The power set of a set

Definition

Let S be a set. The power set (or powerset) of S, denoted $\mathcal{P}(S)$, is the set of *all* subsets of S.

Example

- $\mathcal{P}(\emptyset) = \{\emptyset\}$
- For any non-empty S, $\mathcal{P}(S)$ contains at least two elements: $\emptyset$ and S.
- $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$
- $\mathcal{P}(\{x, y\}) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$
- $\mathcal{P}(\{x, y, z\}) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}$

Theorem

Let S be a set. Then $|\mathcal{P}(S)| = 2^{|S|}$

Proof.

Let $\mathrm{Map}(S,\{0,1\})$ be the set of maps from S to $\{0,1\}$. Since $|\mathrm{Map}(S,\{0,1\})| = 2^{|S|}$ (for S finite this can be proven; for S infinite this is the definition of $2^{|S|}$) the idea is to prove that $|\mathcal{P}(S)| = |\mathrm{Map}(S,\{0,1\})|$.

Define $g : \mathrm{Map}(S,\{0,1\}) \to \mathcal{P}(S)$ by $g(f) = \{s \in S \,:\, f(s) = 1\}$ where f is a map $S \to \{0,1\}$.

Define $h : \mathcal{P}(S) \to \mathrm{Map}(S,\{0,1\})$ by $h(Y) = \chi_Y$, $Y \in \mathcal{P}(S)$ where χ_Y is the *characteristic map* (or the *indicator function*) of Y:

$$\chi_Y(s) = \begin{cases} 1, & s \in Y \\ 0, & s \notin Y \end{cases}$$

Thus, $Y = \{s \in S \,:\, \chi_Y(s) = 1\}$.

We claim that $g \circ h = \mathrm{id}_{\mathcal{P}(S)}$ and $h \circ g = \mathrm{id}_{\mathrm{Map}(S,\{0,1\})}$. Then g, h are both bijective and so $|\mathrm{Map}(S,\{0,1\})| = |\mathcal{P}(S)|$.

Proof (contd.)

Let $Y \in \mathcal{P}(S)$ (that is, $Y \subset S$). Then

$$\begin{aligned}(g \circ h)(Y) &= g(h(Y))\\ &= \{s \in S : h(Y)(s) = 1\}\\ &= \{s \in S : \chi_Y(s) = 1\}\\ &= \{s \in S : s \in Y\}\\ &= Y\end{aligned}$$

Thus, $g \circ h = \mathrm{id}_{\mathcal{P}(S)}$.

Proof (contd.)

Let $f \in \mathrm{Map}(S, \{0,1\})$. We want to show that $(h \circ g)(f) = f$. That is, we want to show that for all $s \in S$, $((h \circ g)(f))(s) = f(s)$. We have

$$\begin{aligned}((h \circ g)(f))(s) &= (h(g(f)))(s) \\ &= \chi_{g(f)}(s) \\ &= \begin{cases} 1, & s \in g(f) \\ 0, & s \notin g(f) \end{cases} \\ &= \begin{cases} 1, & f(s) = 1 \\ 0, & f(s) = 0 \end{cases} \\ &= f(s).\end{aligned}$$

Thus, $h \circ g = \mathrm{id}_{\mathrm{Map}(S,\{0,1\})}$. We proved that g and h are inverses of each other. $\square$

If S is a countable set then we can think of $\mathcal{P}(S)$ as the set of bit strings.

If S is finite, then we only need to consider bit strings of length $|S|$.

Indeed, number each element of S as $s_0, s_1, s_2, s_3, \ldots$. Then $f : S \to \{0, 1\}$ is uniquely determined by the sequence $a_0, a_1, a_2, \ldots$ where $a_i = f(s_i)$.

Identifying f with the corresponding subset of S as in the proof of our previous theorem, we can think of a bit string as a subset of S. Thus, $a_i = 1$ if $s_i \in X$ and $a_i = 0$ if $s_i \notin X$.

One advantage is that we can implement set operations on subsets of S using bitwise logical operations.

