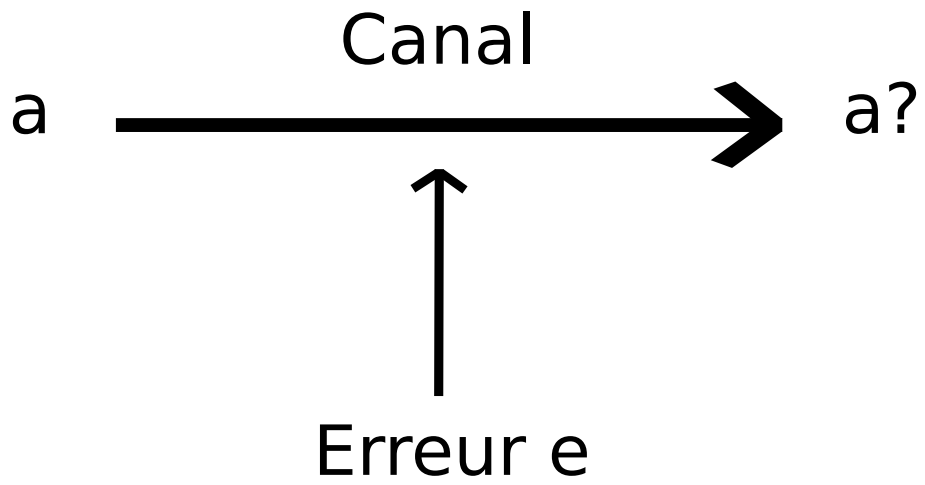
$1 + 1 = 0$ ou comment corriger les erreurs

Nicolas Billerey

Laboratoire de Mathématiques
Université Blaise Pascal – Clermont-Ferrand 2

Journée IREM – Vendredi 7 octobre 2016

Canal imparfait



Sommaire

Arithmétique modulo 2

On note $\mathbf{F}_2$ l'ensemble $\{0, 1\}$ muni des deux lois d'addition et de multiplication suivantes

Arithmétique modulo 2

On note $\mathbf{F}_2$ l'ensemble $\{0, 1\}$ muni des deux lois d'addition et de multiplication suivantes

$\times$	0	1
0	0	0
1	0	1

Arithmétique modulo 2

On note $\mathbf{F}_2$ l'ensemble $\{0, 1\}$ muni des deux lois d'addition et de multiplication suivantes

$\times$	0	1
0	0	0
1	0	1

$+$	0	1
0	0	1
1	1	0

Arithmétique modulo 2

On note $\mathbf{F}_2$ l'ensemble $\{0, 1\}$ muni des deux lois d'addition et de multiplication suivantes

$\times$	0	1
0	0	0
1	0	1

$+$	0	1
0	0	1
1	1	0

- L'ensemble $\mathbf{F}_2$ ainsi construit est un *corps*.

Arithmétique modulo 2

On note $\mathbf{F}_2$ l'ensemble $\{0, 1\}$ muni des deux lois d'addition et de multiplication suivantes

$\times$	0	1
0	0	0
1	0	1

$+$	0	1
0	0	1
1	1	0

- L'ensemble $\mathbf{F}_2$ ainsi construit est un *corps*.
- Un élément de l'ensemble $\mathbf{F}_2$ s'appelle un *bit*.

Arithmétique modulo 2

On note $\mathbf{F}_2$ l'ensemble $\{0, 1\}$ muni des deux lois d'addition et de multiplication suivantes

$\times$	0	1
0	0	0
1	0	1

$+$	0	1
0	0	1
1	1	0

- L'ensemble $\mathbf{F}_2$ ainsi construit est un *corps*.
- Un élément de l'ensemble $\mathbf{F}_2$ s'appelle un *bit*.
- Une suite de bits s'appelle un *mot* (binaire).

Un intérêt pratique

Les bits forment les briques du langage des ordinateurs :

Un intérêt pratique

Les bits forment les briques du langage des ordinateurs :
$0 \leftrightarrow$ le circuit est ouvert (le courant ne passe pas)

Un intérêt pratique

Les bits forment les briques du langage des ordinateurs :
$0 \leftrightarrow$ le circuit est ouvert (le courant ne passe pas)
$1 \leftrightarrow$ le circuit est fermé (le courant passe)

La représentation ASCII

- On dispose de 128 caractères (caractères latins, chiffres, signes de ponctuation, etc) :

La représentation ASCII

- On dispose de 128 caractères (caractères latins, chiffres, signes de ponctuation, etc) :

```
 !"#$%&'()*+,-./
0123456789:;<=>?
@ABCDEFGHIJKLMNO
PQRSTUVWXYZ[\]^_
`abcdefghijklmno
pqrstuvwxyz{|}~
```

La représentation ASCII

- On dispose de 128 caractères (caractères latins, chiffres, signes de ponctuation, etc) :

```
 !"#$%&'()*+,-./
0123456789:;<=>?
@ABCDEFGHIJKLMNO
PQRSTUVWXYZ[\]^_
`abcdefghijklmno
pqrstuvwxyz{|}~
```

- Chaque caractère est représenté par un mot de 7 bits.

