May 16, 2021

Algebra.

Elements of Set Theory.

Inclusion-exclusion principle.

The inclusion-exclusion principle generalizes the familiar method of obtaining the number of elements in the union of two finite sets. For two sets, it is symbolically expressed as,

$$|A+B| = |A| + |B| - |AB|$$

where $|A|$, in general, denotes the cardinality, or cardinal number of the set A. The cardinal number extends the concept of the number of elements in a set to infinite sets. In formal set theory, it is defined in such a way that any method of counting sets using it gives the same result. For finite sets it is simply identified with the number of elements in a set, $|A| = n(A)$.

For three sets,

$$|A+B+C| = |A| + |B| + |C| - |AB| - |BC| - |AC| + |ABC|$$

This can be obtained by successive application of the rule for two sets and using the rules of the set algebra, in particular, using $(AC)(BC) = ABC$,

$$|A+B+C| = |(A+B)+C| = |(A+B)| + |C| - |(A+B)C| = |A| + |B| - |AB| - |AC+BC| = |A| + |B| - |AB| - |AC| - |BC| + |(AC)(BC)|.$$

And, in general, for n sets,

$$\left|\sum_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1\le i\le j\le n}^{n} |A_i A_j| + \sum_{1\le i\le j\le k\le n}^{n} |A_i A_j A_k| \dots + (-1)^{n-1}|A_1 \dots A_n|$$

The summation signs with indices denote adding intersections of all possible selections of pairs, triplets, quadruplets, and so on, of sets in the set of sets $\{A_n\}$. This appears as a complicated expression. Some insight into its meaning can be obtained by considering how many times elements belonging to an intersection of these n sets, $X = A_1 A_2 \dots A_n = A_1 \cap A_2 \cap \dots \cap A_n$, are counted.

The intersection set X belongs to each set $A_k, 1 \le k \le n$, and therefore the first sum adds it n times. The set X also belongs to all pairwise intersections. There are $\binom{n}{2} = \frac{n!}{2!(n-2)!}$ possible pair selections (= terms in the second sum), and therefore the second sum subtracts the number of elements in X, $\binom{n}{2}$ times. The third sum adds these elements $\binom{n}{3}$ times, and so on. As a result, X is counted $\binom{n}{1} - \binom{n}{2} + \binom{n}{3} - \cdots + (-1)^n \binom{n}{n}$ times, i.e. only once, as expected.

Exercise. Show that $\binom{n}{1} - \binom{n}{2} + \binom{n}{3} - \cdots + (-1)^n \binom{n}{n} = 1$.

In applications, it is often useful to write the inclusion-exclusion principle expressed in its complementary form. That is, counting the number of elements complementing a union of sets to a finite universal set I containing all of A_i. Applying rules of set algebra and De Morgan's laws to sets we have,

$$|I| - \left|\sum_{i=1}^{n} A_i\right| = \left|\left(\sum_{i=1}^{n} A_i\right)'\right| = \left|\bigcap_{i=1}^{n} A_i'\right| \equiv \left|\prod_{i=1}^{n} A_i'\right| =$$

$$|I| - \sum_{i=1}^{n} |A_i| + \sum_{1 \le i \le j \le n}^{n} |A_i A_j| - \sum_{1 \le i \le j \le k \le n}^{n} |A_i A_j A_k| \ldots + (-1)^n |A_1 \ldots A_n|$$

Thus obtained inclusion-exclusion principle can be proven by mathematical induction.

Theorem. $\forall n$,

$$\left|\sum_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i \le j \le n}^{n} |A_i A_j| + \sum_{1 \le i \le j \le k \le n}^{n} |A_i A_j A_k| \ldots + (-1)^{n-1} |A_1 \ldots A_n|$$

Proof (Mathematical Induction).

