Chapitre 7

Techniques de dénombrement

Introduction

Objectifs de ce chapitre : Etudier des techniques de *dénombrement d'ensembles*.

Exemples d'applications pratiques :

- Déterminer le temps et l'espace requis pour résoudre un problème algorithmique donné ?
- Les techniques de dénombrement sont à la base de la théorie des probabilités (second semestre)
- A l'origine de deux techniques de démonstration importantes : le principe des tiroirs et les démonstrations combinatoires.

- Dans la séquence de 90 nombres à 25 chiffres ci-dessous, est-il possible de trouver deux sous-ensembles de nombres partageant la même somme ?

20480135385502964448038	3171004832173501394113017	5763257331083479647409398	8247331000042995311646021
489445991866915676240992	3208234421597368647019265	5800949123548989122628663	8496243997123475922766310
1082662032430379651370981	3437254656355157864869113	6042900801199280218026001	8518399140676002660747477
1178480894769706178994993	3574883393058653923711365	6116171789137737896701405	8543691283470191452333763
1253127351683239693851327	3644909946040480189969149	6144868973001582369723512	8675309258374137092461352
1301505129234077811069011	3790044132737084094417246	6247314593851169234746152	8694321112363996867296665
1311567111143866433882194	3870332127437971355322815	6814428944266874963488274	8772321203608477245851154
1470029452721203587686214	4080505804577801451363100	6870852945543886849147881	8791422161722582546341091
1578271047286257499433886	4167283461025702348124920	6914955508120950093732397	9062628024592126283973285
1638243921852176243192354	4235996831123777788211249	6949632451365987152423541	9137845566925526349897794
1763580219131985963102365	4670939445749439042111220	7128211143613619828415650	9153762966803189291934419
1826227795601842231029694	4815379351865384279613427	7173920083651862307925394	9270880194077636406984249
1843971862675102037201420	4837052948212922604442190	7215654874211755676220587	9324301480722103490379204
2396951193722134526177237	5106389423855018550671530	7256932847164391040233050	9436090832146695147140581
2781394568268599801096354	5142368192004769218069910	7332822657075235431620317	9475308159734538249013238
2796605196713610405408019	5181234096130144084041856	7426441829541573444964139	9492376623917486974923202
2931016394761975263190347	5198267398125617994391348	7632198126531809327186321	9511972558779880288252979
2933458058294405155197296	5317592940316231219758372	7712154432211912882310511	9602413424619187112552264
3075514410490975920315348	5384358126771794128356947	7858918664240262356610010	9631217114906129219461111
3111474985252793452860017	5439211712248901995423441	7898156786763212963178679	9908189853102753335981319
3145621587936120118438701	5610379826092838192760458	8147591017037573337848616	9913237476341764299813987
3148901255628881103198549	5632317555465228677676044	8149436716871371161932035	
3157693105325111284321993	5692168374637019617423712	8176063831682536571306791	

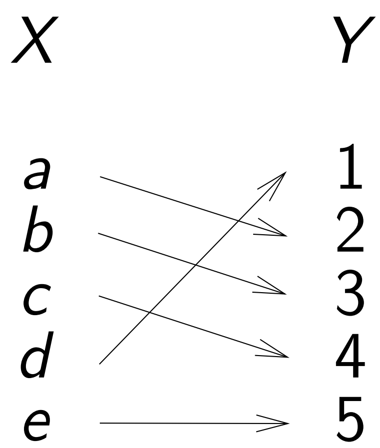
Bijections

Définition : Une fonction $f : X \longrightarrow Y$ est une *bijection* si et seulement si les deux conditions suivantes sont satisfaites :

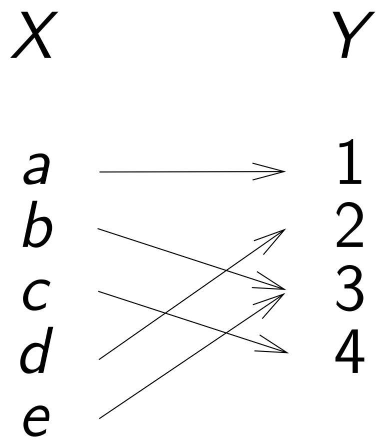
- $(\forall y \in Y)(\exists x \in X) \;\; (f(x) = y)$
- $(\forall x_1, x_2 \in X) \;\; [(f(x_1) = f(x_2)) \Rightarrow (x_1 = x_2)].$