La représentation ASCII

- On dispose de 128 caractères (caractères latins, chiffres, signes de ponctuation, etc) :

```
 !"#$%&'()*+,-./
0123456789:;<=>?
@ABCDEFGHIJKLMNO
PQRSTUVWXYZ[\]^_
`abcdefghijklmno
pqrstuvwxyz{|}~
```

- Chaque caractère est représenté par un mot de 7 bits.
- Par exemple, a correspond à 1100001, et 1111000 à x.

Sommaire

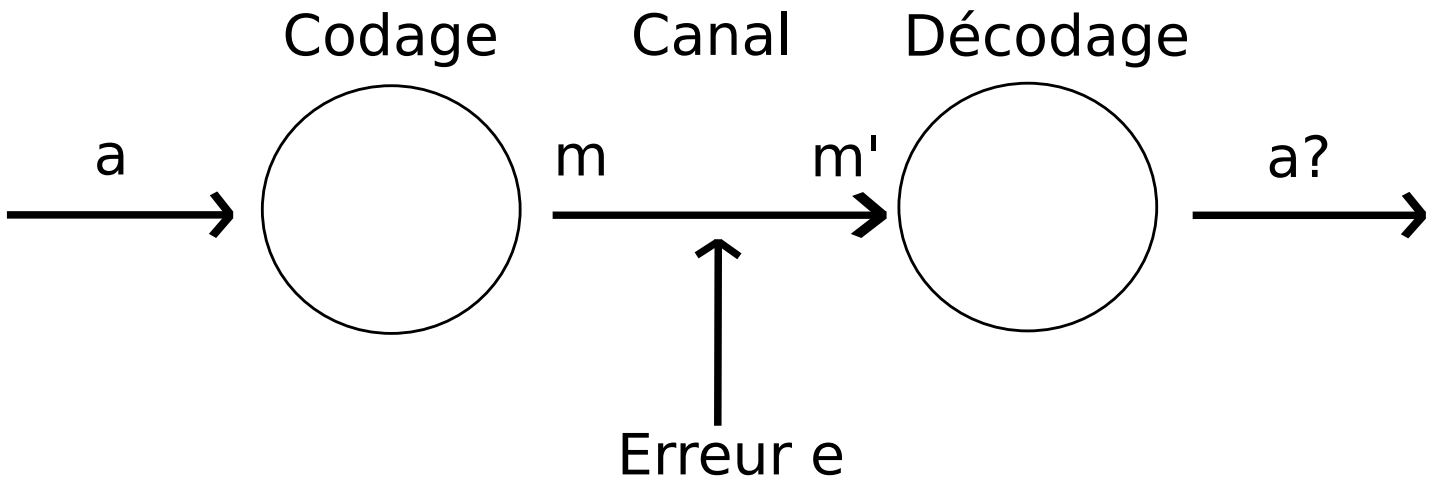
Comment faire ?

Comment faire ?

Il faut ajouter de la redondance...

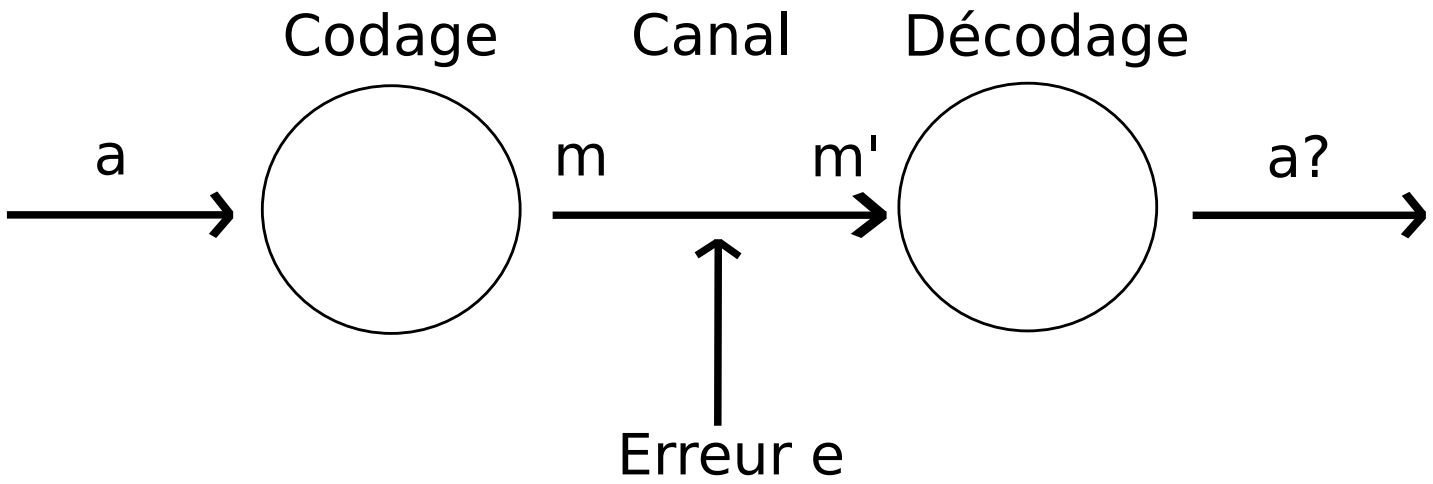
Comment faire ?

