Exercice 1 :

Soit $n_1, \ldots, n_{12}$ une famille de 12 nombres entiers. Démontrer qu'il existe $i \neq j$ tels que $n_i - n_j$ est un multiple de 11 (au moins deux d'entre eux ont une différence divisible par 11).

Solution:

Regarder les restes des nombres n i par la division euclidienne par 11. Il y a 11 restes possibles, donc au moins deux valeurs distinctes parmi les n i ont le même reste. Leur différence est divisible par 11.

Exercice 2 :

Dans un groupe de six personnes, il existe un groupe de trois personnes qui se connaissent mutuellement ou un groupe de trois personnes qui ne se connaissent ni l'une ni l'autre.

Solution:

Par le principe des tiroirs, chaque personne connait au moins 3 personnes ou ne connait pas au moins 3 personnes. Si la personne 1 connait au moins 3 personnes, soit ces 3 personnes ne se connaissent pas, soit au moins deux se connaissent, ce qui fait un groupe de trois personnes qui se connaissent mutuellement. Le raisonnement est dual si la personne 1 ne connait pas au moins 3 personnes.

Exercice 3 :

Un mot de passe est considéré comme *valide* s'il vérifie les conditions suivantes :

- Il est formé de 8 caractères pris parmi les 26 lettres (minuscules) de l'alphabet, les chiffres entre 0 et 9, et les 7 caractères spéciaux !, ?, %, #, @, &, $.
- Il comprend au moins une lettre de l'alphabet.
- Il comprend au moins un chiffre.
- Il comprend au moins un caractère spécial.

Déterminer le nombre de mots de passe valides.

Solution:

Il y a a priori $26 + 10 + 7 = 43$ caractères dont 43^8 mots de 8 caractères. On cherche le nombre de non valides :

- Soit A l'ensemble des mots qui ne contiennent pas de lettre de l'alphabet ; $|A| = 17^8$.
- Soit B l'ensemble des mots qui ne contiennent pas de chiffre ; $|B| = 33^8$.
- Soit C l'ensemble des mots qui ne contiennent pas de caractère spécial ; $|C| = 36^8$.

On utilise la formule du crible :

- $A \cap B$ est l'ensemble des mots écrits uniquement avec des caractères spéciaux, donc $|A \cap B| = 7^8$.
- $A \cap C$ est l'ensemble des mots écrits uniquement avec des chiffres, donc $|A \cap C| = 10^8$.
- $B \cap C$ est l'ensemble des mots écrits uniquement avec des lettres, donc $|B \cap C| = 26^8$.
- $A \cap B \cap C$ est l'ensemble vide.

Donc $|A \cup B \cup C| = 17^8 + 33^8 + 36^8 - (7^8 + 10^8 + 26^8)$,
et il y a donc $43^8 - (17^8 + 33^8 + 36^8) + (7^8 + 10^8 + 26^8) (= 7662638823840)$.

Exercice 4 :

Soit m, n deux entiers naturels. On note $s(m,n)$ le nombre de surjections d'un ensemble de cardinal m sur un ensemble de cardinal n.

1. Que valent $s(m,n)$ si $m < n$? Si $m = n$?

Solution:
$s(m,n) = 0$ si $m < n$, $s(m,n) = n!$ si $m = n$.

2. En utilisant la formule du crible, justifier l'égalité :

$$s(m,n) = n^m - n(n-1)^m + \binom{n}{2}(n-2)^m + \cdots + (-1)^k\binom{n}{k}(n-k)^m + \cdots + (-1)^n n$$

Solution:
Soit $I \subset [\![1,n]\!]$. On pose $E_I = \mathcal{F}([\![1,m]\!], [\![1,n]\!] \setminus I)$ (les applications de $[\![1,m]\!]$ dans $[\![1,n]\!]$ qui évitent I). Le cardinal de E_I est $(n-|I|)^m$. On applique la formule du crible à $\cup_{i\in[\![1,n]\!]} E_{\{i\}}$, qui est le complémentaire de l'ensemble des surjections, en constatant que $\cap_{i\in I} E_{\{i\}} = E_I$.

