S is a set with n elements. Every subset A of S with r elements corresponds to a subset of S with $n - r$ elements, namely \overline{A} . Consequently, $C(n, r) = C(n, n - r)$.