

MCS 256 DISCRETE CALCULUS AND PROBABILITY Set 7
How to Count: Enumerative Combinatorics

Show the form of computation to get each answer. Calculate values of small and moderate numbers. For very large numbers, give approximate answers to four significant digits in scientific notation.

Problems

- (1) In a monoalphabetic substitution cipher, each letter is replaced by another in a one-to-one fashion. For example, the following enciphering table specifies a particular monoalphabetic substitution cipher.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
K	E	Y	W	O	R	D	A	B	C	F	G	H	I	J	L	M	N	P	Q	S	T	U	V	X	Z

It is called *monoalphabetic* because just *one* substitution “alphabet” is used. Here I have followed the usual convention of writing the plaintext in lower case letters, and the ciphertext in upper case.

- (a) How many different monoalphabetic substitution ciphers are possible?
 (b) (EXTRA CREDIT) Some monoalphabetic substitution ciphers never encipher a letter as itself. This is a rule, for example, in newspaper cryptograms. It is not true of the example above, however, because there $z = Z$. What fraction of monoalphabetic substitution ciphers encipher every letter by a different letter? Give an approximate answer that is correct to four decimal places.
- (2) The Enigma machine was an encryption device used by the Germans during World War II. Its main components were a “plugboard” and three different hard-wired rotors. Assuming a 26-letter alphabet, it worked essentially as follows. A letter was entered. It first went through the plugboard, which performed a monoalphabetic substitution of a special type. Then each rotor in turn enciphered the output of the previous stage by one of its 26 possible monoalphabetic substitution ciphers. (All the substitution ciphers of a rotor were circular (mod 26) shifts of one another.) Thus, the input letter would go through four stages of monoalphabetic encipherments. After a letter was enciphered, the rotors would advance odometer-style to a new position, so that the next letter would be enciphered by a different substitution rule. The overall result is a “polyalphabetic” substitution cipher.

- (a) Initially the plugboard had six cables used to interchange pairs of letters. E.g., $A \longleftrightarrow B$, $C \longleftrightarrow E$, $D \longleftrightarrow R$, $F \longleftrightarrow L$, $G \longleftrightarrow I$, $H \longleftrightarrow N$. Thus, the monoalphabetic substitution would be as follows.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	A	E	R	C	L	I	N	G	J	K	F	M	H	O	P	Q	D	S	T	U	V	W	X	Y	Z

Twelve letters are changed; fourteen are not. How many different possible monoalphabetic substitution ciphers are possible with six cables?

- (b) How many different settings of the plugboard and three rotors are possible? Note that the rotors could be permuted as well as rotated.
 (c) Later, to increase security, the Germans changed the plugboard system so that ten cables were used. Thus, 20 letters were changed; 6 were not. They also provided a total of five different rotors, three of which were selected for use on

any given day. How many different possible settings of the components were possible?

- (3) What is the number of nonnegative integer solutions (x_1, \dots, x_n) of the inequality $x_1 + \dots + x_n \leq r$? Here n and r are integers, $n \geq 1$, and $r \geq 0$.
- (4) How many multisets of 5 or fewer elements may be formed from the multiset $\{5 \cdot 1, 5 \cdot 2, 5 \cdot 3, 5 \cdot 4, 5 \cdot 5, 5 \cdot 6, 5 \cdot 7, 5 \cdot 8, 5 \cdot 9\}$?
- (5) How many different orders of at least one and at most five one-scoop cones are possible at an ice cream shop that offers 31 flavors?
- (6) How many ways can you distribute 5 marshmallows to little Joey, Katie, and Zena if each child must get at least one? (Assume the marshmallows are indistinguishable.)
- (7) How many different ways can one distribute a identical articles into b distinct boxes if no boxes are allowed to be empty?
- (8) My laptop keyboard provides me with 92 printable symbols. Assuming that they are all valid for use in a password...
 - (a) How many different passwords of length 6–8 are there in which every symbol is different?
 - (b) How many different passwords of length 6–8 are there if there is no restriction on repeating characters?
 - (c) What fraction of all possible passwords of length 6–8 use letters only?
- (9) How many five-letter strings of upper-case letters are there in which there are at most two A 's, at most one B , and at most three C 's (and any valid number of the other letters)?
- (10) How many different five-card hands can be formed by drawing from a standard deck of 52 cards?
- (11) If five decks are shuffled together, how many different five-card hands can be drawn from these 260 cards?
- (12)
 - (a) How many distinguishable ways are there to assign 5 different tasks to 3 distinct processors?
 - (b) How many distinguishable ways are there to assign 5 identical tasks to 3 distinct processors?
 - (c) How many distinguishable ways are there to assign 5 different tasks to 3 identical processors?
 - (d) (Extra credit) How many distinguishable ways are there to assign 5 identical tasks to 3 identical processors?
 - (e) If six different tasks are assigned at random to three different processors, what is the probability that each processor gets two tasks?

EXTRA CREDIT

- (1) (Flagpole problem; ordered distributions) How many ordered distributions of a distinguishable articles into b distinguishable boxes are there? Equivalently, how many ways can one arrange $f = a$ distinguishable flags on $p = b$ distinct poles. Carefully set forth your reasoning for the general case. It's easy to get bogged down in cases and details, but there is an elegant and short way to count the cases by "stages." Also there is an elegant, super-short answer.
- (2) (Continuation) [1]
 - (a) How many ways can one arrange f *indistinguishable* flags on p distinct poles?
 - (b) Find the ratio of the answers to this problem and the previous problem (general case). Explain the result you get.

REFERENCES

- [1] Marcus, Daniel A., *Combinatorics: A Problem Oriented Approach*, The Mathematical Association of America, Washington, DC, 1998.
- [2] Singh, Simon, *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*, Doubleday, New York, 1999.