Exercice 5 :

(Théorème de Ramsey)

1. Montrer que $\forall (n_r, n_b) \in \mathbb{N}^2, \exists N \in \mathbb{N}$ tel que pour toute coloration en 2 couleurs $\{r, b\}$ du graphe complet K_N d'ordre N, il existe une couleur $c \in \{r, b\}$ et un sous-graphe complet de K_N d'ordre n_c qui soit monochromatique de couleur c.
(le plus petit N vérifiant cette propriété est noté $R(n_r, n_b)$).

Solution:
On raisonne par récurrence sur $n_r + n_b$. La définition implique clairement que, pour tout n, $R(n,1) = R(1,n) = 1$. Montrons que $R(n_r, n_b)$ existe en en donnant un majorant explicite. On suppose (hypothèse de récurrence) que $R(n_r - 1, n_b)$ et $R(n_r, n_b - 1)$ existent. On va montrer que $R(n_r, n_b) \leq R(n_r - 1, n_b) + R(n_r, n_b - 1)$.
Considérons un graphe complet 2-coloré ayant $R(r-1,s) + R(r,s-1)$ sommets. Choisissant un sommet v, on définit une partition des autres sommets en deux ensembles $M = \{w, (v,w) \text{ est rouge}\}$ et $N = \{w, (v,w) \text{ est bleue}\}$. Le graphe ayant $R(r-1,s) + R(r,s-1) = |M| + |N| + 1$ sommets, on a $|M| \leq R(r-1,s)$ ou $|N| \leq R(r,s-1)$. Dans le premier cas, si M contient un K_{n_b} monochromatique bleu, il en est du même du graphe initial ; sinon, M contient un K_{n_r-1} monochromatique rouge, et donc $M \cup v$ contient un K_{n_r} rouge par définition de M. Échangeant les couleurs, on a le même résultat (pour N) dans le second cas. L'inégalité est donc démontrée, ce qui achève par récurrence la démonstration du théorème pour deux couleurs.

2. Montrer que $\forall k \in \mathbb{N}, \forall (n_1, n_2, \ldots, n_k) \in \mathbb{N}^k, \exists N \in \mathbb{N}$ tel que pour toute coloration en k couleurs du graphe complet K_N d'ordre N, il existe une couleur $c \in [\![1,k]\!]$ et un sous-graphe complet de K_N d'ordre n_c qui soit monochromatique de couleur c.
(le plus petit N vérifiant cette propriété est noté $R(n_1, \ldots, n_k)$).

Solution:
On raisonne par récurrence sur k. Le résultat est trivial pour $k = 1$ et vient d'être démontré pour $k = 2$. Si $k > 2$, on va montrer l'inégalité suivante :
$R(n_1, \ldots, n_k) \leq R(n_1, \ldots, n_{k-2}, R(n_{k-1}, n_k)) = t$.

Soit une k-coloration du graphe complet K_t ayant t sommets. Identifiant les couleurs $k-1$ et k, on obtient une $(k-1)$-coloration du graphe qui, d'après l'hypothèse de récurrence, contient soit un K_{n_i} monochromatique de couleur i avec $1 \leq i \leq k-2$, soit un $K_{R(n_{k-1},n_k)}$ de la couleur obtenue par identification. Le premier cas satisfait l'inégalité ; dans le second, on est donc ramené à un problème de 2-coloration et, par définition de $R(n_{k-1}, n_k)$, on doit avoir soit un $K_{n_{k-1}}$ $(k-1)$-monochrome, soit un K_{n_k} k-monochrome. Dans les deux cas, ceci achève la démonstration de l'inégalité. Par récurrence, le cas général est donc prouvé.

Exercice 6 :

On a coloré des arcs sur un cercle de diamètre 1. La somme des longueurs des arcs colorés est $< \pi/2$. Démontrer qu'il existe un diamètre du cercle dont les deux extrémités ne sont pas colorées.

Solution:

On colore aussi les arcs symétriques des arcs colorés sur le cercle. La longueur des arcs colorés est alors 2 fois la longueur initialement colorée, donc $< \pi$. Le diamètre d'extrémité un point non coloré convient.

Exercice 7 :

Soit $n+1$ nombres $m_1, ..., m_{n+1}$ choisis parmi les nombres entiers naturels $1, 2, ..., 2n$. Montrer qu'il existe i, j, $1 \leq i \neq j \leq n+1$ tels que m_i divise m_j.

