4.1 Basic Counting.

A <u>string</u> is simply a finite sequence of symbols from some alphabet.

<u>Ex</u> How many strings of length 2 from the alphabet $\{a, \dots, z\}$ of lower case latin letters are there?

$$26 \left\{ \begin{array}{cccc} \multicolumn{4}{c}{\overbrace{\hspace{4cm}}^{26}} \\ aa & ab & \cdots & az \\ ba & bb & \cdots & bz \\ \vdots & \vdots & & \vdots \\ za & za & \cdots & zz \end{array} \right. \qquad 26 \cdot 26 = 676$$

<u>Product Rule</u>

Suppose a task T can be broken down into two subtasks T_1, T_2 to be performed in succession. Suppose T_1 can be performed in n_1 ways, and when T_1 is complete, T_2 can be performed in n_2 ways. Then T can be performed in $n_1 \cdot n_2$ ways.

More generally suppose T can be broken down into m successive subtasks $T_1, \dots, T_m$, and that after $T_1, \dots, T_{i-1}$ are complete T_i can be performed in n_i ways $(1 \leq i \leq m)$. Then T can be performed in $n_1 \cdot n_2 \cdots n_m$ ways.

Ex How many strings of length 5 from $\{a, \ldots, z\}$ are there?

$$\underset{1}{\underline{26}} \quad \underset{2}{\underline{26}} \quad \underset{3}{\underline{26}} \quad \underset{4}{\underline{26}} \quad \underset{5}{\underline{26}}$$

$26^5 = 11{,}881{,}376$

Ex How many such strings have no repeated letter?

$$\underset{1}{\underline{26}} \quad \underset{2}{\underline{25}} \quad \underset{3}{\underline{24}} \quad \underset{4}{\underline{23}} \quad \underset{5}{\underline{22}}$$

$26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 = 7{,}893{,}600$

Ex How many bit strings of length n are there? (i.e. strings from the alphabet $\{0,1\}$.)

$$\underset{1}{\underline{2}} \quad \underset{2}{\underline{2}} \quad \underset{3}{\underline{2}} \quad \cdots\cdots \quad \underset{n}{\underline{2}}$$

$2 \cdot 2 \cdot 2 \cdots 2 = 2^n$

Ex The number of strings of length n from an alphabet of size m is m^n.

$$\underset{1}{\underline{m}} \quad \underset{2}{\underline{m}} \quad \underset{3}{\underline{m}} \quad \cdots\cdots \quad \underset{n}{\underline{m}}$$

EX. DETERMINE THE NUMBER OF STRINGS OF LENGTH n FROM AN ALPHABET OF SIZE m, IN WHICH NO SYMBOL IS REPEATED.

$$\underset{1}{\underline{m}} \quad \underset{2}{\underline{m-1}} \quad \underset{3}{\underline{m-2}} \quad , \ldots , \quad \underline{m-n+1}$$

$$m(m-1)(m-2)\ldots(m-n+1) = \frac{m!}{(m-n)!}$$

THEOREM

IF A, B ARE FINITE SETS, THEN SO IS $A \times B$, AND $|A \times B| = |A| \cdot |B|$

PROOF

TO FORM AN ORDERED PAIR $(x,y) \in A \times B$ ONE FIRST CHOOSES $x \in A$ IN ONE OF $|A|$ WAYS, THEN CHOOSES $y \in B$ IN ANY OF $|B|$ WAYS. ///

THEOREM

IF S IS A FINITE SET THEN SO IS $\mathbb{P}(S)$ AND $|\mathbb{P}(S)| = 2^{|S|}$.

PROOF:

THE TASK OF CONSTRUCTING A SUBSET $A \subseteq S$ BREAKS NATURALLY INTO $|S|$ SUBTASKS: FOR EACH $x \in S$, DECIDE WHETHER OR NOT $x \in A$. SINCE EACH SUBTASK CAN BE

PERFORMED IN 2 WAYS ($x \in A$ OR $x \notin A$), THERE ARE

$$\underbrace{2 \cdot 2 \cdot 2 \cdot \cdots \cdot 2}_{|S|} = 2^{|S|}$$

WAYS TO CONSTRUCT $A \subseteq S$. THUS THERE ARE $2^{|S|}$ SUBSETS OF S. ///.

<u>REMARK</u>: SUPPOSE $|S| = n$, SAY $S = \{x_1, x_2, \ldots, x_n\}$. THEN THERE IS A BIJECTION

$$f : \mathbb{P}(S) \to \{\text{BIT STRINGS OF LENGTH } n\}$$

DEFINED AS FOLLOWS: FOR $A \subseteq S$, LET $f(A)$ BE THE BIT STRING WHOSE i^{TH} BIT IS 1 IFF $x_i \in A$.

