Codes pour les nuls

ou

A-t-on vraiment besoin d'espaces?

Francesco Dolce

LaCIM UQÀM

12 juin 2018

Séminaire étudiant

juliemangeunepomme

monpayscenestpasunpays

ilestlouis

quelquebec ?

Julie mange une pomme

monpayscenestpasunpays

ilestlouis

quelquebec ?

Julie mange une pomme

Mon pays, ce n'est pas un pays

ilestlouis

quelquebec ?

Julie mange une pomme

Mon pays, ce n'est pas un pays

Il est Louis ou Île St. Louis

quelquebec ?

Julie mange une pomme

Mon pays, ce n'est pas un pays

Il est Louis ou Île St. Louis

Quel Québec ? ou Quelque bec ?

Quelques mots sur les mots

A *alphabet*

ex.
$A = \{a, b, c\}$

Quelques mots sur les mots

A *alphabet*

ex.

$A = \{a, b, c\}$

A^+ *semigroupe libre*

ex.

$u = aac, \quad v = bc \ \in A$

Quelques mots sur les mots

A *alphabet*

ex.
$A = \{a, b, c\}$

A^+ *semigroupe libre*

ex.
$u = aac, \quad v = bc \ \in A$
$aac.bc = u.v \neq v.u = bc.aac$

Quelques mots sur les mots

A *alphabet* — ex. $A = \{a, b, c\}$

A^+ *semigroupe libre* — ex. $u = aac, \quad v = bc \ \in A$

$aac.bc = u.v \neq v.u = bc.aac$

$A^* = A^+ \cup \{\varepsilon\}$ *monoïde libre* — ex. $u.\varepsilon = u = \varepsilon.u$

Quelques mots sur les mots

A *alphabet*

ex.
$A = \{a, b, c\}$

A^+ *semigroupe libre*

ex.
$u = aac, \quad v = bc \ \in A$
$aac.bc = u.v \neq v.u = bc.aac$

$A^* = A^+ \cup \{\varepsilon\}$ *monoïde libre*

ex.
$u.\varepsilon = u = \varepsilon.u$

$|u|$ *longueur* de u

ex.
$|aac| = 3, \quad |bc| = 2$

Quelques mots sur les mots

A *alphabet*

ex.
$A = \{a, b, c\}$

A^+ *semigroupe libre*

ex.
$u = aac, \quad v = bc \ \in A$
$aac.bc = u.v \neq v.u = bc.aac$

$A^* = A^+ \cup \{\varepsilon\}$ *monoïde libre*

ex.
$u.\varepsilon = u = \varepsilon.u$

$|u|$ *longueur* de u

ex.
$|aac| = 3, \quad |bc| = 2$
$|uv| = |u| + |v| = |vu|$

Quelques mots sur les mots

A *alphabet*

ex.
$A = \{a, b, c\}$

A^+ *semigroupe libre*

ex.
$u = aac, \quad v = bc \ \in A$
$aac.bc = u.v \neq v.u = bc.aac$

$A^* = A^+ \cup \{\varepsilon\}$ *monoïde libre*

ex.
$u.\varepsilon = u = \varepsilon.u$

$|u|$ *longueur* de u

ex.
$|aac| = 3, \quad |bc| = 2$
$|uv| = |u| + |v| = |vu|$
$|\varepsilon| = 0$

Quelques mots sur les mots

A *alphabet*

ex.
$A = \{a, b, c\}$

A^+ *semigroupe libre*

ex.
$u = aac, \quad v = bc \ \in A$
$aac.bc = u.v \neq v.u = bc.aac$

$A^* = A^+ \cup \{\varepsilon\}$ *monoïde libre*

ex.
$u.\varepsilon = u = \varepsilon.u$

$|u|$ *longueur* de u

ex.
$|aac| = 3, \quad |bc| = 2$
$|uv| = |u| + |v| = |vu|$
$|\varepsilon| = 0$

$S \subseteq A^*$

ex.
$S = \{a, b, ac, baa, abcba\}$

Codes

$X \subset A^+$ est un *code* sur A si $\quad \forall \; m, n \geq 0$

$\forall \; x_1, x_2, \ldots, x_n, \; y_1, y_2, \ldots, y_m \in X$

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m \quad \Longrightarrow \quad \begin{cases} n = m \\ x_i = y_i \;\; \forall \; i = 1, 2, \ldots, n \end{cases}$$

Codes

$X \subset A^+$ est un *code* sur A si $\quad \forall \; m, n \geq 0$

$\forall \; x_1, x_2, \ldots, x_n, \; y_1, y_2, \ldots, y_m \in X$

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m \quad \Longrightarrow \quad \begin{cases} n = m \\ x_i = y_i \;\; \forall \; i = 1, 2, \ldots, n \end{cases}$$

Exemples

- $X_1 = \{a, ab, ba\}$ n'est pas un code, car $aba = a.ba = ab.a$.