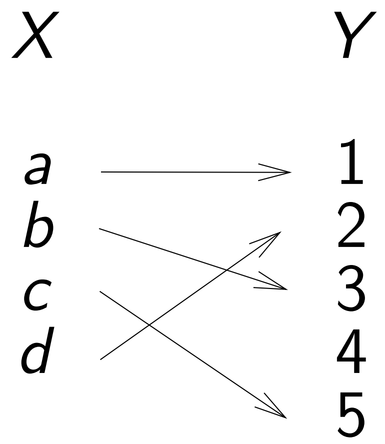
Exemples :

- La fonction représentée ci-dessous est une bijection.



- Les fonctions représentées ci-dessous ne sont pas des bijections.





Propriété : S'il existe une bijection $f : A \longrightarrow B$, alors $|A| = |B|$.

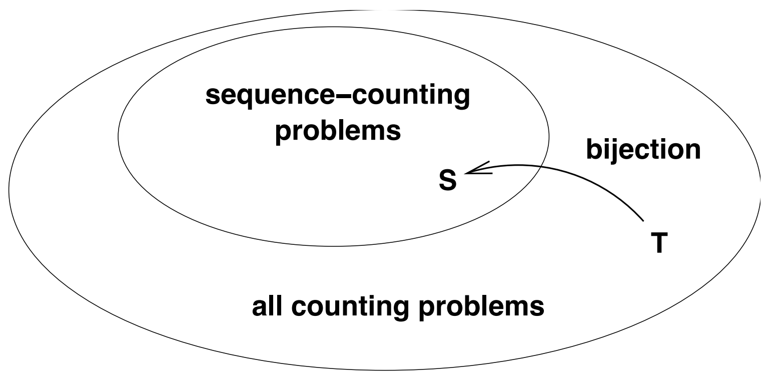
Application : Soient

- $A =$ l'ensemble des possibilités pour sélectionner 12 objets lorsqu'il en existe 5 sortes différentes ;
- $B =$ l'ensemble des séquences de 16 bits comportant exactement quatre “1”.

On peut représenter biunivoquement les manières de sélectionner 12 objets parmi 5 sortes disponibles par les séquence de 16 bits comportant exactement quatre “1” :

$$\underbrace{00}_{\text{Sorte A}}\quad 1\quad \underbrace{\qquad}_{\text{Sorte B}}\quad 1\quad \underbrace{000000}_{\text{Sorte C}}\quad 1\quad \underbrace{00}_{\text{Sorte D}}\quad 1\quad \underbrace{00}_{\text{Sorte E}}$$

On a donc $|A| = |B|$.



Stratégie générale pour le dénombrement :

- Apprendre à compter certains types d'objets
- Utiliser la règle de bijection pour compter tout le reste

Dans ce cours, on va apprendre à dénombrer les *séquences*.

Une séquence est une collection ordonnée d'éléments (appelés composants ou termes).

Exemple : (a,b,c) et (c,b,a) sont deux séquences différentes

Produits cartésiens

Définition (rappel) : Si $P_1, P_2, \ldots, P_n$ sont des ensembles, alors le *produit cartésien*

$$P_1 \times P_2 \times \cdots \times P_n$$

est l'ensemble de toutes les séquences $(p_1, p_2, \ldots, p_n)$ avec $p_1 \in P_1$, $p_2 \in P_2$, $\ldots$, $p_n \in P_n$.

Propriété : Si $P_1, P_2, \ldots, P_n$ sont des ensembles, alors

$$|P_1 \times P_2 \times \cdots \times P_n| = |P_1| \cdot |P_2| \cdots |P_n|.$$

Application : sous-ensembles

Soit $X = \{x_1, x_2, \dots, x_n\}$ un ensemble comportant n éléments.

Question : Combien existe-t-il de sous-ensembles de X ?

Exemple : L'ensemble $X = \{x_1, x_2, x_3\}$ admet 8 sous-ensembles :
$\{\}, \{x_1\}, \{x_2\}, \{x_3\}, \{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}, \{x_1, x_2, x_3\}$.