(1) <u>Base case</u>. $|A_1| = |A_1|$, $|A_1 + A_2| = |A_1| + |A_2| - |A_1 A_2|$.
(2) <u>Induction step</u>. Assume the above is true for n. Then, for $n + 1$,

$$\left|\sum_{i=1}^{n+1} A_i\right| = \left|\left(\sum_{i=1}^{n} A_i\right) + A_{n+1}\right| = \left|\sum_{i=1}^{n} A_i\right| + |A_{n+1}| - \left|\sum_{i=1}^{n} A_i A_{n+1}\right|$$

$$= \sum_{i=1}^{n+1} |A_i| - \sum_{1\le i\le j\le n}^{n} |A_i A_j| + \sum_{1\le i\le j\le k\le n}^{n} |A_i A_j A_k| - \cdots$$

$$+ (-1)^{n-1}|A_1 \dots A_n| - \sum_{1\le i\le n}^{n} |A_i A_{n+1}| + \sum_{1\le i\le j\le n}^{n} |A_i A_j A_{n+1}| - \cdots$$

$$+ (-1)^n |A_1 \dots A_{n+1}| =$$

$$= \sum_{i=1}^{n+1} |A_i| - \sum_{1\le i\le j\le n+1}^{n+1} |A_i A_j| + \sum_{1\le i\le j\le k\le n+1}^{n+1} |A_i A_j A_k| - \cdots + (-1)^n |A_1 \dots A_{n+1}|$$

Example. How many natural numbers $n \le 100$ are not divisible by 3, 4, or 5? For $n \le 100$, there are 33 numbers divisible by 3, $|A_3| = 33$, 25 divisible by 4, $|A_4| = 25$, 20 divisible by 5, $|A_5| = 20$. Also, there are 8 numbers divisible by 3·4=12, 6 divisible by 3·5=15, 5 divisible by 4·5=20, and 1 divisible by 3·4·5=60. Hence, the answer is $100 - |A_3 + A_4 + A_5| = 100 - (33 + 25 + 20 - 8 - 6 - 5 + 1) = 40$.

<u>**Application to the theory of probability**</u>.

The set of all possible outcomes of an experiment can be denoted by I, while the subset of particular "favorable" outcomes of interest we denote $A \subset I$. Then, the probability of a favorable outcome is given by the ratio of the number of elements in the set A, $n(A)$, to the number all possible outcomes, i.e. the number of elements in the set I, $n(I)$, where $n(A) \le n(I)$,

$$P(A) = \frac{n(A)}{n(I)}$$

For example, if A is the set of spades in the deck of 52 cards, then the probability of drawing a spade from the well-shuffled deck is $P = \frac{n(spades)}{n(cards\ in\ the\ deck)} = \frac{13}{52} = \frac{1}{4}$.

Using the algebra of sets can facilitate calculating the probabilities when the probabilities of certain outcomes are known, and the probability of other set of outcomes is required. For example, knowing $P(A)$, $P(B)$ and $P(AB)$ allows calculating

$P(A+B) = P(A) + P(B) - P(AB)$.

Similarly, for three subsets, A, B, C, we obtain,

$P(A+B+C) = P(A) + P(B) + P(C) - P(AB) - P(BC) - P(AC) + P(ABC)$.

Exercise. Three digits, 1, 2, 3, are written down in random order. What is the probability that at least one digit will occupy its place? What is the probability for four digits? Five? What is the probability for n digits?

<u>**Arrangements and Derangements**</u>.

Arrangements of a subset of k distinct objects chosen from a set of n distinct objects are $A_n^k = \frac{n!}{(n-k)!}$ permutations [order matters] of distinct subsets of k elements chosen from that set. The total **number of arrangements** of any subset of a set of n distinct objects is the number of unique sequences [order matters] that can be formed from any subset of $0 \leq k \leq n$ objects of the set,

$$a_n = \sum_{k=0}^{n} A_n^k = \sum_{k=0}^{n} k! \binom{n}{k} = \sum_{k=0}^{n} \frac{n!}{(n-k)!} = n! \sum_{k=0}^{n} \frac{1}{k!} \equiv ¡n$$

This number is obviously larger than the number of permutations of n distinct objects given by $n!$. Hence, a supfactorial, $¡n$, notation has been suggested. It is easy to check that $¡n$ satisfies the following recurrence relation,

$$¡n = n \cdot ¡(n-1) + 1$$

For very large $n \gg 1$, the supfactorial is nearly a constant times the factorial, $¡n \approx e \cdot n!$

Exercise. How many possible passwords can be composed using an alphabet of $n = 26$ letters, if a password is required to have at least 8 characters and have no repeating characters? Answer: $a_{26} - a_7 = 26! \sum_{k=8}^{26} \frac{1}{k!}$.