Il faut ajouter de la redondance...



Comment faire ?

Il faut ajouter de la redondance... mais pas trop !



Code de parité : définition

- mot de 7 bits $\rightsquigarrow$ mot de 8 bits (=octet).

Code de parité : définition

- mot de 7 bits $\rightsquigarrow$ mot de 8 bits (=octet).
- Le 8-ième bit, appelé *bit de parité*, vaut

$$\begin{cases} 0 & \text{si le nombre de 1 du mot de 7 bits est pair} \\ 1 & \text{si le nombre de 1 du mot de 7 bits est impair} \end{cases}$$

Code de parité : définition

- mot de 7 bits $\rightsquigarrow$ mot de 8 bits (=octet).
- Le 8-ième bit, appelé *bit de parité*, vaut

$$\begin{cases} 0 & \text{si le nombre de 1 du mot de 7 bits est pair} \\ 1 & \text{si le nombre de 1 du mot de 7 bits est impair} \end{cases}$$

- Maintenant a est codé par 11000011 et x par 11110000

Code de parité et addition dans $\mathbf{F}_2$

Définition

On appelle *code de parité* l'ensemble des mots de 8 bits de la forme

$$b_1 b_2 b_3 b_4 b_5 b_6 b_7 (b_1 + b_2 + b_3 + b_4 + b_5 + b_6 + b_7)$$

où $b_i = 0$ ou 1 et l'addition est celle de $\mathbf{F}_2$.

Code de parité et addition dans $\mathbf{F}_2$

Définition

On appelle *code de parité* l'ensemble des mots de 8 bits de la forme

$$b_1 b_2 b_3 b_4 b_5 b_6 b_7 (b_1 + b_2 + b_3 + b_4 + b_5 + b_6 + b_7)$$

où $b_i = 0$ ou 1 et l'addition est celle de $\mathbf{F}_2$.

- 01101010, 10101010, 00001111 sont des éléments du code de parité.

Code de parité et addition dans $\mathbf{F}_2$

Définition

On appelle *code de parité* l'ensemble des mots de 8 bits de la forme

$$b_1 b_2 b_3 b_4 b_5 b_6 b_7 (b_1 + b_2 + b_3 + b_4 + b_5 + b_6 + b_7)$$

où $b_i = 0$ ou 1 et l'addition est celle de $\mathbf{F}_2$.

- 01101010, 10101010, 00001111 sont des éléments du code de parité.
- 00001110, 11000001, 01010111 ne le sont pas.

Code de parité et détection

Code de parité et détection

- Si on change 1 bit dans un octet du code de parité, le résultat n'est plus dans le code de parité (et vice-versa).

Code de parité et détection

- Si on change 1 bit dans un octet du code de parité, le résultat n'est plus dans le code de parité (et vice-versa).
- Le code de parité détecte donc 1 erreur, mais il ne la corrige pas.

Code de parité et détection

- Si on change 1 bit dans un octet du code de parité, le résultat n'est plus dans le code de parité (et vice-versa).
- Le code de parité détecte donc 1 erreur, mais il ne la corrige pas.
- On parle de *code détecteur*.

Le numéro INSEE

Le numéro INSEE

- Les deux derniers chiffres du numéro INSEE correspondent à la clé.

Le numéro INSEE

- Les deux derniers chiffres du numéro INSEE correspondent à la clé.
- La clé est définie par

$$97 - (\text{le reste de la division euclidienne de } N \text{ par } 97),$$

où N est le nombre formé des 13 premiers chiffres.

Comment corriger les erreurs trouvées ?

- Choisir un entier entre 0 et 15.

- Choisir un entier entre 0 et 15.
- Répondre aux sept questions suivantes. On a le droit de mentir au plus UNE fois.

- Choisir un entier entre 0 et 15.
- Répondre aux sept questions suivantes. On a le droit de mentir au plus UNE fois.

1. L'entier choisi est-il inférieur ou égal à 7 ?
2. L'entier choisi est-il dans l'ensemble $\{0, 1, 2, 3, 8, 9, 10, 11\}$?
3. L'entier choisi est-il dans l'ensemble $\{0, 1, 4, 5, 8, 9, 12, 13\}$?
4. L'entier choisi est-il pair ?
5. L'entier choisi est-il dans l'ensemble $\{0, 2, 5, 7, 9, 11, 12, 14\}$?
6. L'entier choisi est-il dans l'ensemble $\{0, 3, 4, 7, 9, 10, 13, 14\}$?
7. L'entier choisi est-il dans l'ensemble $\{0, 3, 5, 6, 8, 11, 13, 14\}$?