Réponse : Bijection entre l'ensemble des sous-ensembles de X et les séquences de n bits :

$$S \mapsto (b_1, b_2, \ldots, b_n),$$

- $S \subseteq X$,
- $b_i = 1$ si et seulement si $x_i \in S$.

sous-ensemble :	$\{$		$x_2,$	$x_3,$		$x_5,$		$x_7,$			x_{10} $\}$
séquence :	$($	0	1	1	0	1	0	1	0	0	1 $)$

Comme l'ensemble des séquences de n bits est $\{0,1\} \times \{0,1\} \times \cdots \times \{0,1\} = \{0,1\}^n$, il en existe 2^n.

L'ensemble X admet donc 2^n sous-ensembles.

Unions disjointes

Propriété : Si $A_1, A_2, \ldots, A_n$ sont des ensembles disjoints, alors

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

Remarque : Si les ensembles $A_1, A_2, \ldots, A_n$ ne sont pas nécessairement disjoints, alors le calcul de $|A_1 \cup A_2 \cup \cdots \cup A_n|$ est plus compliqué, et sera étudié plus tard.

Application : mots de passe

Considérons un programme dans lequel un mot de passe est dit valide si

- il contient entre 6 et 8 caractères,
- son premier caractère est une lettre (majuscule ou minuscule), et
- les autres caractères sont soit des lettres, soit des chiffres.

Question : Combien existe-t-il de mots de passe valides ?

Réponse : Définissons F et S par

- $F = \{a, b, \ldots, z, A, B, \ldots, Z\}$,
- $S = \{a, b, \ldots, z, A, B, \ldots, Z, 0, 1, \ldots, 9\}$.

L'ensemble des mots de passe valides est

$$(F \times S^5) \cup (F \times S^6) \cup (F \times S^7).$$

Comme $(F \times S^5)$, $(F \times S^6)$ et $(F \times S^7)$ sont disjoints, on a

$$\begin{aligned} & |(F \times S^5) \cup (F \times S^6) \cup (F \times S^7)| \\ = \ & |(F \times S^5)| + |(F \times S^6)| + |(F \times S^7)| \\ = \ & 52 \cdot 62^5 + 52 \cdot 62^6 + 52 \cdot 62^7 \\ \approx \ & 1,8 \cdot 10^{14} \text{ mots de passe valides.} \end{aligned}$$

Principe des tiroirs (Pigeonhole principle)

Principe des tiroirs : Si $|X| > |Y|$, alors, pour toute fonction $f : X \to Y$, il existe deux éléments distincts de X qui sont associés au même élément de Y.

Source : `http ://en.wikipedia.org/wiki/Pigeonhole_principle`

Exemples

- Si n chaussettes occupent m tiroirs, et si $n > m$, alors au moins un tiroir doit contenir strictement plus d'une chaussette. *(version française du "pigeonhole principe")*
- Un tiroir dans une chambre sombre contient des chaussettes rouges, des chaussettes vertes et des chaussettes bleues. Combien faut-il en retirer du tiroir pour être sûr d'avoir deux chaussettes de la même couleur ?
- S'il y a n personnes qui se serrent la main ($n > 1$), il y a toujours deux personnes qui saluent le même nombre de personnes.
- Tout algorithme de compression sans perte ne fonctionnera pas pour certaines entrées (le taux de compression sera inférieur à 1).

Principe des tiroirs généralisé : Si $|X| > k \cdot |Y|$, alors toute fonction $f : X \to Y$ fait correspondre au moins $k + 1$ éléments distincts de X vers le même élément de Y.

Exemple : Démontrons qu'au moins 5 liégeois ont exactement le même nombre de cheveux

- Environ 900.000 personnes habitant la province de Liège ne sont pas chauves. Soit A cet ensemble.
- Le nombre de cheveux sur une personne est au plus de 200.000. Soit $B = \{1, 2, \ldots, 200.000\}$.
- On a $|A| > 4 \cdot |B|$.
- Dès lors, au moins 5 liégeois ont exactement le même nombre de cheveux.

Application : sous-ensembles partageant la même somme

- Dans la séquence de 90 nombres à 25 chiffres ci-dessous, est-il possible de trouver deux sous-ensembles de nombres partageant la même somme ?

