II/ Opérations dans $\mathbb{N}$

1. Réunion - Intersection d'ensembles finis

Si A et B sont disjoints (i.e. $A \cap B = \varnothing$), $Card(A \cup B) = Card(A) + Card(B)$: C'est la définition de « + »

Cas général : $Card(A \cup B) = Card(A) + Card(B) - Card(A \cap B)$

Extension à 3 ensembles …

2. Produit cartésien d'ensembles, n-uples

- Définition : $A \times B = \{(x, y) / x \in A \text{ et } y \in B\}$
- Si A et B sont finis, $Card(A \times B) = Card(A) \times Card(B)$: C'est la définition de « × »
- Définition : F^E est l'ensemble des applications de E dans F
- Si E est fini, de cardinal $n > 0$ ($E = \{x_1 x_2, ..., x_n\}$) alors F^E est équipotent à $F \times F \times ... \times F$ (ensemble des n-uples d'éléments de F) donc $Card(F^E) = Card(F)^n$.

  Si E et F sont finis, $Card(F^E) = Card(F)^{Card(E)}$.

  (C'est une définition de l'opération 'puissance' dans $\mathbb{N}$)

  Si $n = 0$, $F^{\varnothing} = \{\text{la fonction de graphe vide}\}$ donc si $p \neq 0$, $p^0 = 1$.
- Interprétation de p^n : n tirages à p choix avec remise , rangement d'objets de p sortes dans n casiers.

3. Ensemble des parties

- Fonction indicatrice d'une partie B de A : c'est la fonction φ_B : $\begin{array}{ccc} A & \to & \{0,1\} \\ x & \to & \begin{array}{l} 1 \text{ si } x \in B \\ 0 \text{ si } x \notin B \end{array} \end{array}$
- Pour tout ensemble A , l'ensemble $\mathcal{P}(A)$ des parties de A est équipotent à l'ensemble $\{0,1\}^A$ des applications de A dans $\{0,1\}$.
- Si A est fini, de cardinal n, $Card(\mathcal{P}(A)) = 2^n = 2^{Card(A)}$

III/ Dénombrement

1. *Partitions - Principe du berger*

Soit E un ensemble fini, $A_1, A_2, ..., A_n$ n parties de E.

On dit que $A_1, A_2, ..., A_n$ forme une partition de E ssi les A_i sont disjoints 2 à 2 et leur réunion est égale à E.

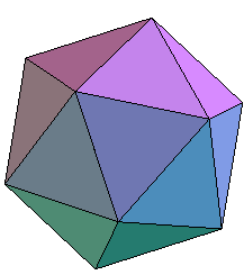
c'est-à-dire $\bigcup_{i=1}^{n} A_i = E$ et $\forall i, j$ tels que $1 \leqslant i < j \leqslant n$, $A_i \cap A_j = \varnothing$

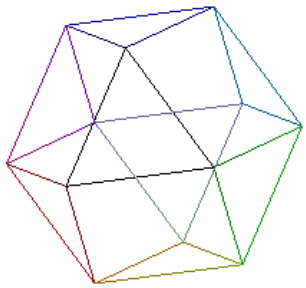
Cela signifie aussi que tout élément de E appartient à un et un seul des A_i

Dans le cas particulier où tous les A_i ont le même cardinal p, on a $card(E) = n.p$, ou $n = \dfrac{Card(E)}{p}$

Exemples

- Combien de triangles peut-on faire avec n points ?
- L'icosaèdre régulier a 20 faces.
  chacune d'elle est un triangle équilatéral.
  Combien a-t-il d'arêtes
- L'octaèdre tronqué a 14 faces :
  6 carrés et 8 triangles.
  Combien a-t-il de sommets ? d'arêtes ?





2. *Puissances - Arrangements- Combinaisons*

Soit E un ensemble à n éléments $(n > 0)$. Soit p un naturel.

- L'ensemble des p-uples d'éléments de E a comme cardinal n^p .
- Si $p \leqslant n$, l'ensemble des p-uples d'éléments de E distincts 2 à 2

  a comme cardinal $n(n-1)...(n-p+1) = \dfrac{n!}{(n-p)!}$. On le note A_n^p

  Si $p > n$, c'est l'ensemble vide On écrit $A_n^p = 0$
- Cas particulier : l'ensemble des n-uples d'éléments de E disticts 2 à 2 a comme cardinal $n!$
  De même l'ensemble des permutations de E (i.e. bijections $E \to E$)
  ou l'ensemble des façons de mettre dans un certain ordre les éléments de E
  ou l'ensemble des anagrammes d'un mot de n lettres distinctes 2 à 2.
- Si $p \leqslant n$, l'ensemble des parties à p éléments de E

  a comme cardinal $\dfrac{n(n-1)...(n-p+1)}{p(p-1)...1} = \dfrac{n!}{p!(n-p)!}$.

  On le note C_n^p ou $\binom{n}{p}$ « p parmi n »

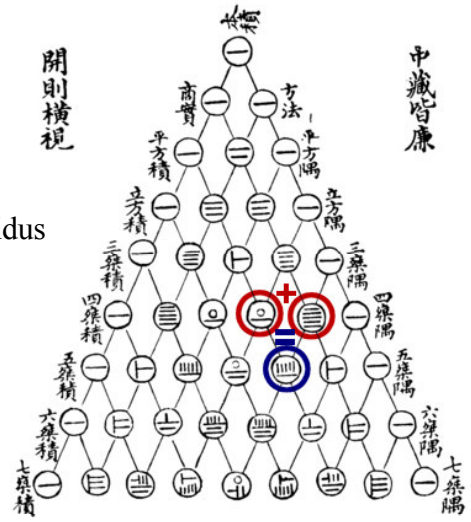
  Si $p > n$, c'est l'ensemble vide. On écrit $C_n^p = 0$

  Interprétations : Tirage avec remise, sans tenir compte de l'ordre.
  Tirages d'un échantillon de p individus dans une population de n individus
  Nombre de mains (5 cartes) au poker.