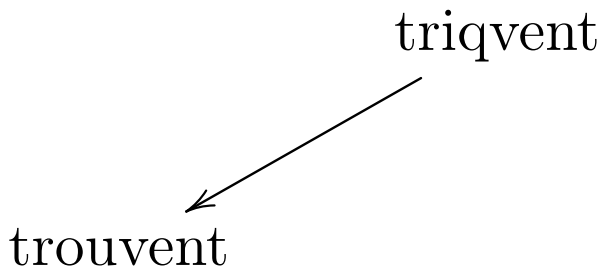
Sommaire

« Des chercheurs qui cherchent, on en trouve. Des chercheurs qui triqvent, on en cherche. »

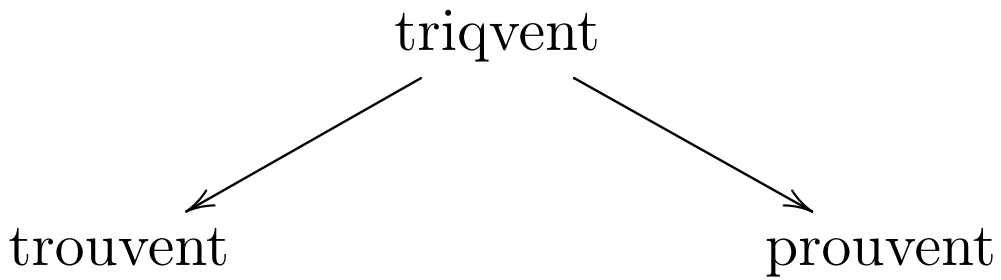
« Des chercheurs qui cherchent, on en trouve. Des chercheurs qui triqvent, on en cherche. »

triqvent

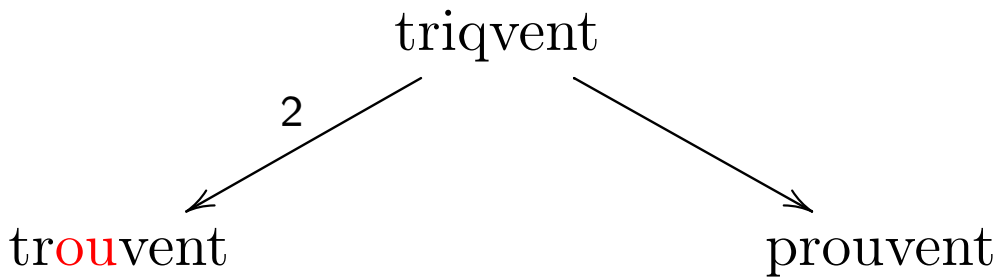
« Des chercheurs qui cherchent, on en trouve. Des chercheurs qui triqvent, on en cherche. »



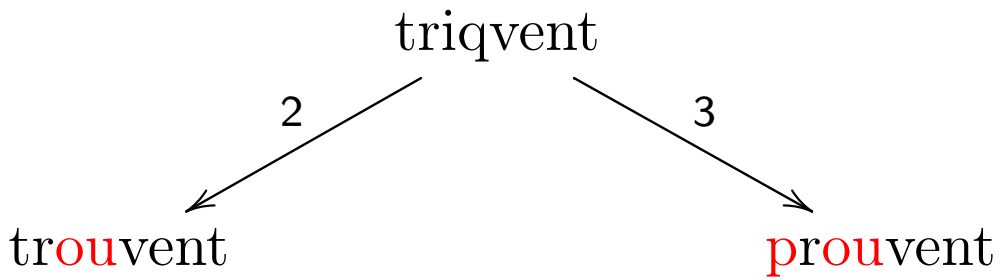
« Des chercheurs qui cherchent, on en trouve. Des chercheurs qui triqvent, on en cherche. »



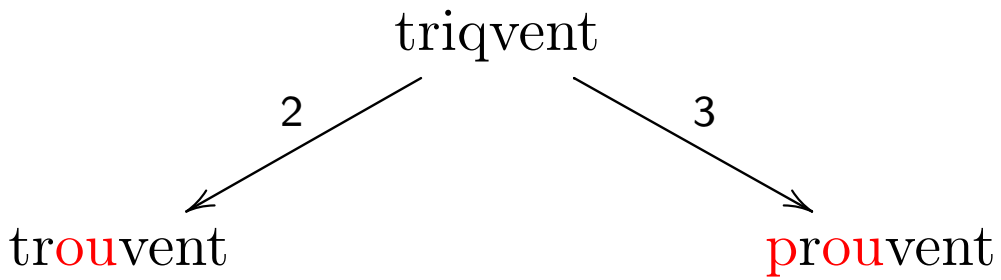
« Des chercheurs qui cherchent, on en trouve. Des chercheurs qui triqvent, on en cherche. »



« Des chercheurs qui cherchent, on en trouve. Des chercheurs qui triqvent, on en cherche. »



« Des chercheurs qui cherchent, on en trouve. Des chercheurs qui triqvent, on en cherche. »



On corrige au plus proche.