20480135385502964448038	3171004832173501394113017	5763257331083479647409398	8247331000042995311646021
489445991866915676240992	3208234421597368647019265	5800949123548989122628663	8496243997123475922766310
1082662032430379651370981	3437254656355157864869113	6042900801199280218026001	8518399140676002660747477
1178480894769706178994993	3574883393058653923711365	6116171789137737896701405	8543691283470191452333763
1253127351683239693851327	3644909946040480189969149	6144868973001582369723512	8675309258374137092461352
1301505129234077811069011	3790044132737084094417246	6247314593851169234746152	8694321112363996867296665
1311567111143866433882194	3870332127437971355322815	6814428944266874963488274	8772321203608477245851154
1470029452721203587686214	4080505804577801451363100	6870852945543886849147881	8791422161722582546341091
1578271047286257499433886	4167283461025702348124920	6914955508120950093732397	9062628024592126283973285
1638243921852176243192354	4235996831123777788211249	6949632451365987152423541	9137845566925526349897794
1763580219131985963102365	4670939445749439042111220	7128211143613619828415650	9153762966803189291934419
1826227795601842231029694	4815379351865384279613427	7173920083651862307925394	9270880194077636406984249
1843971862675102037201420	4837052948212922604442190	7215654874211755676220587	9324301480722103490379204
2396951193722134526177237	5106389423855018550671530	7256932847164391040233050	9436090832146695147140581
2781394568268599801096354	5142368192004769218069910	7332822657075235431620317	9475308159734538249013238
2796605196713610405408019	5181234096130144084041856	7426441829541573444964139	9492376623917486974923202
2931016394761975263190347	5198267398125617994391348	7632198126531809327186321	9511972558779880288252979
2933458058294405155197296	5317592940316231219758372	7712154432211912882310511	9602413424619187112552264
3075514410490975920315348	5384358126771794128356947	7858918664240262356610010	9631217114906129219461111
3111474985252793452860017	5439211712248901995423441	7898156786763212963178679	9908189853102753335981319
3145621587936120118438701	5610379826092838192760458	8147591017037573337848616	9913237476341764299813987
3148901255628881103198549	5632317555465228677676044	8149436716871371161932035	
3157693105325111284321993	5692168374637019617423712	8176063831682536571306791	

- Considérons un ensemble S de 90 nombres à 25 chiffres.
- Soit A l'ensemble des sous-ensembles de S.
- Soit B l'ensemble des sommes potentielles.
- Il y a $|A| = 2^{90}$ sous-ensembles possibles. On a $2^{90} \geq 1,237 \cdot 10^{27}$.
- La somme de tout sous-ensemble vaut au maximum $90 \cdot 10^{25}$. Les sommes potentielles sont donc $B = \{0, 1, \ldots, 90 \cdot 10^{25}\}$. Il y en a $90 \cdot 10^{25} + 1 \leq 0,901 \cdot 10^{27}$.
- On a $|A| > |B|$.
- Par le principe des tiroirs, deux sous-ensembles partagent la même somme.

Produits cartésiens généralisés

Propriété : Soit S un ensemble de séquences, chacune de longueur k. S'il y a

- n_1 possibilités pour les premiers éléments,
- n_2 possibilités pour les deuxièmes éléments quand le premier élément est fixé,
- n_3 possibilités pour les troisièmes éléments quand le premier et le deuxième élément sont fixés, etc.,

alors

$$|S| = n_1 \cdot n_2 \cdot n_3 \dots n_k.$$

Application : permutations

Définition : Une *permutation* d'un ensemble S est une séquence qui contient chaque élément de S exactement une fois.

Exemple : Les permutations de l'ensemble $\{a, b, c\}$ sont

$$(a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a).$$

Question : Considérons un ensemble de n éléments. Combien de permutations de cet ensemble existe-t-il ?

Réponse :

- Il y a n choix possibles pour le premier élément.
- Pour chacun d'entre-eux, il y a $n-1$ choix possibles pour le deuxième élément.
- Une fois que les deux premiers éléments sont fixés, il y a $n-2$ possibilités pour le troisième élément, etc.
- Il y a donc