Codes

$X \subset A^+$ est un *code* sur A si $\forall\ m, n \geq 0$

$\forall\ x_1, x_2, \ldots, x_n,\ y_1, y_2, \ldots, y_m \in X$

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m \quad \Longrightarrow \quad \begin{cases} n = m \\ x_i = y_i \ \ \forall\ i = 1, 2, \ldots, n \end{cases}$$

Exemples

- $X_1 = \{a, ab, ba\}$ n'est pas un code, car $aba = a.ba = ab.a$.
- $X_2 = \{aa, baa, ba\}$ est un code (ex. $baaaaa = ba.aa.aa$).

Codes

$X \subset A^+$ est un *code* sur A si $\forall\ m, n \geq 0$
$\forall\ x_1, x_2, \dots, x_n,\ y_1, y_2, \dots, y_m \in X$

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m \implies \begin{cases} n = m \\ x_i = y_i \ \ \forall\ i = 1, 2, \dots, n \end{cases}$$

Exemples

- $X_1 = \{a, ab, ba\}$ n'est pas un code, car $aba = a.ba = ab.a$.
- $X_2 = \{aa, baa, ba\}$ est un code (ex. $baaaaa = ba.aa.aa$).

Proposition

Si $X \subset A^+$ est un code, alors toute bijection $B \leftrightarrow X$ s'étend à un morphisme $B^* \hookrightarrow A^*$.

Codes

$X \subset A^+$ est un *code* sur A si $\forall \; m, n \geq 0$
$\forall \; x_1, x_2, \ldots, x_n, \; y_1, y_2, \ldots, y_m \in X$

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m \quad \Longrightarrow \quad \begin{cases} n = m \\ x_i = y_i \;\; \forall \, i = 1, 2, \ldots, n \end{cases}$$

Exemples

- $X_1 = \{a, ab, ba\}$ n'est pas un code, car $aba = a.ba = ab.a$.
- $X_2 = \{aa, baa, ba\}$ est un code (ex. $baaaaa = ba.aa.aa$).

Proposition

Si $X \subset A^+$ est un code, alors toute bijection $B \leftrightarrow X$ s'étend à un morphisme $B^* \hookrightarrow A^*$.
S'il existe un morphisme $\beta : B^* \hookrightarrow A^*$ alors $\beta(B)$ est un code.

Codes

$X \subset A^+$ est un *code* sur A si $\quad \forall \; m, n \geq 0$
$\forall \; x_1, x_2, \ldots, x_n, \; y_1, y_2, \ldots, y_m \in X$

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_m \quad \Longrightarrow \quad \begin{cases} n = m \\ x_i = y_i \;\; \forall \; i = 1, 2, \ldots, n \end{cases}$$

Exemples

- $X_1 = \{a, ab, ba\}$ n'est pas un code, car $aba = a.ba = ab.a$.
- $X_2 = \{aa, baa, ba\}$ est un code (ex. $baaaaa = ba.aa.aa$).

Proposition

Si $X \subset A^+$ est un code, alors toute bijection $B \leftrightarrow X$ s'étend à un morphisme $B^* \hookrightarrow A^*$.
S'il existe un morphisme $\beta : B^* \hookrightarrow A^*$ alors $\beta(B)$ est un code.

Un tel β est dit un *morphisme de codage* pour X.

Codes uniformes

$A^n = \{u \in A^* \mid |u| = n\}$ est dit le *code uniforme* (de degre n).

Codes uniformes

$A^n = \{u \in A^* \mid |u| = n\}$ est dit le *code uniforme* (de degre n).

Exemples

- $A^2 = \{aa, ab, ba, bb\}$
  ex. $ab.aa.ba.bb.ab$, $bb.bb$, $ab.aa$

Codes uniformes

$A^n = \{u \in A^* \mid |u| = n\}$ est dit le *code uniforme* (de degre n).