Une distance entre les mots binaires ?

Définition intuitive : pour m et m' deux mots de même longueur,

Une distance entre les mots binaires ?

Définition intuitive : pour m et m' deux mots de même longueur,

$$d(m, m') = \sharp\{\text{bits différents entre } m \text{ et } m'\}$$

Une distance entre les mots binaires ?

Définition intuitive : pour m et m' deux mots de même longueur,

$$d(m, m') = \sharp\{\text{bits différents entre } m \text{ et } m'\}$$

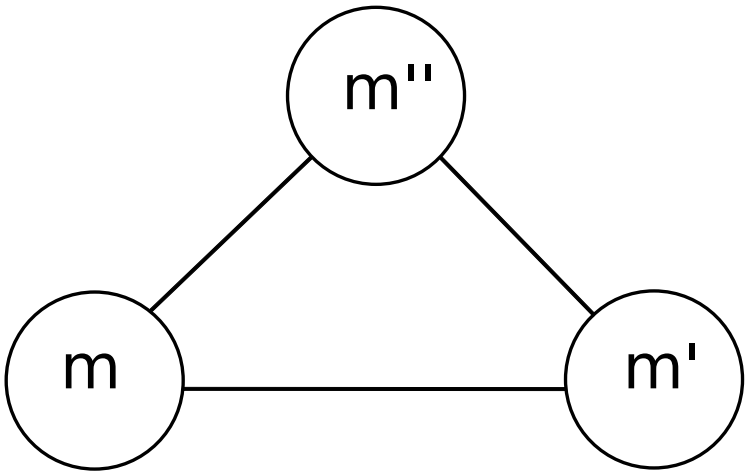
Propriétés élémentaires

$$d(m, m) = 0 \quad \text{et} \quad d(m, m') = d(m', m)$$

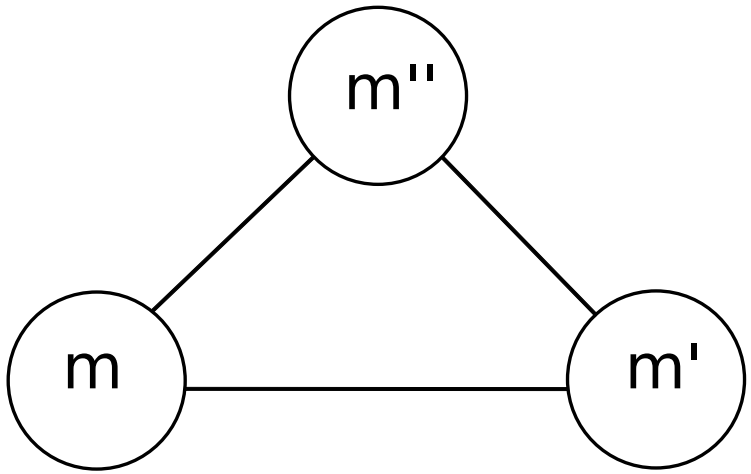
quels que soient m et m'.

L'inégalité triangulaire

L'inégalité triangulaire



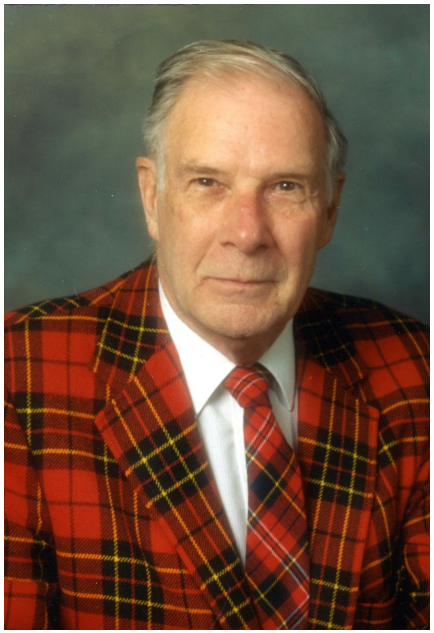
L'inégalité triangulaire



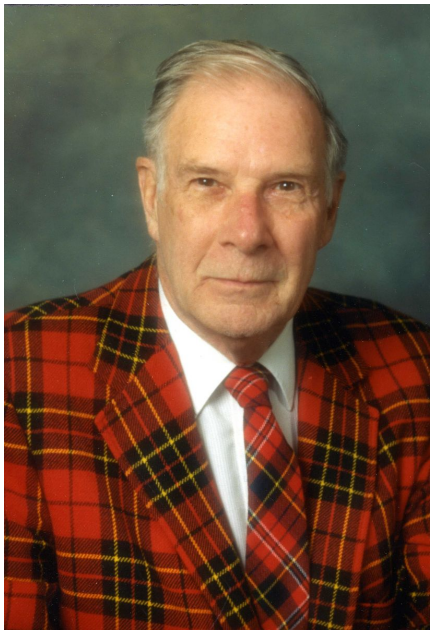
$$d(m, m') \leq d(m, m'') + d(m'', m')$$