<u>EX.</u> $S = \{1, 2, 3\}$, $\mathbb{P}(S) = \{\phi, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, S\}$

$f(\phi) = 000$	$f(\{1,2\}) = 110$
$f(\{1\}) = 100$	$f(\{1,3\}) = 101$
$f(\{2\}) = 010$	$f(\{2,3\}) = 011$
$f(\{3\}) = 001$	$f(S) = 111$

DEFN

LET A, B BE SETS. WE DENOTE BY B^A THE SET OF FUNCTIONS WITH DOMAIN A AND CODOMAIN B.

$$B^A = \{ f : A \to B \}$$

THEOREM

IF A, B ARE FINITE SETS, THEN SO IS B^A, AND

$$|B^A| = |B|^{|A|}$$

PROOF:

SUPPOSE $|A| = m$ AND $|B| = n$. THE TASK OF CONSTRUCTING A FUNCTION $f : A \to B$ BREAKS INTO m SUCCESSIVE SUBTASKS: FOR EACH $x \in A$ CHOOSE ONE OF THE n ELEMENTS IN B AS $f(x)$. SINCE THERE ARE m SUBTASKS, EACH WITH ALTERNATIVES, THE PRODUCT RULE SAYS THERE ARE

$$\underbrace{n \cdot n \cdot n \cdots n}_{m} = n^m$$

WAYS TO CONSTRUCT SUCH A FUNCTION. HENCE $|B^A| = n^m$ AS REQUIRED. ///

EX. HOW MANY FUNCTIONS $f: A \to B$ ARE INJECTIVE?

LET $|A| = m$, $|B| = n$ AS BEFORE, AND SUPPOSE $A = \{x_1, \ldots, x_m\}$. NOTE THAT IF $n < m$ THERE ARE NO INJECTIVE FUNCTIONS. IF $n \geq m$ THE TASK OF CONSTRUCTING AN INJECTIVE FUNCTION $f: A \to B$ BREAKS INTO m SUBTASKS:

choose $f(x_1) \in B$: n WAYS
choose $f(x_2) \in B$: $(n-1)$ WAYS
choose $f(x_3) \in B$: $(n-2)$ WAYS
$\vdots$
choose $f(x_m) \in B$: $(n-m+1)$ WAYS

THUS, THE NUMBER OF INJECTIVE FUNCTIONS IN B^A IN THIS CASE IS:

$$n \cdot (n-1) \cdot (n-2) \cdots (n-m+1) = \frac{n!}{(n-m)!}$$

IN GENERAL THE NUMBER OF INJECTIVE FUNCTIONS FROM A TO B IS:

$$\begin{cases} 0 & \text{IF } n < m \\ \dfrac{n!}{(n-m)!} & \text{IF } n \geq m \end{cases}$$

SUM RULE

SUPPOSE A TASK T CAN BE PERFORMED BY ONE OF TWO SUBTASKS T_1 OR T_2, BUT NOT BOTH. SUPPOSE T_1 CAN BE PERFORMED IN n_1 WAYS, AND T_2 IN n_2 WAYS. THEN T CAN BE PERFORMED IN n_1+n_2 WAYS.

STATED IN TERMS OF SETS, THE SUM RULE SAYS THAT IF A, B ARE FINITE SETS WITH $A \cap B = \emptyset$, THEN

$$|A \cup B| = |A| + |B|.$$

MORE GENERALLY IF T CAN BE PERFORMED BY DOING EXACTLY ONE OF THE SUBTASKS $T_1, \ldots, T_m$, AND T_i CAN BE DONE IN n_i WAYS $(1 \le i \le m)$, THEN T CAN BE PERFORMED IN $n_1+n_2+\cdots+n_m$ WAYS.

IN TERMS OF SETS WE WOULD SAY THAT IF $A_1, \ldots, A_m$ ARE PAIRWISE DISJOINT (i.e. $A_i \cap A_j = \emptyset$ FOR $i \neq j$) THEN

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = |A_1| + |A_2| + \cdots + |A_m|.$$

Ex. How many strings of length at most 5 can be formed from an alphabet of size 12? (Include the empty string.)

We have 6 subtasks:

- Form all strings of length 5: 12^5 ways
- " " " " " 4: 12^4 ways
- .... 3: 12^3 ways
- .... 2: 12^2 ways
- .... 1: 12^1 ways
- .... 0: 12^0 ways.

By the sum rule there are

$$12^0 + 12^1 + 12^2 + 12^3 + 12^4 + 12^5 = \frac{12^6 - 1}{12 - 1} = 271,453$$

strings of length at most 5.

Ex. A computer system uses passwords consisting of 6 to 8 characters which are either upper or lower case alphabetic (52) or digits (10) subject to the following constraints: A password must contain at least 1 digit and at least 1 alphabetic character. How many valid passwords are there?