Solution:

On décompose chaque entier m_i sous la forme $2^{k_i} q_i$, avec q_i un entier impair compris entre 1 et $2n-1$. Il y a n entiers impairs entre 1 et $2n$, donc par le principe des tiroirs, il existe $i \neq j$ tels que $q_i = q_j$. Alors m_i divise m_j ou m_i est un multiple de m_j.

Exercice 8 :

Pour toute relation binaire R on définit sa "clôture transitive à gauche".

$$\frac{xRy}{xR^g y} \qquad \frac{xR^g y \quad yRz}{xR^g z}$$

Montrer que $R^g = R^+$.

Solution:

On montre d'abord que $R^g \subseteq R^+$ en utilisant le principe de preuve induit par la définition de R^g. Soit $Q \subseteq E \times E$ vérifiant les deux propriétés ci-dessous.

- $R \subseteq Q$
- $(xQy \wedge yRz) \Rightarrow xQz$

Alors $R^g \subseteq Q$.

- $R \subseteq R^+$ par la règle $+_1$.
- Si xR^+y et yRz, alors xR^+y et yR^+z (car $R \subseteq R^+$), donc xR^+z par la règle $+_2$.

Ainsi $R^g \subseteq R^+$.

Il est plus compliqué de montrer que $R^+ \subseteq R^g$. Pour utiliser le principe de preuve induit par la définition de R^+, il faut d'abord montrer que R^g est transitive.

Soit $x \in E$. On cherche à montrer que pour tout $y, z \in E$, si xR^gy et yR^gz, alors xR^gz. Informellement, on le montre par induction sur yR^gz. Plus précisément, on définit $Q_x \subseteq E \times E$ par yQ_xz ssi $yR^gz \wedge (xR^gy \Rightarrow xR^gz)$, puis on montre que $R^g \subseteq Q_x$ grâce au principe de preuve induit par la définition de R^g.

- Supposons que yRz. Alors yR^gz par la règle t_1, et xR^gy implique xR^gz par la règle t_2. Ainsi, $R \subseteq Q_x$
- Supposons que yQ_xz et zRu,

$$\begin{aligned} yQ_xz \wedge zRu &\Leftrightarrow yR^gz \wedge (xR^gy \Rightarrow xR^gz) \wedge zRu \\ &\Rightarrow yR^gu \wedge (xR^gy \Rightarrow xR^gz) \wedge zRu \text{ par la règle } t_2 \\ &\Rightarrow yR^gu \wedge (xR^gy \Rightarrow (xR^gz \wedge zRu)) \\ &\Rightarrow yR^gu \wedge (xR^gy \Rightarrow xR^gu) \text{ par la règle } t_2 \\ &\Rightarrow yQ_xu \end{aligned}$$

Ainsi, $R^g \subseteq Q_x$, et cela pour tout x.

Finalement, soient $x, y, z \in E$ tels que xR^gy et yR^gz.

$$\begin{aligned} xR^gy \wedge yR^gz &\Rightarrow xR^gy \wedge yQ_xz \text{ comme prouvé plus haut.} \\ &\Rightarrow xR^gy \wedge (xR^gy \Rightarrow xR^gz) \text{ par définition de } Q_x \\ &\Rightarrow xR^gz \end{aligned}$$

Cela montre que R^g est transitive. Comme $R \subseteq R^g$, le principe de preuve induit par la définition de R^+ implique que $R^+ \subseteq R^g$.

Exercice 9 :

(Exercice forestier)

1. Un arbre binaire est un arbre fini dont chaque noeud a zéro ou deux enfants. Donner une définition par récurrence de la description informelle ci-dessus.

   Solution:

   $$\frac{}{[] \in B} \qquad \frac{x \in B \quad y \in B}{[x; y] \in B}$$

   On aurait pu juste utiliser une grammaire : $B ::= [] \mid [B; B]$.