Distance de Hamming et détection

Distance de Hamming et détection



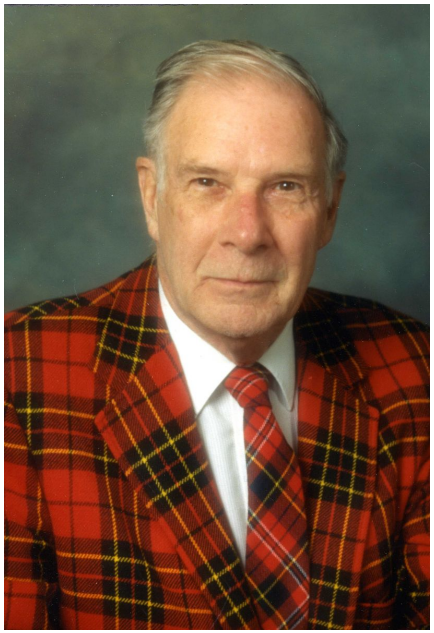
Distance de Hamming et détection



Définition

Un code est un ensemble de mots de même longueur. La longueur du code est la longueur des mots.

Distance de Hamming et détection



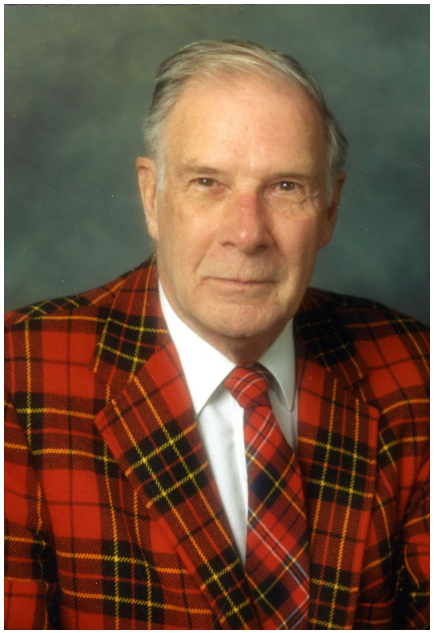
Définition

Un code est un ensemble de mots de même longueur. La longueur du code est la longueur des mots.

Définition

La distance de Hamming d_H d'un code est la distance minimale entre deux mots distincts du code.

Distance de Hamming et détection



Définition

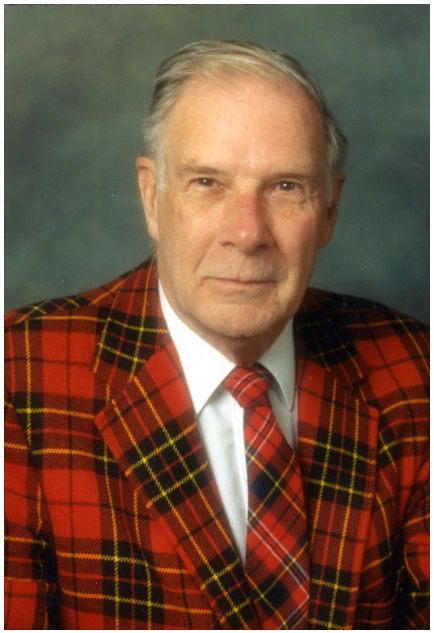
Un code est un ensemble de mots de même longueur. La longueur du code est la longueur des mots.

Définition

La distance de Hamming d_H d'un code est la distance minimale entre deux mots distincts du code.

- La distance de Hamming du code de parité est

Distance de Hamming et détection



Définition

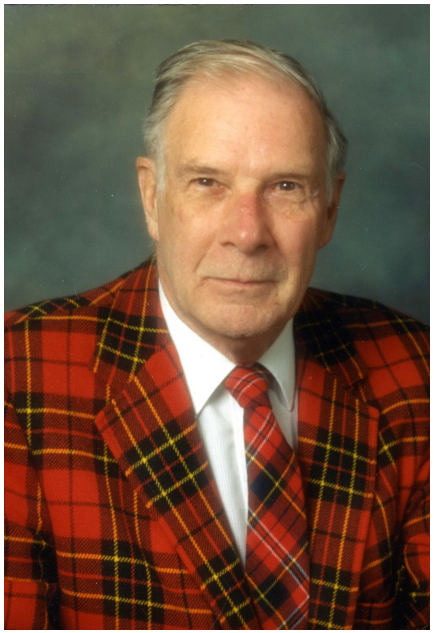
Un code est un ensemble de mots de même longueur. La longueur du code est la longueur des mots.

