Théorie des codes

Olivier Bernard

14 janvier 2010

Codes

Soit A un alphabet, et $X \subsetneq A^*$.

Définition

$X \subsetneq A^*$ est un code si :

$$\begin{array}{l}\forall n, m \in \mathbb{N} \setminus \{0\} \\ \forall (x_i)_{i \in [\![1,n]\!]}, (x'_j)_{j \in [\![1,m]\!]} \in X,\end{array} \quad x_1 \dots x_n = x'_1 \dots x'_m \Longrightarrow \left\{ \begin{array}{l} n = m \\ \forall i \in [\![1, n]\!], \quad x_i = x'_i \end{array} \right.$$

Remarques :

- Pour tout code X, $\varepsilon \notin X$.
- Tout sous-ensemble d'un code est encore un code. En particulier, l'ensemble vide est un code.

Ensembles complets

Soit $S \subseteq A^*$ un ensemble quelconque.

Définition

Un mot $m \in A^*$ est dit complétable dans S si :

$$\exists u, v \in A^* \text{ tels que } umv \in S \qquad , \text{ ie } \quad A^* m A^* \cap S \neq \emptyset.$$

Définition

S est dense dans A si tous les mots de A^* sont complétables dans S.

Remarque : Si S n'est pas dense, on dit que S est maigre.

Définition

S est dit complet si S^* est dense.

Remarques :

- S dense $\Longrightarrow$ S complet.
- L'inverse est faux en général.

Soit A un alphabet, et $X \subsetneq A^*$.

Définition

Un code X est dit maximal sur A si pour tout code X' sur A,
$X \subseteq X' \implies X = X'$.

Théorème

Tout code X sur A est inclus dans un code maximal sur A.

Preuve : Soit $\mathcal{F} = \{W \text{ tq } W \text{ code sur } A,\ X \subseteq W\}$, ordonné par l'inclusion.

- non-vide ;
- inductif.

$\Rightarrow$ Lemme de Zorn. $\square$

Codes complets

Soit A un alphabet.

Théorème

Tout code X sur A est inclus dans un code complet sur A.

- Si $\#A = 1$, obvious.
- Si $\#A \geq 2$, on a une preuve constructive et (donc) venimeuse.

Théorème

Tout code maximal est complet !

Distributions de Bernoulli

Soit A un alphabet.

Définition

Une distribution de Bernoulli sur A^* est un morphisme de monoïdes :

$$\pi : A^* \longrightarrow (\mathbb{R}_+, \times) \quad \text{tel que} \sum_{a \in A} \pi(a) = 1.$$

Elle est dite positive si $\forall a \in A,\ \pi(a) \neq 0$.

On pose naturellement, $\forall L \subseteq A^*,\ \pi(L) = \sum_{l \in L} \pi(l)$.

Proposition

$\pi : \mathfrak{P}(A^*) \longrightarrow \mathbb{R}_+ \cup \{\infty\}$ *est une mesure positive sur* A^*, *ie :*

- $\pi(\emptyset) = 0$ *et* $\forall L \subseteq A^*, \pi(L) \geq 0$;
- $\forall (E_n)_{n \in \mathbb{N}}$ *tq les* $E_n \subseteq A^*$ *sont deux à deux disjoints,* $\pi(\cup E_n) = \sum \pi(E_n)$.

Caractérisations

Soit X un code.

$$\pi(X^*) = \pi\left(\bigcup_{n\in\mathbb{N}} X^n\right) = \sum_{n\in\mathbb{N}} \pi(X^n) = \sum_{n\in\mathbb{N}} \pi^n(X).$$

Proposition

Pour toute distribution de Bernoulli π sur A^*, $\pi(X) \leq 1$.

Remarques :

- Ceci conforte l'intuition qu'un code n'a que peu de mots.
- On peut montrer que s'il existe une distribution de Bernoulli positive telle qu'il y a égalité, alors X est maximal.

Maigre, mais complet

Soit X un code sur A.

Récapitulons :

$\exists\pi$ distribution de Bernoulli positive tq $\pi(X) = 1 \implies X$ maximal $\implies X$ complet.

Proposition

Soit $X \subsetneq A^*$ un ensemble maigre et complet.
Pour toute distribution de Bernoulli positive sur A^*, $\pi(X) \geq 1$.

Preuve : Utilise un lemme technique que vous n'avez pas envie de connaître. $\square$

The théorème final

Soit X un code sur A.

Théorème

X complet $\iff$ X dense ou maximal.

Preuve :

- Si X est maximal, X est complet.
  Si X est dense, X est complet.
- Si X est complet et maigre,
  - X est un code $\Rightarrow \pi(X) \leq 1$;
  - X est maigre complet $\Rightarrow \pi(X) \geq 1$.

  $\Rightarrow \pi(X) = 1$ et X est maximal.

$\square$