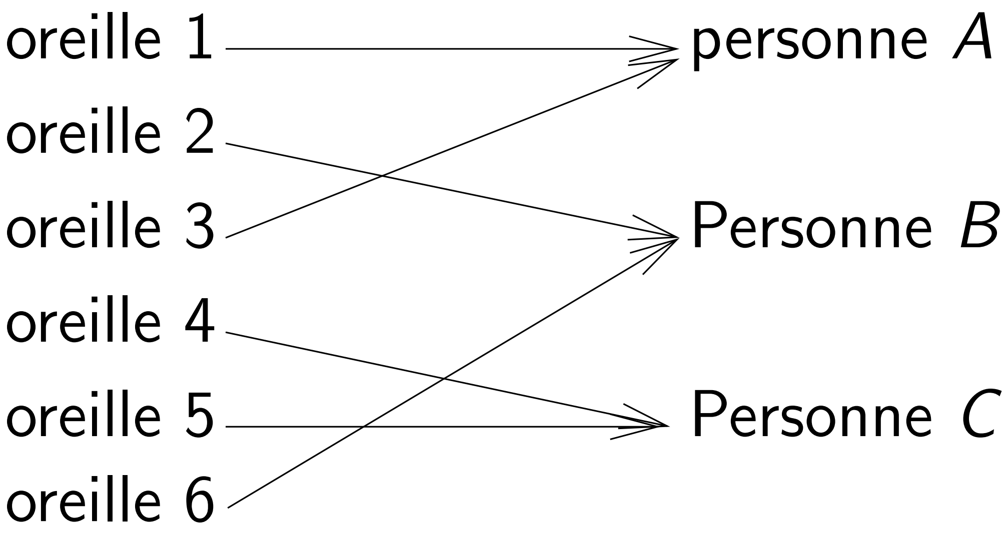
$$n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1 = n!$$

permutations possibles pour un ensemble à n éléments.

Règle de division

Définition : Soit $f : X \to Y$ une fonction. Cette fonction est une *fonction k-vers*-1 si et seulement si elle fait correspondre exactement k éléments de X vers chaque élément de Y.

Exemple de fonction 2-vers-1 :

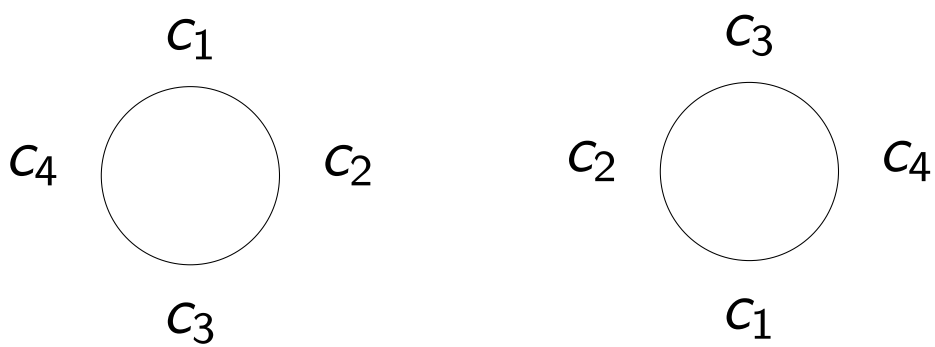


Propriété : Si $f : X \to Y$ est une fonction k-vers-1, alors $|X| = k \cdot |Y|$.

Application : permutations cycliques

Question : De combien de manières peut-on disposer n personnes autour d'une table ronde ?

Remarque : Les deux dispositions suivantes sont équivalentes :



Réponse :

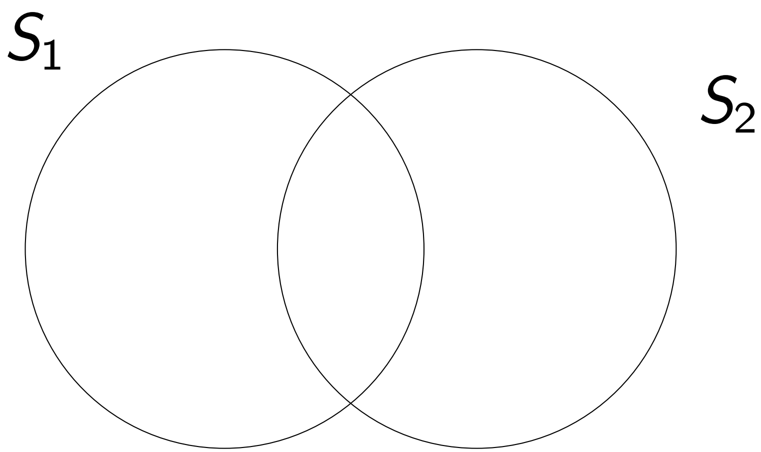
- Soit A l'ensemble des *permutations* des n personnes.
- Soit B l'ensemble des *dispositions* possibles.
- Soit $f : A \rightarrow B$ la fonction qui fait correspondre les permutations aux dispositions correspondantes.
- Cette fonction est une fonction n-vers-1.
- Par la règle de division, on obtient

$$
\begin{aligned}
|B| &= \frac{|A|}{n} \\
&= \frac{n!}{n} \\
&= (n-1)!
\end{aligned}
$$