Définition

La distance de Hamming d_H d'un code est la distance minimale entre deux mots distincts du code.

- La distance de Hamming du code de parité est 2.

Distance de Hamming et détection



Définition

Un code est un ensemble de mots de même longueur. La longueur du code est la longueur des mots.

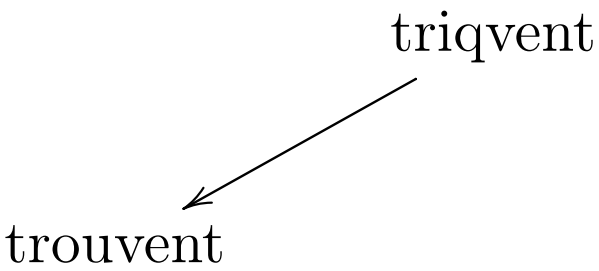
Définition

La distance de Hamming d_H d'un code est la distance minimale entre deux mots distincts du code.

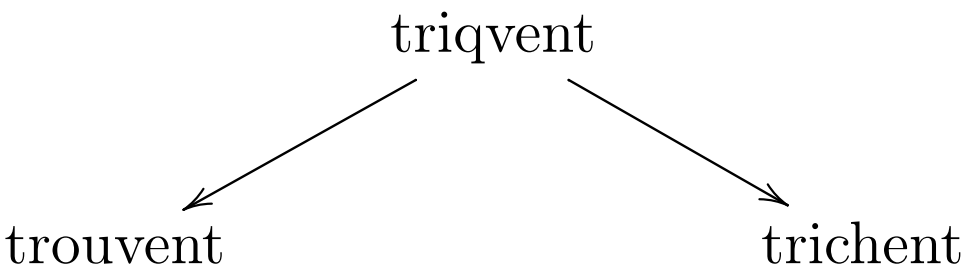
- La distance de Hamming du code de parité est 2.
- Un code de distance de Hamming d détecte $d-1$ erreurs.