Example

Let $S = \{1, 2, \ldots, 16\}$, $X = \{1, 3, 5, 6, 7, 9, 11, 12\}$, $Y = \{2, 3, 9, 10, 11, 13\}$. Find $X \cap Y$, $X \cup Y$, $X \triangle Y$, $X \setminus Y$.

X corresponds to the bit string 1010111010110000 and Y corresponds to the bit string 0110000011101000. Then $X \cap Y$ corresponds to $1010111010110000 \wedge 0110000011101000 = 0010000010100000$ which is $\{3, 9, 11\}$,

$X \cup Y$ corresponds to $1010111010110000 \vee 0110000011101000 = 1110111011111000$ which is $\{1, 2, 3, 5, 6, 7, 9, 10, 11, 12, 13\}$,

$X \triangle Y$ corresponds to $1010111010110000 \oplus 0110000011101000 = 1100111001010000$ which gives $\{1, 2, 5, 6, 7, 10, 12\}$.

Finally, $X \setminus Y$ corresponds to $1010111010110000 \wedge \overline{0110000011101000} = 1010111010110000 \wedge 1001111100010111 = 1000111000010000$ which is $\{1, 5, 6, 7, 12\}$.

This technique can be used to program set operations. For example, to check that X is a subset of Y we represent both by bit strings and perform $\wedge$. If the result is equal to X (which is easily checked) then $X \subset Y$.

Theorem

Let S be a set and $\mathcal{P}(S)$. Then $|S| < |\mathcal{P}(S)|$. In particular, if S is countable infinite then $\mathcal{P}(S)$ is uncountable.

Corollary

Let n be a positive integer. Then $n < 2^n$.

Proof.

Define $g : S \to \mathcal{P}(S)$ by $g(s) = \{s\}$. This map is manifestly injective and so $|S| \leq |\mathcal{P}(S)|$.
Suppose that $|S| = |\mathcal{P}(S)|$. Then there is a bijection $f : S \to \mathcal{P}(S)$. Let $X = \{s \in S \ : \ s \notin f(s)\}$. Since $X \in \mathcal{P}(S)$ (as a subset of S), it is then equal to $f(s_0)$ for some $s_0 \in S$.
Now, by definition of X, $s_0 \in X$ if and only if $s_0 \notin f(s_0) = X$. This is clearly a contradiction.
We proved that a bijection $f : S \to \mathcal{P}(S)$ does not exist. Thus, $|S| \leq |\mathcal{P}(S)|$ and $|S| \neq |\mathcal{P}(S)|$. Therefore, $|S| < |\mathcal{P}(S)|$. $\square$

Example

In particular, this gives an alternative proof that the set of all *infinite bit strings* is uncountable.
Indeed, the set of all infinite bit strings identifies with $\mathcal{P}(\mathbb{N})$ and it follows from our theorem that $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$.

Counting subsets with a given number of elements.

Example

- How many ways are there to choose k objects from a collection of m indistinguishable objects (number of *combinations*)?
- How many subsets of cardinality k are in the set of m elements?
- What is the number of sequences of integers $1 \leq i_1 < i_2 < \cdots < i_k \leq m$?

Given a set S, denote $\mathcal{P}_k(S) \subset \mathcal{P}(S)$ the set of all subsets of S of cardinality k: $\mathcal{P}_k(S) = \{X \in \mathcal{P}(S) : |X| = k\} = \{X \subset S : |X| = k\}$.

Definition

Let m, k be non-negative integers. Define $\binom{m}{k}$ (reads "m choose k") as $|\mathcal{P}_k(S)|$ where $|S| = m$.

By definition $\binom{m}{k}$ is a non-negative integer.

Some properties of $\binom{m}{k}$

- $\binom{m}{k} = 0$ if $k > m$.
  Indeed, if $|A| = m$, all its subsets have cardinality $\leq m$
- $\binom{m}{0} = 1 = \binom{m}{m}$; $\binom{m}{1} = \binom{m}{m-1} = m$.
- $\binom{m}{k} = \binom{m}{m-k}$, $0 \leq k \leq m$.

Proof.

