Notes de cours Informatique théorique - II.
(version 1.2, 25.01.2010)

S.V.P. ME SIGNALER TOUTE FAUTE DE FRAPPE, GRAMMAIRE, ORTHOGRAPHE OU LOGIQUE; LES FAUTES DE LOGIQUE VOUS APPORTENT DES POINTS SUPPLÉMENTAIRES POUR LA NOTE FINALE. TOUTE SUGGESTION D'UNE MEILLEURE TRADUCTION D'UN TERME ANGLAIS SERA ÉGALEMENT BIENVENUE.

1 Le dénombrable

Définition 1 *Un ensemble X est* dénombrable *s'il existe une bijection entre X et l'ensemble $\mathbb{N}$ d'entiers non-négatifs.*

Notons que certains auteurs définissent comme dénombrable tout ensemble X qui soit est fini, soit possède une bijection avec $\mathbb{N}$. Ceci est équivalent à :
Un ensemble X est dénombrable s'il existe une injection de X dans $\mathbb{N}$.

Dans la suite, X est *dénombrable* s'il vérifie la définition 1.

Nous allons prouver que pour tout alphabet Σ, l'ensemble de mots sur Σ est dénombrable. On se servira des faits suivants (rappel : pour un ensemble X, sa cardinalité - le nombre de ses éléments quand X est fini - est noté X) que nous ramassons en un lemme.

Lemme 1 *Soit $k \in \mathbb{N}$*

1. $|\{0,1\}^k| = 2^k$
2. $\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$

Démonstration : Le nombre de mots de longueur k sur l'alphabet $\{0,1\}$ est 2^k parce qu'il y a deux choix pour le premier symbole, deux pour le deuxième, et, en général, deux choix pour le i-ème, donc, en tout, 2^k possibilité.
La deuxième identité est évidemment vraie pour $k = 0$. Si elle est vérifiée pour k, on a $\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$. Si on ajoute un terme à la somme, on obtient $\sum_{i=0}^{k+1} 2^i = 2^{k+1} - 1 + 2^{k+1} = 2 \cdot 2^{k+1} - 1 = 2^{k+2} - 1$. Donc, par récurrence, l'identité est vraie pour tout k.
On peut aussi voir la deuxième identité comme le résultat de la substitution de 2 pour x dans l identité évidente

$$x^{k+1} - 1 = (x-1) \sum_{i=0}^{k} x^i.$$

□

Lemme 2 *L'ensemble* $\{0,1\}^*$ *est dénombrable.*

Démonstration : Rappelons que $\{0,1\}^* = \cup_{k\in\mathbb{N}}\Sigma^k$. Suivant cette définition, on va donner une bijection explicite entre $\mathbb{N}$ et $\{0,1\}^*$. Il y a 2^k mots dans $\{0,1\}^k$. Donc pour chaque k, il y a $\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$ mots de longueur au plus k. On va définir la bijection $c : \{0,1\}^* \longrightarrow \mathbb{N}$ par $c(a_1a_2\dots a_k) = 2^k - 1 + n(a_1\dots a_k)$, où $n(a_1\dots a_k)$ est l'entier dont la représentation en binaire est $a_1\dots a_k$; afin que tout marche comme il faut, on doit définir $n(\varepsilon) = 0$. Pour prouver que l'on a vraiment une bijection, définissons l'inverse. Soit $c^{-1}(n) = (n+1-2^{\lfloor \lg n+1\rfloor})_{\lfloor \lg n+1\rfloor}$; ici n_k est la représentation en binaire de n en k bits. Donc si $n = 0$, on obtient la représentation de 0 en zéro bits, i.e. ε. On voit alors que c est surjective. Elle est également injective car si $c(a_1a_2\dots a_k) = c(a'_1a'_2\dots a'_m)$, alors $k = m$ et $a_i = a'_i$ parce que si, sans perte de généralité, $k < m$, alors $c(a_1a_2\dots a_k) = 2^k - 1 + n(a_1a_2\dots a_k) < 2^k - 1 + 2^k < 2^{k+1} - 1 \leq 2^m - 1 \leq c(a'_1a'_2\dots a'_m)$ et quand $k = m$ alors $n(a'_1a'_2\dots a'_m) = n(a_1\dots a_k)$. □

Théorème 1 *L'ensemble* Σ^* *est dénombrable pour tout alphabet* Σ.

Démonstration : Ceci suit facilement du lemme précédent et est donc laissé en exercice. Voici quelques indications - il faut fournir les détails.

Il suffit d'observer que les symboles d'un alphabet Σ de k éléments peuvent être codés en binaire par des mots de longueur $\lceil \lg k\rceil$ (*codé* veut dire que tout mot sur $\{0,1\}$ représente au plus un mot sur Σ. Exercice: formaliser cette notion). Donc pour tout alphabet Σ, l'ensemble de mots binaires qui représentent des mots de Σ^* est une partie de $\{0,1\}^*$ et donc sa cardinalité ne peut pas dépasser celle de $\{0,1\}^*$. □

Exercise 1 *Fournissez les détails de la preuve.*

Définition 2 *Soit* X *un ensemble. L'ensemble de ses parties, noteé* $\mathcal{P}(X)$ *ou, mieux,* 2^X*, est (comme le nom l'indique) l'ensemble* $\{Y : Y \subseteq X\}$.

Remarque 1 *La notation* 2^X *est logique. En voici l'explication. Soit* X, Y *deux ensembles et soit* $Y^X = \{f : X \longrightarrow Y \ : f \text{ est une fonction}\}$*, i.e., l'ensemble des fonctions de* X *dans* Y*. Si* $|Y| = 2$*, on le note souvent - sans perte de généralité -* $\{0,1\}$ *(c'est l'ensemble canonique à 2 éléments, l'alphabet binaire).*
Soit maintenant Y *une partie de* X*. On peut définir une fonction (appelée* caractéristique *$\chi_Y : X \longrightarrow 2$ par $\chi_Y(x) = 1$ si et seulement si $x \in Y$. Inversement, une fonction $f : X \longrightarrow 2$ définit un ensemble $Y_f = \{x \in X : f(x) = 1\}$.*

Exercise 2 *Prouvez que pour tout ensemble* X*, tout* $Y \subseteq X$ *et tout* $f : X \longrightarrow 2$*, on a*

$$Y_{\chi_Y} = Y$$

et

$$\chi_{Y_f} = f.$$

Le résultat important non seulement pour ce qu'il dit mais surtout pour sa technique de preuve que nous reverrons plusieurs fois dans le cours est le théorème de Cantor.

Théorème 2 *Soit X un ensemble. Alors $|2^X| > |X|$.*

Démonstration : Puisque $\{x\} \in 2^X$ pour tout $x \in X$, $|2^X| \geq |X|$. Il faut donc prouver que $|2^X| \neq |X|$. Supposons le contraire, c'est-à-dire, supposons qu'il existe un bijection $f : X \longrightarrow 2^X$. Soit $D = \{x \in X : x \notin f(x)\}$. Puisque f est une bijection, il existe un $d \in X$ tel que $f(d) = D$. Mais alors $d \in D$ si et seulement si $d \notin f(d)$ si et seulement si $d \notin D$. Cette impossibilité implique que f ne peut pas exister. □