A (complete) **derangement** is a permutation of the elements of a set of distinct elements such that none of the elements appear in their original position. The number of derangements of a set of n distinct objects, i. e. the number of permutations with no rencontres, or the number of permutations of n distinct objects with no fixed point, is called the subfactorial, $!\,n$. It can be obtained by using the inclusion-exclusion principle. The universal set of permutations P has $n!$ elements. Denote P_1 the subset of permutations that keep element 1 in its place, P_2 those that keep element 2 in its place, P_k that keep element k in its place, and so on. The set of permutations that keep at least 1 element in its original place is then, $P_{>1} = P_1 \cup P_2 \cup P_3 \dots \cup P_n$. The number of derangement is given by the number of elements complementing this set to P,

$$d_n = |P| - \left|\sum_{i=1}^{n} P_i\right| =$$

$$n! - \sum_{i=1}^{n} |P_i| + \sum_{1 \le i \le j \le n}^{n} |P_i P_j| - \sum_{1 \le i \le j \le k \le n}^{n} |P_i P_j P_k| \dots + (-1)^n |P_1 \dots P_n|$$

Using the fact that $|P_i|, |P_i P_j|, |P_i P_j P_l|, \dots$ are equal to $(n-1)!, (n-2)!, (n-3)!, \dots$, correspondingly, for every choice of $i, \{i, j\}, \{i, j, l\}, \dots$ and there are $\binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \dots \binom{n}{k}, \dots$ such choices, respectively, we obtain,

$$d_n = n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \dots + (-1)^n \binom{n}{n} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \equiv\, !\,n$$

The number of derangements also obeys the following recursion relations,

$d_n = n \cdot d_{n-1} + (-1)^n$, or, $!\,n = n \cdot !\,(n-1) + (-1)^n$, and,

$d_n = (n-1) \cdot (d_{n-1} + d_{n-2})$, or, $!\,n = (n-1) \cdot \big(!\,(n-1) + !\,(n-2)\big)$.

Note that the latter recursion formula also holds for $n!$; for very large $n \gg 1$, the subfactorial is nearly a factorial divided by a constant, $!\,n \approx \frac{n!}{e}$. Starting with $n = 0$, the numbers of derangements of a set of n elements are,

1, 0, 1, 2, 9, 44, 265, 1854, 14833, 133496, 1334961, 14684570, 176214841, 2290792932, …

Exercise. A group of n men enter a restaurant and check their hats. The hat-checker is absent minded, and upon leaving, redistributes the hats back to the men at random. What is the probability, P_n, that no man gets his correct hat?

This is the old hats problem, which goes by many names. It was originally proposed by French mathematician P. R. de Montmort in 1708, and solved by him in 1713. At about the same time it was also solved by Nicholas Bernoulli using inclusion-exclusion principle.

An alternative solution is to devise a recurrence by noting that for a full derangement, every of n men should get somebody else's hat. Assume man x got the hat of man y. In the case that man y got the hat of man x, there are d_{n-2} such possible derangements. However, we also have to account for the possibility that man y, whose hat went to man x, did not get "his" hat of man x in return. This gets us to the situation of the full derangement for $n-1$ men. Adding the two possibilities and multiplying with $n-1$ possible choices of man y we obtain, $d_n = (n-1)(d_{n-1} + d_{n-2})$, or, $P_n = \left(\frac{n-1}{n} P_{n-1} + \frac{1}{n} P_{n-2}\right)$, wherefrom the above expression for the derangement can be derived.

If some, but not necessarily all, of the items are not in their original ordered positions, the configuration can be referred to as a partial derangement. The number of partial derangements with k fixed points (rencontres) is,

$$d_{n,k} = \binom{n}{k} d_{n-k} = \binom{n}{k} \sum_{p=0}^{k} \frac{(-1)^p}{p!}$$

Here is the beginning of this array.

n/k	0	1	2	3	4	5	6	7
0	1							
1	0	1						
2	1	0	1					
3	2	3	0	1				
4	9	8	6	0	1			
5	44	45	20	10	0	1		
6	265	264	135	40	15	0	1	
7	1854	1855	924	315	70	21	0	1