Consider the map $f : \mathcal{P}(S) \to \mathcal{P}(S)$, $X \mapsto S \setminus X$. Since $S \setminus (S \setminus X) = X$, we have $f \circ f = \mathrm{id}_{\mathcal{P}(S)}$. Thus, f is its own inverse and hence is bijective. Since S is finite, $|f(X)| = |S \setminus X| = m - |X|$. Thus, $f(\mathcal{P}_k(S)) \subset \mathcal{P}_{m-k}(S)$ and $f(\mathcal{P}_{m-k}(S)) \subset \mathcal{P}_k(S)$. Since $f|_{\mathcal{P}_k(S)}$ is injective and $f|_{\mathcal{P}_{m-k}(S)}$ is injective, it follows that $|\mathcal{P}_k(S)| \leq |\mathcal{P}_{m-k}(S)| \leq |\mathcal{P}_k(S)|$. $\square$

- $\binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{m-1} + \binom{m}{m} = \sum_{k=0}^{m} \binom{m}{k} = 2^m$

Proof.

If $|S| = m$ then $\mathcal{P}(S)$ has cardinality 2^m. Since $\mathcal{P}(S) = \bigcup_{0 \leq k \leq m} \mathcal{P}_k(S)$ and $\mathcal{P}_k(S) \cap \mathcal{P}_l(S) = \emptyset$ if $k \neq l$ we have
$2^m = |\mathcal{P}(S)| = |\mathcal{P}_0(S)| + \cdots + |\mathcal{P}_m(S)| = \binom{m}{0} + \cdots + \binom{m}{m}$. $\square$

Theorem (Pascal's rule)

Let $1 \leq k \leq m$. *Then* $\binom{m}{k} = \binom{m-1}{k} + \binom{m-1}{k-1}$.

Proof.

Denote $[r] = \{1, \ldots, r\}$. Let $A = \{X \in \mathcal{P}_k([m]) : m \in X\}$, $B = \{X \in \mathcal{P}_k([m]) : m \notin X\}$.
Clearly, $\mathcal{P}_k([m]) = A \cup B$ and $A \cap B = \emptyset$ so $|\mathcal{P}_k([m])| = |A| + |B|$.
Note that $B = \mathcal{P}_k([m-1])$. Therefore, $|B| = \binom{m-1}{k}$.
To find $|A|$, note that we have a map $g : A \to \mathcal{P}_{k-1}([m-1])$ given by $X \mapsto X \setminus \{m\}$. This map is bijective because the map $h : \mathcal{P}_{k-1}([m-1]) \to A$ defined by $Y \mapsto Y \cup \{m\}$ is easily seen to be its inverse. Thus, $|A| = \binom{m-1}{k-1}$. □

Pascal's triangle

Pascal's rule allows us to compute the $\binom{m}{k}$ recursively.

$m = 0$	1										
$m = 1$	1	1									
$m = 2$	1	2	1								
$m = 3$	1	3	3	1							
$m = 4$	1	4	6	4	1						
$m = 5$	1	5	10	10	5	1					
$m = 6$	1	6	15	20	15	6	1				
$m = 7$	1	7	21	35	35	21	7	1			
$m = 8$	1	8	28	56	70	56	28	8	1		
$m = 9$	1	9	36	84	126	126	84	36	9	1	
$m = 10$	1	10	45	120	210	252	210	120	45	10	1

Binomial identity

Theorem

Suppose that $xy = yx$. *Then for any non-negative integer* n

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

Proof.

We have $(x+y)^n = \sum_{S\subset\{1,\ldots,n\}} a(S)$, where $a(S) = a(S)_1 \cdots a(S)_n$ with $a(S)_i = y$ if $i \in S$ and $a(S)_i = x$ if $i \notin S$. Since, clearly, $a(S) = x^{n-|S|} y^{|S|}$, it follows that

$$(x+y)^n = \sum_{k=0}^{n} |\mathcal{P}_k(\{1,\ldots,n\})| x^{n-k} y^k = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k. \qquad \square$$

Exercise

Use Pascal's rule and induction to prove the binomial identity.

A formula for $\binom{m}{k}$

Theorem

For all $0 \leq k \leq m$ *we have* $\binom{m}{k} = \frac{m(m-1)\cdots(m-k+1)}{k!} = \frac{m!}{k!(m-k)!}$.

Inductive proof.