2. Définir une traduction de tout arbre binaire en un arbre au sens ensembliste, sur l'alphabet $\{0, 1\}$.

   Solution:

   $$\begin{array}{rrcl} t : & B & \to & \mathcal{P}(\{0,1\}^*) \\ & [] & \mapsto & \{\epsilon\} \\ & [x; y] & \mapsto & 0 \cdot t(x) \cup 1 \cdot t(y) \end{array}$$

   où $0 \cdot t(x) := \{0w \mid w \in t(x)\}$.

3. Trouver sans justification une relation entre le nombre de feuilles et le nombre de noeuds internes d'un arbre binaire.

Solution:

$$\begin{array}{rccl} f: & B & \to & \mathbb{N} \\ & [] & \mapsto & 1 \\ & [x;y] & \mapsto & f(x)+f(y) \end{array} \qquad \begin{array}{rccl} i: & B & \to & \mathbb{N} \\ & [] & \mapsto & 0 \\ & [x;y] & \mapsto & 1+i(x)+i(y) \end{array}$$

- f calcule le nombre de feuilles d'un arbre donné.
- i calcule le nombre de noeuds internes d'un arbre donné.

Proposition formelle : pour tout $x \in B$, on a $f(x) = i(x) + 1$.

4. Définir les arbres finis et les forêts (listes finis d'arbres) par récurrence structurelle mutuelle, d'abord en utilisant les grammaires.

Solution:

- $A := [F]$
- $F := nil \quad | \quad A :: F$

5. Les définir maintenant par règles d'inférence.

Solution:

$$\frac{l \in F}{[l] \in A} \qquad \frac{}{nil \in F} \qquad \frac{x \in A \quad l \in F}{x :: l \in F}$$

6. Trouver une alternative pour éviter la récurrence mutuelle dans la définition des arbres.

Solution:

- $A := [F]$
- $F := nil \quad | \quad [F] :: F$

C'est-à-dire :

$$\frac{l \in F}{[l] \in A} \qquad \frac{}{nil \in F} \qquad \frac{l' \in F \quad l \in F}{[l'] :: l \in F}$$

7. Définir une traduction (fidèle) des arbres définis par récurrence mutuelle vers les arbres définis par la deuxième méthode.
8. Avec ces nouvelles définitions non mutuelles, définir des fonctions calculant le nombre de noeuds internes et la hauteur.

Soit Σ un alphabet fini.

Exercice 10 :

Soit u et v deux mots de Σ^*. Démontrer par récurrence sur $|u| + |v|$ que $uv = vu \Rightarrow \exists w \in \Sigma^*, \{u, v\} \subset w^*$.

Solution:

Si $|u| = 0$, on pose $w = v$. Sinon, supposons par exemple que u est un préfixe de v ; alors $v = ut$ et $uut = uv = vu = utu$ donc $ut = tu$ avec $|u| + |t| < |u| + |v|$, donc par hypothèse, $\exists w \mid \{u, t\} \subset w^*$. Comme $v = tu$, $v \in w^*$.

Exercice 11 :

Soit m et n des entiers naturels > 0. Résoudre dans Σ^* l'équation $u^m = v^n$.

Solution:

On pose $w = u^m = v^n$.

Supposons $|u|$ et $|v|$ premiers entre eux. On peut supposer $|v| > |u|$. Il existe une relation de Bezout $1 = a|v| - b|u|$ avec a et b entiers naturels, $a < |u|$ et $b < |v|$. Alors, soit $s = |w| = m|u| = n|v|$, avec m multiple de $|v|$ et n multiple de $|u|$. Alors pour tout i entre 1 et s, si $w_i = w_{i+k|u|} = w_{i+l|v|}$ tant que $1 \leq i + k|u| \leq s$ et $1 \leq i + l|v| \leq s$. Pour $i \leq |v|$, $i + a|v| \leq (a+1)|v| \leq |u||v| \leq n|u| = s$ donc $w_i = w_{i+a|v|} = w_{i+a|v|-b|u|} = w_{i+1}$. Ceci démontre que v donc w donc u s'écrit sur une seule lettre. Le cas général s'en déduit en considérant l'alphabet Σ^d où d est le pgcd de $|u|$ et $|v|$.

Exercice 12 :

Soit Σ un alphabet fini. Deux mots u et v de Σ^* sont dits conjugués s'il existe deux mots x et y tels que $u = xy$ et $v = yx$. Démontrer que les mots u et v sont conjugués si et seulement si il existe un mot z tel que $uz = zv$.