- Triangle de Pascal

  $\forall n \in \mathbb{N}, \binom{n}{0} = \binom{n}{n} = 1$ et $\forall n, p \in \mathbb{N}$ $\binom{n}{p} + \binom{n}{p+1} = \binom{n+1}{p+1}$
- Formule du binôme de Newton

  $\forall a, b \in \mathbb{C}$ $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

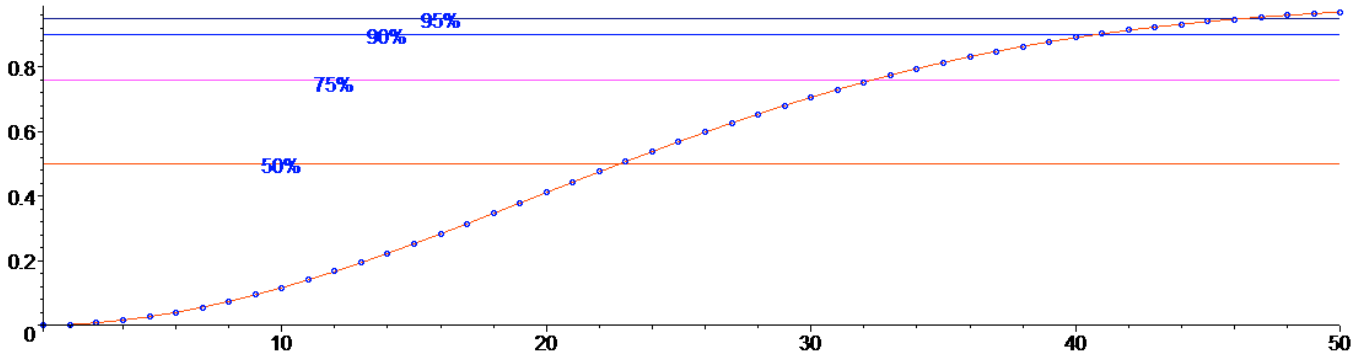


Triangle de Jia Xian (Zhu Shijie 1303)

3. *Exemple de dénombrement - paradoxe des anniversaires*

La probabilité que parmi n personnes, deux au moins aient le même jour d'anniversaire est

$$p(n) = 1 - \frac{365 \times 364 \times \ldots \times (365 - n + 1)}{365^n} = 1 - \frac{365!}{(365-n)!\ 365^n} = 1 - \frac{365}{365} \times \frac{364}{365} \times \ldots \times \frac{(365-n+1)}{365}$$



Généralisation

Soit f une application de E dans F. On pose $n = Card(E)$ et $N = Card(F)$

La probabilité que, parmi les éléments de E, deux au moins aient une même image par f est :

$p(n) = 1 - \frac{N!}{(N-n)!\ N^n}$. On écrit $1 - p(n) = \frac{N-1}{N} \times \ldots \times \frac{(N-n+1)}{N} = \prod_{k=1}^{n-1}\left(1 - \frac{k}{N}\right)$

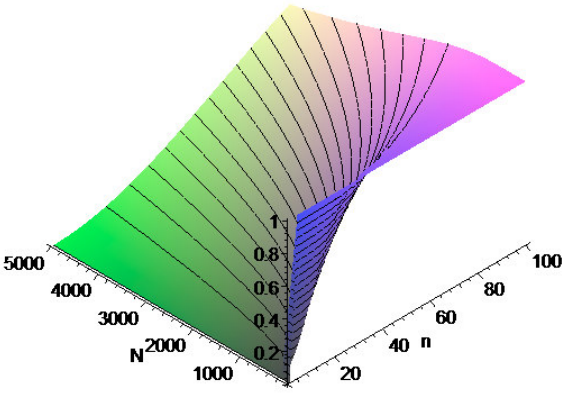
Si n est 'petit' devant N, on a

$$\ln(1 - p(n)) = \sum_{k=1}^{n-1} \ln\left(1 - \frac{k}{N}\right) \sim \sum_{k=1}^{n-1}\left(-\frac{k}{N}\right) = -\frac{n(n-1)}{2N}$$

et $p(n) \approx 1 - \exp\left(-\frac{n(n-1)}{2N}\right)$.

Réciproquement $n \approx \sqrt{-2N \ln(1 - p(n))}$

A.N. pour $p(n) = \frac{1}{2}$ on a $n \approx \sqrt{2N \ln(2)} \approx 1.18\sqrt{N}$



Application en cryptographie

Le paradoxe des anniversaires est utilisé en cryptographie pour élaborer des attaques sur les fonctions de hachage. Une des contraintes imposées sur ces fonctions, pour une utilisation cryptographique, est de produire peu de collisions, autrement dit, de rarement prendre la même valeur sur des entrées différentes.

Le paradoxe des anniversaires donne une borne sur le nombre moyen d'éléments nécessaires pour avoir une collision avec une probabilité p = 1/2, à savoir essentiellement la racine carrée du nombre de valeurs possibles pour la fonction de hachage, sous l'hypothèse que cette fonction est uniformement distribuée sur ses valeurs d'arrivée.

Plus concrètement, si une fonction de hachage a une sortie de N bits alors l'ensemble d'arrivée possède 2^N éléments et il faut environ$2^{N/2}$ hachés d'éléments distincts pour produire une collision avec 50 % de chance.

https://fr.wikipedia.org/wiki/Paradoxe_des_anniversaires