Exemples

- $A^2 = \{aa, ab, ba, bb\}$
  ex. $ab.aa.ba.bb.ab$, $bb.bb$, $ab.aa$
- $\{aaa, aba, bab\} \subset A^3$ est un code
  ex. $aba.aaa.aaa.bab$

Codes uniformes

$A^n = \{u \in A^* \mid |u| = n\}$ est dit le *code uniforme* (de degre n).

Exemples

- $A^2 = \{aa, ab, ba, bb\}$
  ex. $ab.aa.ba.bb.ab$, $bb.bb$, $ab.aa$
- $\{aaa, aba, bab\} \subset A^3$ est un code
  ex. $aba.aaa.aaa.bab$

Exemple

00010101 01011101 10101000 00110101 10101010 00101010 10111010 10000101
01011010 10100101 00101000 01101011 10101000 10101000 10101110 01101011
00101111 01010101 11111111 01010000 11110101 01001010 00011101 01011111
01010101 00100010 01010110 11111000 00010100 10101001 01101011 11110101
01010101 00000101 11100110 00110011 00011000 11001100 01100011 00000000

Codes préfixes, suffixes et bifixes

$X \subset A^+$ est *préfixe* (résp. *suffixe*) si aucun élément de X est un préfixe (résp. suffixe) propre d'un autre élément de X.

X est *bifixe* s'il est à la fois préfixe et suffixe.

Exemple

- $\{aa, ab, ba\}$
- $\{aa, ab, bba, bbb\}$
- $\{ac, bcc, bcbca\}$
- { ici, icitte, là }
- { bec, bise, Québec }
- { tu-veux, veux-tu, tu-veux-tu }

Codes préfixes, suffixes et bifixes

$X \subset A^+$ est *préfixe* (résp. *suffixe*) si aucun élément de X est un préfixe (résp. suffixe) propre d'un autre élément de X.

X est *bifixe* s'il est à la fois préfixe et suffixe.

Exemple

- $\{aa, ab, ba\}$
- $\{aa, ab, bba, bbb\}$
- $\{ac, bcc, bcbca\}$
- $\{a^n b^n \mid n \geq 0\}$
- $b \cup ab^*a = \{b\} \cup \{ab^n a \mid n \geq 0\}$
- { ici, icitte, là }
- { bec, bise, Québec }
- { tu-veux, veux-tu, tu-veux-tu }
- $a^* b = \{a^n b \mid n \geq 0\}$

Codes préfixes, suffixes et bifixes

$X \subset A^+$ est *préfixe* (résp. *suffixe*) si aucun élément de X est un préfixe (résp. suffixe) propre d'un autre élément de X.

X est *bifixe* s'il est à la fois préfixe et suffixe.

Exemple

- $\{aa, ab, ba\}$
- $\{aa, ab, bba, bbb\}$
- $\{ac, bcc, bcbca\}$
- $\{a^n b^n \mid n \geq 0\}$
- $b \cup ab^*a = \{b\} \cup \{ab^n a \mid n \geq 0\}$
- { ici, icitte, là }
- { bec, bise, Québec }
- { tu-veux, veux-tu, tu-veux-tu }
- $a^*b = \{a^n b \mid n \geq 0\}$

Proposition

Tout $X \subset A^+$ préfixe (resp. suffixe, bifixe) est un code.

Codes sémaphores

$\bullet\bullet\bullet-\ \ \bullet\bullet\ \ \bullet\bullet\bullet-\ \ \bullet\qquad \bullet-\bullet\bullet\ \ \bullet-\qquad \bullet--\bullet\ \ ---\ \ \bullet\bullet-\ \ -\ \ \bullet\bullet\ \ \bullet-\ \ \bullet$

Codes sémaphores

●●●— ●● ●●●— ● ●—●● ●— ●——● ——— ●●— — ●● ●— ●

$A = \{\bullet, -, \textvisiblespace\}, \quad X \subset A^{+}$

●—␣	●●●●␣	———␣	●●●—␣
—●●●␣	●●␣	●——●␣	●——␣
—●—●␣	●———␣	——●—␣	—●●—␣
—●●␣	—●—␣	●—●␣	—●——␣
●␣	●—●●␣	●●●␣	——●●␣
●●—●␣	——␣	—␣	
——●␣	●—␣	●●—␣	

Codes sémaphores

• • • –   • •   • • • –   •   • – • •   • –   • – – •   – – –   • • –   –   • •   • –   •