We use induction on m. For $m = 0$ and $m = 1$ the assertion is clear (we use the convention that an empty product is equal to 1).

For the inductive step, we have

$$\begin{aligned}
\binom{m+1}{k} &= \binom{m}{k} + \binom{m}{k-1} && \text{by Pascal's rule} \\
&= \frac{m!}{k!(m-k)!} + \frac{m!}{(k-1)!(m-k+1)!} && \text{by induction hypothesis} \\
&= \frac{m!}{k!(m-k+1)!}\,(m-k+1) + \frac{m!}{k!(m-k+1)!}\,k \\
&= \frac{m!}{k!(m-k+1)!}(m-k+1+k) \\
&= \frac{(m+1)m!}{k!(m+1-k)!} \\
&= \frac{(m+1)!}{k!(m+1-k)!}
\end{aligned}$$

$\square$

Bijective proof

Here we introduce another useful counting technique.

Theorem

Let A and B be finite sets. Suppose that there exists a surjective map $f : A \to B$ such that $|f^{-1}(\{b\})| = k$ for all $b \in B$. Then $|A| = k|B|$.

Proof.

If $g : A \to B$ is *any* map and $b \neq b' \in B$ then $g^{-1}(\{b\}) \cap g^{-1}(\{b'\}) = \emptyset$.
If $g : A \to B$ is *surjective* then

$$A = \bigcup_{b \in B} g^{-1}(\{b\})$$

and so

$$|A| = \sum_{b \in B} |g^{-1}(\{b\})|.$$

Applying this to our map f we obtain $|A| = \sum_{b \in B} k = k|B|$. $\square$

Bijective proof.

We want to prove that $k!\binom{m}{k} = m(m-1)\cdots(m-k+1)$.
Denote $[r] = \{1, \ldots, r\}$. Let $\mathrm{Inj}([k], [m])$ be the set of all injective maps $[k] \to [m]$.
The right hand side of our equality is $|\,\mathrm{Inj}([k], [m])|$.
The idea is to construct a surjective map $\mathrm{Inj}([k], [m]) \to \mathcal{P}_k([m])$ and to use Theorem from slide *17*.
Define a map $F : \mathrm{Inj}([k], [m]) \to \mathcal{P}([m])$ by $F(f) = \operatorname{im} f = \{f(1), \ldots, f(k)\}$.
Since f is injective, $|\operatorname{im} f| = k$. Thus, F is actually a map $\mathrm{Inj}([k], [m]) \to \mathcal{P}_k([m])$.
We claim that $F : \mathrm{Inj}([k], [m]) \to \mathcal{P}_k([m])$ is surjective. Indeed, let $X = \{i_1, \ldots, i_k\} \in \mathcal{P}_k([m])$. Here we chose a way to enumerate elements of X; for example, we can assume that $i_1 < i_2 < \cdots < i_k$. All the i_r are distinct (otherwise $|X| < k$). Define a map $f_X : [k] \to [m]$ by $f_X(r) = i_r$, $1 \leq r \leq k$. This map is injective and $F(f_X) = X$.

Bijective proof (cont.)

Now we claim that if $X \in \mathcal{P}_k([m])$ then

$$|F^{-1}(\{X\})| = k! \tag{$\star$}$$

Indeed, $F(f) = X$ if and only if f is a permutation of X (that is, a bijective map $[k] \to X$), and there are $k!$ of them.

Example

- How many ways are there to select a soccer team out of twenty candidates (there are eleven players on the team)?
  This is the number of subsets of 11 elements in a set of 20 elements, that is, $\binom{20}{11} = \binom{20}{9} = 167,960$.
- What if we take into account that the team must have a goalkeeper, a captain (who will be a forward), two more forwards and four defenders?
  First we choose the captain (which can be done in 20 ways), then the goalkeeper (there are 19 choices), then two more forwards ($\binom{18}{2}$ ways), then four defenders ($\binom{16}{4}$ ways). We still need to select $11 - 1 - 1 - 2 - 4 = 11 - 8 = 3$ players out of $16 - 4 = 12$ remaining candidates, which gives $\binom{12}{3}$ possibilities. Thus, the total number is $20 \cdot 19 \cdot \binom{18}{2} \cdot \binom{16}{4} \cdot \binom{12}{3} = 23,279,256,000$.