LET P BE THE NUMBER OF SUCH PASSWORDS, AND P_i BE THE NUMBER OF PASSWORDS OF LENGTH i $(i=6,7,8)$. THEN $P = P_6 + P_7 + P_8$ BY THE SUM RULE, AND

$$P_6 = 62^6 - 52^6 - 10^6 \approx (3.7)\cdot 10^{10}$$
$$P_7 = 62^7 - 52^7 - 10^7 \approx (1.0)\cdot 10^{12}$$
$$P_8 = 62^8 - 52^8 - 10^8 \approx (1.6)\cdot 10^{14}$$

$\therefore P \approx (1.61037)\cdot 10^{14} \approx 161$ TRILLION

PRINCIPLE OF INCLUSION-EXCLUSION (PIE)

RECALL THAT IF A, B ARE FINITE SETS, NOT NECESSARILY DISJOINT, THEN

$$|A \cup B| = |A| + |B| - |A \cap B|$$

EX. HOW MANY BIT STRINGS OF LENGTH 7 EITHER BEGIN WITH 2 0'S OR END WITH 3 1'S ?

LET $A = \{00xxxxx\}$, $B = \{xxxx111\}$. THEN $A \cap B = \{00xx111\}$ AND

$$|A \cup B| = 2^5 + 2^4 - 2^2 = 44$$

RECALL THE <u>EULER TOTIENT FUNCTION</u> $\phi(n)$ IS DEFINED TO BE THE NUMBER OF NUMBERS IN $\{1, 2, \ldots, n\}$ WHICH ARE RELATIVELY PRIME TO n.

<u>EX.</u> DETERMINE $\phi(1000)$ (NOTE THIS WAS AN EARLIER HW ASSIGNMENT.)

$$\phi(1000) = 1000 - (\text{\# OF \#'s } \underline{\text{NOT}} \text{ REL. PRM. TO } 1000)$$

A NUMBER IS NOT RELATIVELY PRIME TO 1000 IFF IT HAS A FACTOR IN COMMON WITH $1000 = 2^3 \cdot 5^3$, i.e. DIVISIBLE BY 2 OR 5.

$$(\text{\# OF \#'s DIVISIBLE BY } 2) = \frac{1000}{2} = 500$$
$$(\text{\# OF \#'s DIVISIBLE BY } 5) = \frac{1000}{5} = 200$$
$$(\text{\# OF \#'s DIVISIBLE BY BOTH}) = \frac{1000}{2 \cdot 5} = \frac{1000}{10} = 100$$

$$\therefore \phi(1000) = 1000 - (500 + 200 - 100) = 400$$

<u>GENERALIZATIONS OF PIE</u>:

$$|A_1 \cup A_2 \cup A_3| = (|A_1| + |A_2| + |A_3|)$$
$$- (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|)$$
$$+ |A_1 \cap A_2 \cap A_3|$$

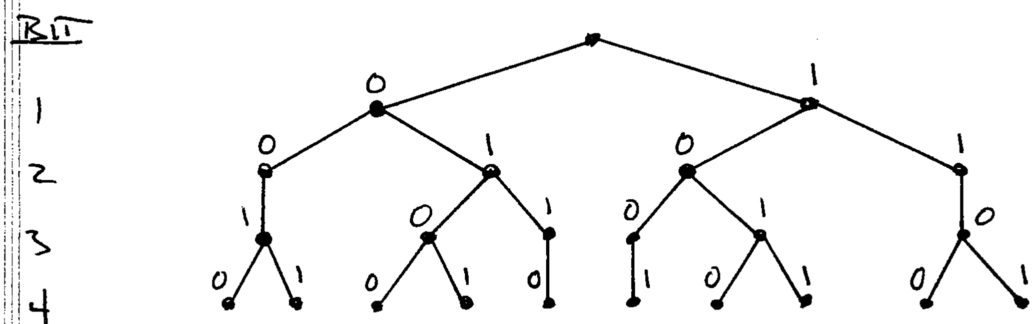
$$\left|\bigcup_{i=1}^{4} A_i\right| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - |A_1 \cap A_2 \cap A_3 \cap A_4|$$

$\vdots$

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \sum_{i<j<k<l} |A_i \cap A_j \cap A_k \cap A_l| + \cdots\cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n| .$$

TREE DIAGRAMS

EX. HOW MANY BIT STRINGS OF LENGTH 4 CONTAIN NEITHER 3 CONSECUTIVE 0'S NOR 3 CONSECUTIVE 1'S ?



STRINGS:

0	0	0	0	0	1	1	1	1	1
0	0	1	1	1	0	0	0	1	1
1	1	0	0	1	0	1	1	0	0
0	1	0	1	0	1	0	1	0	1

$\therefore$ THERE ARE 10 SUCH STRINGS.