Théorie des codes

Nicolas Daviaud

19 janvier 2011

Plan

Plan

Définitions générales

Définition

Un *monoïde* est un ensemble non vide muni d'une LCI associative.

Si A est un alphabet, (A^*, concat) est un monoïde libre.

Définition

Un partie X de A^* est un *code* si elle est la base d'un monoïde libre.
On appelle (ici) *lexème* les éléments d'un code.
Un code est dit *maximal* s'il n'admet pas de surcode strict.

Définitions générales

Définition

Un *monoïde* est un ensemble non vide muni d'une LCI associative.

Si A est un alphabet, (A^*, concat) est un monoïde libre.

Définition

Un partie X de A^* est un *code* si elle est la base d'un monoïde libre.
On appelle (ici) *lexème* les éléments d'un code.
Un code est dit *maximal* s'il n'admet pas de surcode strict.

Plan

1. Définitions générales
2. Mesure
   - Distribution de Bernoulli
   - Caractérisation d'un code
3. Densité
   - Définitions
   - Propriétés
4. Théorème

Distribution de Bernoulli

Définition

Une *distribution de Bernoulli* est un morphisme de monoïde de A^* dans $(\mathbb{R}_+, \times)$ qui vérifie la relation

$$\sum_{a \in A} \pi(a) = 1.$$

Elle est *strictement positive* si $\forall a \in A, \pi(a) > 0$.

On l'étend π à $\mathscr{P}(A^*)$ en posant

$$\forall L \subset A^*, \pi(L) = \sum_{l \in L} \pi(l).$$

Proposition

π est une mesure positive sur $(A^*, \mathscr{P}(A^*))$.

Distribution de Bernoulli

Définition

Une *distribution de Bernoulli* est un morphisme de monoïde de A^* dans $(\mathbb{R}_+, \times)$ qui vérifie la relation

$$\sum_{a \in A} \pi(a) = 1.$$

Elle est *strictement positive* si $\forall a \in A, \pi(a) > 0$.

On l'étend π à $\mathscr{P}(A^*)$ en posant

$$\forall L \subset A^*, \pi(L) = \sum_{l \in L} \pi(l).$$

Proposition

π est une mesure positive sur $(A^*, \mathscr{P}(A^*))$.

Distribution de Bernoulli

Définition

Une *distribution de Bernoulli* est un morphisme de monoïde de A^* dans $(\mathbb{R}_+, \times)$ qui vérifie la relation

$$\sum_{a \in A} \pi(a) = 1.$$

Elle est *strictement positive* si $\forall a \in A, \pi(a) > 0$.

On l'étend π à $\mathscr{P}(A^*)$ en posant

$$\forall L \subset A^*, \pi(L) = \sum_{l \in L} \pi(l).$$

Proposition

π est une mesure positive sur $(A^*, \mathscr{P}(A^*))$.

Caractérisation d'un code

Proposition

Si X est un code sur A, alors

- $\forall n, \pi\left(X^n\right) = \pi(X)^n$
- *toute distribution de Bernoulli π sur A^* vérifie $\pi(X) \leq 1$.*

Sachant que $\pi(A) = 1$, un code n'est donc pas très gros.

Proposition

Soit X un code sur A. S'il existe une distribution de Bernoulli strictement positive sur A^* telle que $\pi(X) = 1$ alors X est un code maximal.

Caractérisation d'un code

Proposition

Si X est un code sur A, alors

- $\forall n, \pi\left(X^n\right) = \pi(X)^n$
- *toute distribution de Bernoulli π sur A^* vérifie $\pi(X) \leq 1$.*

Sachant que $\pi(A) = 1$, un code n'est donc pas très gros.

Proposition

Soit X un code sur A. S'il existe une distribution de Bernoulli strictement positive sur A^* telle que $\pi(X) = 1$ alors X est un code maximal.

Plan

Définitions

Définition

1. Un sous-ensemble P d'un monoïde M est dit *dense* dans M si pour tout élément m de M
$$\exists u, v \in M : umv \in P$$
Un sous-ensemble d'un monoïde est dit mince ("thin" dans le texte) s'il n'est pas dense.
2. Un sous-ensemble P de M est dit *complet* (dans M) si le monoïde engendré par P est dense dans M.

N.B. : "mince" et "complet" ne sont pas contradictoires.

Définitions

Définition

1. Un sous-ensemble P d'un monoïde M est dit *dense* dans M si pour tout élément m de M
$$\exists u, v \in M : umv \in P$$
Un sous-ensemble d'un monoïde est dit mince ("thin" dans le texte) s'il n'est pas dense.
2. Un sous-ensemble P de M est dit *complet* (dans M) si le monoïde engendré par P est dense dans M.

N.B. : "mince" et "complet" ne sont pas contradictoires.

Propriétés

Proposition

Tout code est inclus dans un code complet.

Proposition

Un code maximal est complet.

Proposition

Soit X un sous-ensemble mince et complet de A^*. Pour toute distribution de Bernoulli π strictement positive, on a

$$\pi(X) \geq 1.$$

Propriétés

Proposition

Tout code est inclus dans un code complet.

Proposition

Un code maximal est complet.

Proposition

Soit X un sous-ensemble mince et complet de A^*. Pour toute distribution de Bernoulli π strictement positive, on a

$$\pi(X) \geq 1.$$

Propriétés

Proposition

Tout code est inclus dans un code complet.

Proposition

Un code maximal est complet.

Proposition

Soit X un sous-ensemble mince et complet de A^*. Pour toute distribution de Bernoulli π strictement positive, on a

$$\pi(X) \geq 1.$$

Plan

Gros théorème sur les codes minces

Théorème

Soit X un code mince. Sont équivalentes :

(i) *X est un code maximal.*

(ii) *Il existe une distribution de Bernoulli définie positive π telle que $\pi(X) = 1$.*

(iii) *Toute distribution de Bernoulli définie positive π vérifie $\pi(X) = 1$.*

(iv) *X est complet.*