We can also choose two forwards first, in $\binom{20}{2}$ ways, then four defenders, in $\binom{18}{4}$ ways, then the goalkeeper, in 14 ways and the captain, in 13 ways, and then the remaining 3 members of the team, in $\binom{12}{3}$ ways. The total is then $\binom{20}{2} \cdot \binom{18}{4} \cdot 14 \cdot 13 \cdot \binom{12}{3} = 23,279,256,000$ as expected.

Another way to see this: we have 11 positions on the team and 20 candidates who can occupy these positions. If each position was numbered, we would be counting the number of injective maps from P (positions) to C (candidates), which is $20!/(20-11)! = 20!/9!$. However, some of these positions need to be "identified": it does not matter to us in which order forwards or defenders are assigned, the only thing that matters is who is assigned to one of these positions. We have $4!$ permutations of defenders, $2!$ permutations of forwards and $3!$ permutations of the remaining members of the team. So, the answer is $20!/(9!2!3!4!)$. It is then easy to see that both our previous answers are equal to this number.

Example

In how many permutations of the string $ABCDEFGH$ the letters A, C and D appear in this order but not necessarily next to each other?

The positions in which 3 letters A, C and D may occur can be chosen in $\binom{8}{3} = 56$ ways. Once these letters are placed, there are $8 - 3 = 5$ positions left and $5!$ ways to place the remaining 5 letters. So, the answer is $5!\binom{8}{3} = 6720$.

Example

What if A, C and D appear in this order but *NOT* next to each other?

There are $(8 - 3 + 1)! = 6!$ permutations of the original string containing ACD, so the answer is $5!\binom{8}{3} - 6! = 5!(\binom{8}{3} - 6) = 5! \cdot 50 = 6000$. Another way of seeing this is that out of $\binom{8}{3}$ ways of selecting three places for letters A, C and D we are *NOT* interested in those which are adjacent, and there are 6 of them. So, there are $\binom{8}{3} - 6$ places where A, C and D can be put, which should be multiplied by $5!$ permutations of the remaining 5 letters.

Example

What if A, B, C must appear in that order, and also D, E, F?

There are $\binom{8}{3}$ ways of choosing places for A, B and C; once these are chosen, there are $\binom{5}{3}$ ways of choosing places for D, E, F. After these letters are placed, there are $(8-6)=2!$ ways of placing the remaining two letters. So, the answer is $\binom{8}{3}\binom{5}{3}2! = 1120$.

Example

How many bit strings of length 10 contain at most three 1s? At least three 1s?

A bit string of length 10 represents subsets of a set of 10 elements. The number of 1s represents the number of elements in the corresponding subset. So, we are counting the number of subsets of a set of 10 elements containing at most 3 elements, that is $\binom{10}{0} + \binom{10}{1} + \binom{10}{2} + \binom{10}{3}$.

This equals to $1 + 10 + 45 + 120 = 176$.

To answer the second question we count the number of subsets of a set of 10 elements containing at least 3 elements, that is,

$\binom{10}{3} + \binom{10}{4} + \cdots + \binom{10}{10} = 2^{10} - \binom{10}{0} - \binom{10}{1} - \binom{10}{2} = 1024 - 1 - 10 - 45 = 968$.

Question

How many bit strings of length 10 contain more zeros than ones?

If a bit string of length 10 contains more 0s than 1s if it contains at least 6 zeros (or, which is the same, at most 4 ones). So, the answer is $\binom{10}{0}+\binom{10}{1}+\binom{10}{2}+\binom{10}{3}+\binom{10}{4}=386$. Since

$$
\begin{aligned}
2^{10} &= \binom{10}{0}+\binom{10}{1}+\binom{10}{2}+\binom{10}{3}+\binom{10}{4}+\binom{10}{5}+\binom{10}{6}+\binom{10}{7}+\binom{10}{8}+\binom{10}{9}+\binom{10}{10} \\
&= \binom{10}{0}+\binom{10}{10}+\binom{10}{1}+\binom{10}{9}+\binom{10}{2}+\binom{10}{8}+\binom{10}{3}+\binom{10}{7}+\binom{10}{4}+\binom{10}{6}+\binom{10}{5} \\
&= 2\binom{10}{0}+2\binom{10}{1}+2\binom{10}{2}+2\binom{10}{3}+2\binom{10}{4}+\binom{10}{5}
\end{aligned}
$$