Solution:

Supposons qu'il existe un mot z tel que $uz = zv$. Si $|z| \leq |u|$, il existe w tel que $u = zw$. Donc $uz = zwz = zv$ et $wz = v$. Sinon, $|z| > |u|$, il existe w tel que $uw = z$. Alors $zv = uwv = uz$ donc $wv = z$; ainsi $uw = wv$ avec $|w| < |z|$, on conclut par récurrence.

Exercice 13 :

Soit Σ un alphabet fini. On considère trois mots x, y, z dans Σ^* tels que $x^2y^2 = z^2$. Justifier qu'il existe un mot w dans Σ et des entiers p et q tels que $x = w^p$, $y = w^q$ et $z = w^{p+q}$.

Solution:

Si $x^2y^2 = z^2$, $|z^2| = |x^2| + |y^2|$, alors $2|z| = 2|x| + 2|y|$, donc $|z| = |x| + |y|$. En particulier, $|z| \leq |x|$ et x est préfixe de z. Posons $z = xu$. Par le même raisonnement, y est suffixe de z et comme $|u| = |y|$, on obtient $y = u$. On a alors $xyxy = xxyy$ donc par simplification dans le monoïde libre Σ^*, $yx = xy$. On sait alors (cf. Exercice **??**) qu'il existe un mot $w \in \Sigma^*$ et des entiers p et q tels que $x = w^p$, $y = w^q$. Et $z = xy = w^{p+q}$.

Exercice 14 :

Si M est un monoïde et K, L deux parties de M, on note $L^{-1}K = \{x \in M \mid \exists y \in L, yx \in K\}$.

1. Soit L un sous-monoïde de Σ^*. Démontrer que L est un monoïde libre si et seulement si $L^{-1}L \cap LL^{-1} = L$.

   Solution:

   Supposons L libre de base B. Soit $m \in L^{-1}L \cap LL^{-1}$. Il existe p et q dans L tels que $pm \in L$ et $mq \in L$. En décomposant p et pm sur la base B, on obtient que $m \in L$.

   Réciproquement, supposons que $L^{-1}L \cap LL^{-1} = L$. Soit B la partie génératrice minimale de L (les éléments de L qui ne sont pas des produits de deux éléments distincts de 1). Soit $u_1 \dots u_m = v_1 \dots v_n$ avec les u_i et v_j dans B. Posons par exemple dans Σ^*, $u_m = wv_n$, alors $u_1 \dots u_{m-1}w = v_1 \dots v_{n-1}$, donc $w \in L^{-1}L \cap LL^{-1} = L$. Par minimalité des éléments de B dans L, $w = 1$. On conclut par récurrence.

2. Soit L un sous-monoïde de Σ^*. On définit par récurrence : $M_0 = L$, $M_{n+1} = {M_n}^{-1}M_n \cap M_n{M_n}^{-1}$. Démontrer qu'on définit ainsi une suite croissante de monoïdes et que $\cup_N M_n$

est le plus petit sous-monoïde libre contenant L.

Solution:

On remarque que pour tout monoïde M, $L \subset M^{-1}M \cap MM^{-1}$ ($\forall u \in M, 1u \in M$ et $u1 \in M$) donc la suite $(M_n)_n$ est bien une suite croissante et donc $M = \cup_n M_n$ est un monoïde.

Démontrons que $M^{-1}M \cap MM^{-1} \subset M$: soit $u \in \Sigma^*$ tel qu'il existe v et w dans M tels que $vu \in M$ et $uv \in M$. $M = \cup_n M_n$, donc il existe des entiers l et m tels que $v \in M_l$ et $w \in M_m$. Pour $n = \max(l, m)$, v et w sont dans M_n, donc $u \in M_n^{-1}M_n \cap M_nM_n^{-1} = M_{n+1} \subset M$.

Enfin, si $N \subset P$ est une inclusion de sous-monoïdes, avec P libre, on a $N^{-1}N \cap NN^{-1} \subset P^{-1}P \cap PP^{-1} = P$, donc si P contient L, il contient aussi tous les M_n et donc M.