$A = \{\bullet, -, \text{␣}\}$, $X \subset A^+$ $B = \{\mathbf{A}, \mathbf{B}, \ldots, \mathbf{Z}\} \leftrightarrow X$, $\beta : B^* \hookrightarrow A^*$

A $\mapsto$ • – ␣	**H** $\mapsto$ • • • • ␣	**O** $\mapsto$ – – –␣	**V** $\mapsto$ • • • – ␣
B $\mapsto$ – • • • ␣	**I** $\mapsto$ • • ␣	**P** $\mapsto$ • – – • ␣	**W** $\mapsto$ • – –␣
C $\mapsto$ – • – • ␣	**J** $\mapsto$ • – – – ␣	**Q** $\mapsto$ – – • – ␣	**X** $\mapsto$ – • • – ␣
D $\mapsto$ – • •␣	**K** $\mapsto$ – • –␣	**R** $\mapsto$ • – •␣	**Y** $\mapsto$ – • – – ␣
E $\mapsto$ •␣	**L** $\mapsto$ • – • • ␣	**S** $\mapsto$ • • •␣	**Z** $\mapsto$ – – • • ␣
F $\mapsto$ • • – • ␣	**M** $\mapsto$ – – ␣	**T** $\mapsto$ –␣	
G $\mapsto$ – – •␣	**N** $\mapsto$ • – ␣	**U** $\mapsto$ • • –␣	

Codes maximaux

Un code $X \subset A^+$ est *maximal* sur A si

$$\left.\begin{array}{c} X \subset Y \\ Y \text{ code sur } \mathsf{A} \end{array}\right\} \implies X = Y$$

Codes maximaux

Un code $X \subset A^+$ est *maximal* sur A si

$$\left.\begin{array}{c} X \subset Y \\ Y \text{ code sur A} \end{array}\right\} \implies X = Y$$

Exemple

A^n est un code maximal sur A.

Codes maximaux

Un code $X \subset A^+$ est *maximal* sur A si

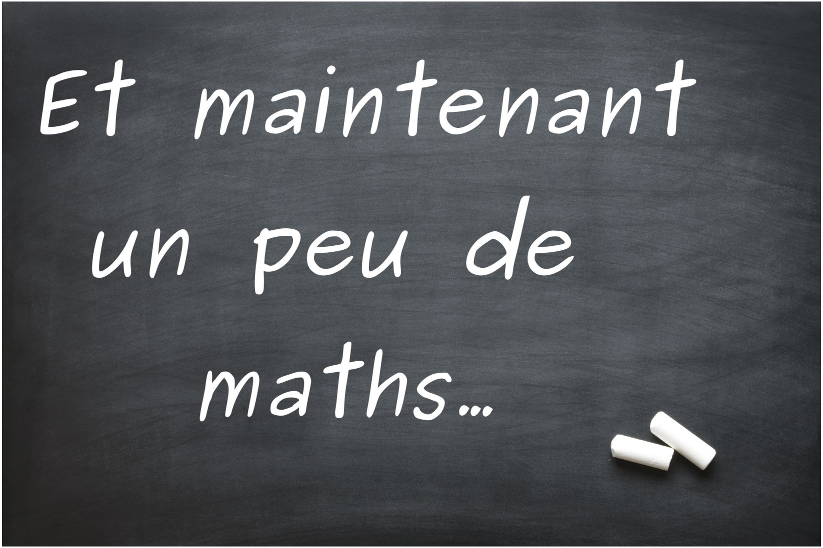
$$\left.\begin{array}{c} X \subset Y \\ Y \text{ code sur A} \end{array}\right\} \quad \Longrightarrow \quad X = Y$$

Exemple

A^n est un code maximal sur A.

Proposition

Tout code $X \subset A^+$ est contenu dans un code maximal sur A.


Et maintenant
un peu de
maths...

Proposition 1.
(2) $\beta : B^* \hookrightarrow A^* \implies \beta(B)$ **code.**

Proposition 1.
(2) $\beta : B^* \hookrightarrow A^* \implies \beta(B)$ **code.**

Proposition 2.
X_M **unique partie génératrice minimale de** M.

Proposition 1.

(2) $\beta : B^* \hookrightarrow A^* \quad \Longrightarrow \quad \beta(B)$ **code.**

Proposition 2.

X_M **unique partie génératrice minimale de** M.

Proposition 3.