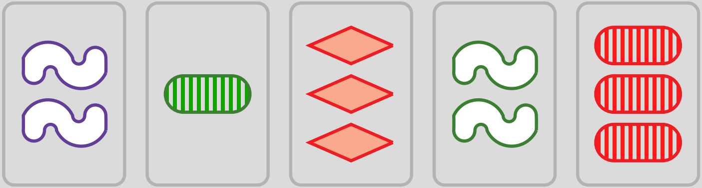
So

$$
\begin{aligned}
\binom{10}{0}+\binom{10}{1}+\binom{10}{2}+\binom{10}{3}+\binom{10}{4} &= 2^9-\frac{1}{2}\binom{10}{5} \\
&= 2^9-\frac{10\cdot 9\cdot 8\cdot 7\cdot 6}{2\cdot 2\cdot 3\cdot 4\cdot 5} = 2^9-\frac{9\cdot 8\cdot 7\cdot 6}{4!} = 2^9-\binom{9}{4}.
\end{aligned}
$$

Example (The game of Set)

Each card has 4 attributes:

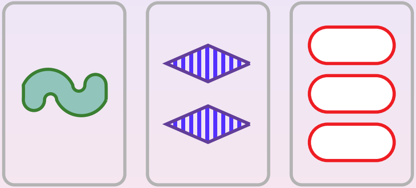
- Number of shapes on the card (1,2,3)
- The color of shapes on the card (red, green, purple)
- Shape (oval, diamond, squiggle)
- Shading (plain, striped, solid)

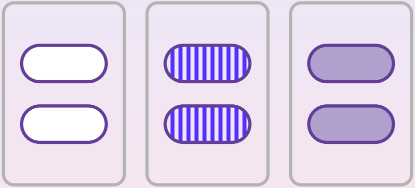


So, if $N = \{1, 2, 3\}$, $C = \{\text{red}, \text{green}, \text{purple}\}$, $S = \{\text{oval}, \text{diamond}, \text{squiggle}\}$ and $F = \{\text{plain}, \text{striped}, \text{solid}\}$ then each card can be represented as an element of $N \times C \times S \times F$.
Alternatively, we can think of each card as an element of $\{0, 1, 2\}^4$ (each attribute has 3 possible values, encoded by 0, 1 and 2.

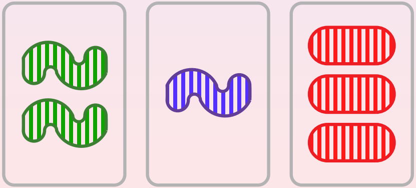
A SET is a collection of 3 cards, (a_1, a_2, a_3, a_4), (b_1, b_2, b_3, b_4) and (c_1, c_2, c_3, c_4) such that for each $1 \leq i \leq 4$, either $a_i = b_i = c_i$ or $a_i \neq b_i \neq c_i$ (that is, each attribute must have the same value in all three cards, or different values in all three cards)

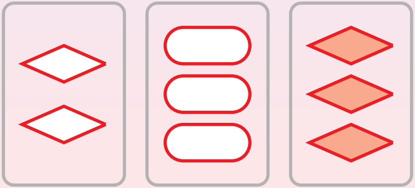
For example, the following two collections of 3 cards are SETs:





And the following two are not:





Question

What is the probability that 3 cards selected randomly form a SET?