Union de deux ensembles

Propriété : Soit S_1 et S_2 deux ensembles non nécessairement disjoints. On a

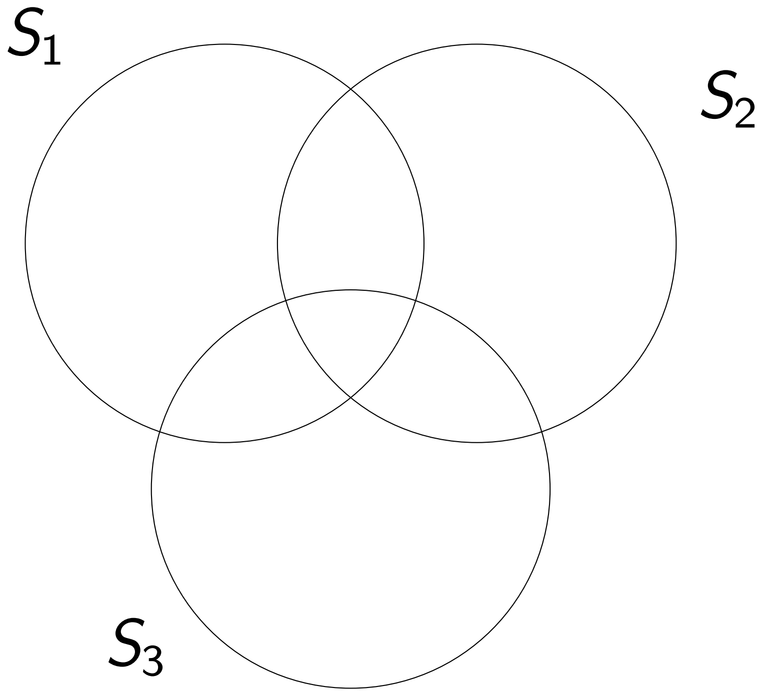
$$|S_1 \cup S_2| = |S_1| + |S_2| - |S_1 \cap S_2|.$$



Union de trois ensembles

Propriété : Soient S_1, S_2 et S_3 trois ensembles non nécessairement disjoints. On a

$$\begin{aligned}|S_1 \cup S_2 \cup S_3| &= |S_1| + |S_2| + |S_3| \\ &\quad -|S_1 \cap S_2| - |S_1 \cap S_3| - |S_2 \cap S_3| \\ &\quad +|S_1 \cap S_2 \cap S_3|.\end{aligned}$$



Application

Considérons les permutations de l'ensemble $\{0, 1, 2, \ldots, 9\}$ dans lesquelles au moins une des conditions suivantes est satisfaite :

- 4 précède directement 2,
- 0 précède directement 4, ou
- 6 précède directement 0.

Question : Combien existe-t-il de telles permutations ?

Réponse :

- Soient P_{42}, P_{60} et P_{04} l'ensemble des permutations dans lesquelles 42, 60 et 04 apparaissent respectivement.
- Il existe une bijection entre P_{42} et l'ensemble des permutations de $\{42, 0, 1, 3, 5, 6, 7, 8, 9\}$. On a donc $|P_{42}| = 9!$.
- Idem pour $P_{60} = P_{04} = 9!$.
- Il existe une bijection entre $P_{42} \cap P_{60}$ et l'ensemble des permutations de $\{42, 60, 1, 3, 5, 7, 8, 9\}$. On a donc $|P_{42} \cap P_{60}| = 8!$.
- Il existe une bijection entre $P_{60} \cap P_{04}$ et l'ensemble des permutations de $\{604, 1, 2, 3, 5, 7, 8, 9\}$. On a donc $|P_{60} \cap P_{04}| = 8!$.
- On a aussi $|P_{42} \cap P_{04}| = 8!$ et $|P_{60} \cap P_{04} \cap P_{42}| = 7!$.
- On obtient $|P_{42} \cup P_{04} \cup P_{60}| = 9! + 9! + 9! - 8! - 8! - 8! + 7!$.