(1) M **libre** $\quad \Longrightarrow \quad X_M$ **code**

(2) $X \subset A^*$ **code** $\quad \Longrightarrow \quad X^*$ **libre et** X **sa partie génératrice minimale**

Proposition 1.
(2) $\beta : B^* \hookrightarrow A^* \quad \Longrightarrow \quad \beta(B)$ **code.**

Proposition 2.
X_M **unique partie génératrice minimale de** M.

Proposition 3.
(1) M **libre** $\quad \Longrightarrow \quad X_M$ **code**
(2) $X \subset A^*$ **code** $\quad \Longrightarrow \quad X^*$ **libre et** X **sa partie génératrice minimale**

Corollaire.
X, Y **codes avec** $X^* = Y^* \quad \Longrightarrow \quad X = Y$

Proposition 1.
(2) $\beta : B^* \hookrightarrow A^* \implies \beta(B)$ **code.**

Proposition 2.
X_M **unique partie génératrice minimale de** M.

Proposition 3.
(1) M **libre** $\implies X_M$ **code**
(2) $X \subset A^*$ **code** $\implies X^*$ **libre et** X **sa partie génératrice minimale**

Corollaire.
X, Y **codes avec** $X^* = Y^* \implies X = Y$

Proposition 4.
N **stable** $\iff N$ **libre**

Proposition 1.

(2) $\beta : B^* \hookrightarrow A^* \implies \beta(B)$ **code.**

Proposition 2.

X_M **unique partie génératrice minimale de** M.

Proposition 3.

(1) M **libre** $\implies X_M$ **code**

(2) $X \subset A^*$ **code** $\implies X^*$ **libre et** X **sa partie génératrice minimale**

Corollaire.

X, Y **codes avec** $X^* = Y^* \implies X = Y$

Proposition 4.

N **stable** $\iff N$ **libre**

Proposition 5.

M **unitaire à droite** $\iff X_M$ **code préfixe**

Proposition 1.
(2) $\beta : B^* \hookrightarrow A^* \implies \beta(B)$ **code.**

Proposition 2.
X_M **unique partie génératrice minimale de** M.

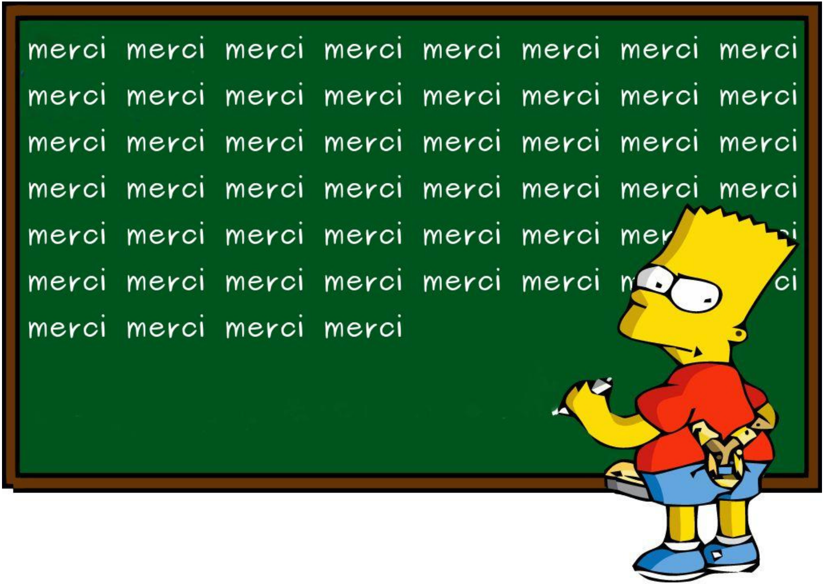
Proposition 3.
(1) M **libre** $\implies X_M$ **code**
(2) $X \subset A^*$ **code** $\implies X^*$ **libre et** X **sa partie génératrice minimale**

Corollaire.
X, Y **codes avec** $X^* = Y^* \implies X = Y$

Proposition 4.
N **stable** $\iff N$ **libre**

Proposition 5.
M **unitaire à droite** $\iff X_M$ **code préfixe**

Proposition 6.
M **libre maximal** $\implies X_M$ **code maximal**


merci merci merci merci merci merci merci merci
merci merci merci merci merci merci merci merci
merci merci merci merci merci merci merci merci
merci merci merci merci merci merci merci merci
merci merci merci merci merci merci
merci merci merci merci merci merci
merci merci merci merci