- How many cards are there in the deck?
  Each card has 4 properties, each property can take 3 values, so the total number is the cardinality of $\{0,1,2\}^4$, that is $3^4 = 81$.
- How many ways are there to choose 3 cards from the deck?
  We are looking for the number of subsets of 3 elements in a set of 81 elements. This number is $\binom{81}{3} = 81 \cdot 80 \cdot 70/3! = 85\,320$.
- How many SETs (in the sense of the game) are there in the deck?
  Recall that once two cards X, Y are chosen, there is a unique card Z such that $\{X, Y, Z\}$ is a SET. Two cards can be selected in $\binom{81}{2}$ ways. However, this is not the end of the story: the same set $\{X, Y, Z\}$ is obtained in 3 different ways (from the pairs $\{X, Y\}$, $\{X, Z\}$ and $\{Y, Z\}$). So, the number of SETs is $\frac{1}{3}\binom{81}{2} = 81 \cdot 80/(3 \cdot 2) = 1,080$.

Answer.

We divide the number of desirable outcomes by the total number of outcomes. This gives

$$\frac{1}{3} \cdot \frac{\binom{81}{2}}{\binom{81}{3}} = \frac{3!}{3 \cdot 2} \cdot \frac{81 \cdot 80}{81 \cdot 80 \cdot 79} = \frac{1}{79}.$$

Thus, the probability is slightly higher than the probability of picking a specific card (which is $1/81$).

Question

How many SETs have d attributes different in all three cards, $1 \leq d \leq 4$?

There are 3^4 ways to select the first card. Once the first card is selected, the second card can be selected in $\binom{4}{d}2^d$ ways, since one value of each of d attributes is excluded and there are $\binom{4}{d}$ ways to select d attributes which are supposed to be different in all three cards. Once two cards are selected, the third card is determined uniquely. Thus, we have $3^4\binom{4}{d}2^d$ *ordered* triples which form a SET with the desired property. Since the order is irrelevant for our purposes, this number must be divided by $3!$. So, the answer is $27 \cdot \binom{4}{d}2^{d-1}$.

The probability to encounter such a set is thus $81 \cdot \binom{4}{d}2^{d-1}/\binom{81}{2} = \binom{4}{d}2^d/80$. The numbers are: $1/10$, $3/10$, $2/5$ and $1/5$ (so the most common SETs are those with 3 different attributes).

Hard questions

- When the game is played, 12 cards are put on the table at the same time. What is the probability that there will be no SETs among these 12 cards?
- What is the minimal number of cards one needs to draw to ensure that there is a SET among them?

What else can we count using $\binom{m}{k}$?

There are $\binom{m}{k}$ ways to choose k indistinguishable objects from a collection of m objects or to fill k indistinguishable boxes so that no box contains more than one object (the number of *combinations* of k objects out of m objects is $\binom{m}{k}$).

There are $\binom{m}{k}$ sequences of integers $1 \leq i_1 < \cdots < i_k \leq m$.

Indeed, such a sequence identifies with a subset of k elements in $\{1, \ldots, m\}$.

Question

Find the number of sequences of integers $1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq m$.

Given $1 \leq i_1 < \cdots < i_k \leq m$, define a sequence $(j_1, \ldots, j_k)$ by
$j_r = i_r + r - 1$, $1 \leq r \leq k$.

Thus, $j_1 = i_1$, $j_2 = i_2 + 1$, $j_3 = i_3 + 2$ and so on.

Then $j_{r+1} - j_r = (i_{r+1} + r) - (i_r + r - 1) = i_{r+i} - i_r + 1 > 0$ because $i_{r+1} - i_r \geq 0$.

So, $1 \leq j_1 < j_2 < \cdots < j_k \leq m + k - 1$.

Conversely, from each such sequence we can obtain a sequence $1 \leq i_1 \leq \cdots \leq i_k \leq m$ where $i_r = j_r - r + 1$.

Thus, there is a bijection between the set of *weakly increasing* sequences of integers between 1 and m of length k and the set of *strictly increasing* sequences of integers between 1 and $m + k - 1$ of length k.

But the number of the latter sequences is $\binom{m+k-1}{k}$.

Permutations vs Combinations

r-permutations of a set of m elements: ordered arrangements of r elements of our sets.

r-combinations of a set of m elements: subsets containing r elements.

In the first case, the order is important. In the second case, the order does not matter.

Since there are $r!$ ways to permute r *different* objects, the number of r-permutations is $r!$ times the number of r-combinations, that is $r!\binom{m}{r} = m(m-1)\cdots(m-r+1)$.