Union de n ensembles

Propriété (Principe d'inclusion-exclusion) : Soient $S_1, S_2, \ldots, S_n$ des ensembles non nécessairement disjoints. On a

$$\begin{array}{rl} & |S_1 \cup S_2 \cup \cdots \cup S_n| \\ = & \text{la somme des tailles des ensembles individuels} \\ - & \text{la somme des tailles des intersections de 2 ensembles} \\ + & \text{la somme des tailles des intersections de 3 ensembles} \\ - & \text{la somme des tailles des intersections de 4 ensembles} \\ + & \ldots \end{array}$$

Plus formellement :

$$\left|\bigcup_{i=1}^{n} S_i\right| = \sum_{\emptyset \neq I \subseteq \{1,\ldots,n\}} (-1)^{|I|+1} \left|\bigcap_{i \in I} S_i\right|$$

Calcul de la fonction indicatrice d'Euler

Rappel : La fonction indicatrice d'Euler $\phi(n)$ désigne le nombre d'entiers de $\{0, 1, 2, \ldots, n-1\}$ premiers avec n.

On peut calculer $\phi(n)$ par le principe d'inclusion-exclusion.

- Soit S l'ensemble des entiers non négatifs plus petits que n qui *ne* sont *pas* premiers avec n. On a $\phi(n) = n - |S|$.
- Supposons la factorisation suivante de n :

  $$n = p_1^{e_1} \ldots p_m^{e_m},$$

  où p_i sont des nombres premiers distincts.
- Soit C_a l'ensemble des entiers positifs plus petit que n et divisible par a, on a :

  $$S = \bigcup_{i=1}^{m} C_{p_i}$$

- Les tailles des intersections entre C_{p_i} sont faciles à calculer.
- Par exemple, $C_{p_i} \cap C_{p_j} \cap C_{p_k}$ est l'ensemble des entiers ($< n$) divisibles par p_i,p_j et p_k. Comme p_i, p_j et p_k sont des premiers distincts, $C_{p_i} \cap C_{p_j} \cap C_{p_k}$ est l'ensemble des entiers ($< n$) divisibles par $p_i \cdot p_j \cdot p_k$:

$$|C_{p_i} \cap C_{p_j} \cap C_{p_k}| = \frac{n}{p_i p_j p_k}.$$

- En appliquant le principe d'inclusion-exclusion, on obtient :

$$\begin{aligned} |S| &= \left|\bigcup_{i=1}^{m} C_{p_i}\right| \\ &= \sum_{i=1}^{m} |C_{pi}| - \sum_{1 \leq i < j \leq m} |C_{p_i} \cap C_{p_j}| \\ &\quad + \sum_{1 \leq i < j < k \leq m} |C_{p_i} \cap C_{p_j} \cap C_{p_k}| - \ldots + (-1)^{m-1} \left|\bigcap_{i=1}^{m} C_{p_i}\right| \end{aligned}$$

$$|S| = n\left(\sum_{i=1}^{m} \frac{1}{p_i} - \sum_{1\le i<j\le m} \frac{1}{p_i p_j} + \sum_{1\le i<j<k\le m} \frac{1}{p_i p_j p_k} - \ldots + (-1)^{m-1} \frac{1}{p_1 p_2 \ldots p_m}\right)$$

- Finalement, on a

$$\begin{aligned} \phi(n) &= n - |S| \\ &= n\left(1 - \sum_{i=1}^{m} \frac{1}{p_i} + \sum_{1\le i<j\le m} \frac{1}{p_i p_j} - \ldots + (-1)^m \frac{1}{p_1 p_2 \ldots p_m}\right) \\ &= n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right). \end{aligned}$$

- En remplaçant n par sa factorisation :

$$\begin{aligned} \phi(n) &= \prod_{i=1}^{m} p_i^{e_i} \left(1 - \frac{1}{p_i}\right) \\ &= \prod_{i=1}^{m} (p_i^{e_i} - p_i^{e_i - 1}). \end{aligned}$$