Distance de Hamming et correction

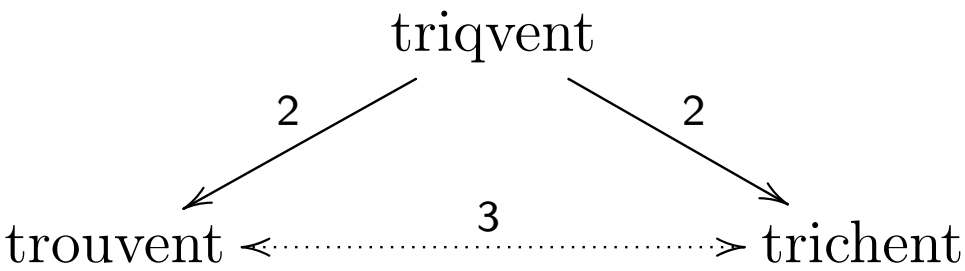
Distance de Hamming et correction



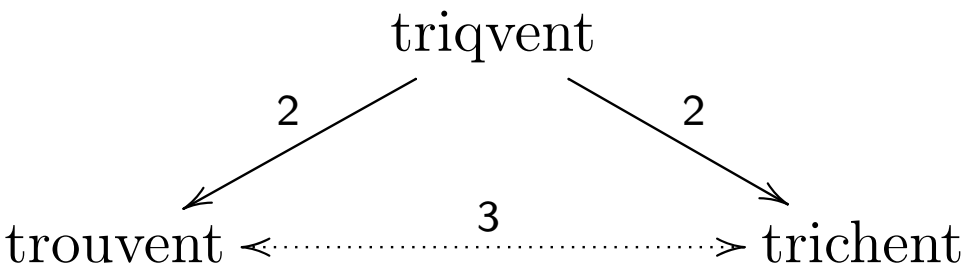
Distance de Hamming et correction



Distance de Hamming et correction

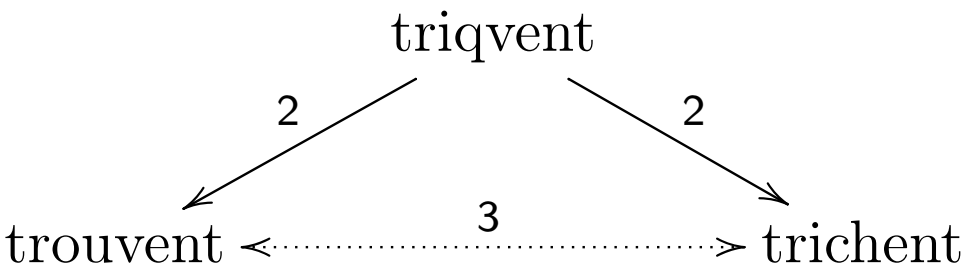


Distance de Hamming et correction



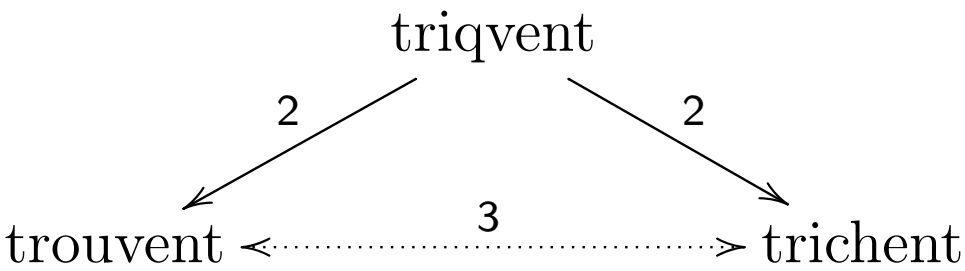
Lequel choisir ?

Distance de Hamming et correction



Lequel choisir ? On ne sait pas !

Distance de Hamming et correction



Lequel choisir ? On ne sait pas !

Définition

Un code C est dit t-correcteur s'il permet de corriger t erreurs, autrement dit, si pour tout mot m', il existe au plus un élément $m \in C$ tel que $d(m', m) \leq t$.

Distance de Hamming et correction (suite)

- Un code de distance de Hamming d est -correcteur.

Distance de Hamming et correction (suite)

- Un code de distance de Hamming d est $\left\lfloor \frac{d-1}{2} \right\rfloor$-correcteur.

Distance de Hamming et correction (suite)

- Un code de distance de Hamming d est $\left\lfloor \frac{d-1}{2} \right\rfloor$-correcteur.
- En particulier, un code de distance 3 corrige $\left\lfloor \frac{3-1}{2} \right\rfloor = 1$ erreur...

Le code de Hamming $[7, 4, 3]$

Le code de Hamming $[7, 4, 3]$ est le code de longueur 7 constitué des seize mots suivants :

$$0000000,\ 0001111,\ 0010011,\ 0011100,\ 0100101,$$

$$0101010,\ 0110110,\ 0111001,\ 1000110,\ 1001001,\ 1010101,$$

$$1011010,\ 1100011,\ 1101100,\ 1110000,\ 1111111$$

Le code de Hamming $[7, 4, 3]$

Le code de Hamming $[7, 4, 3]$ est le code de longueur 7 constitué des seize mots suivants :

$$0000000,\ 0001111,\ 0010011,\ 0011100,\ 0100101,$$

$$0101010,\ 0110110,\ 0111001,\ 1000110,\ 1001001,\ 1010101,$$

$$1011010,\ 1100011,\ 1101100,\ 1110000,\ 1111111$$

C'est l'ensemble des mots de la forme

$$b_1 b_2 b_3 b_4 (b_1 + b_2 + b_4)(b_1 + b_3 + b_4)(b_2 + b_3 + b_4)$$

avec $b_i = 0$ ou 1.

Le code de Hamming $[7, 4, 3]$ (suite)

Le code de Hamming $[7, 4, 3]$ correspond (bijectivement) à l'image de $\mathbf{F}_2^4$ par la matrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_{7,4}(\mathbf{F}_2)$$

Le code de Hamming $[7, 4, 3]$ (suite)

Le code de Hamming $[7, 4, 3]$ correspond (bijectivement) à l'image de $\mathbf{F}_2^4$ par la matrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_{7,4}(\mathbf{F}_2)$$

appelée matrice génératrice.

Le code de Hamming $[7, 4, 3]$ (suite)

Le code de Hamming $[7, 4, 3]$ correspond (bijectivement) à l'image de $\mathbf{F}_2^4$ par la matrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_{7,4}(\mathbf{F}_2)$$

appelée matrice génératrice. C'est donc un sous-espace vectoriel de dimension 4 de $\mathbf{F}_2^7$.

Le code de Hamming $[7, 4, 3]$ (suite)

Le code de Hamming $[7, 4, 3]$ correspond (bijectivement) à l'image de $\mathbf{F}_2^4$ par la matrice

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_{7,4}(\mathbf{F}_2)$$

appelée matrice génératrice. C'est donc un sous-espace vectoriel de dimension 4 de $\mathbf{F}_2^7$. Sa distance de Hamming vaut 3.

Le tour déjoué

Le tour déjoué

On a $\{0, \ldots, 15\} \overset{1:1}{\longleftrightarrow} \mathbf{F}_2^4$ par l'application qui à un entier N associe ses décimales (b_1, b_2, b_3, b_4) dans son écriture binaire :

Le tour déjoué

On a $\{0, \ldots, 15\} \overset{1:1}{\longleftrightarrow} \mathbf{F}_2^4$ par l'application qui à un entier N associe ses décimales (b_1, b_2, b_3, b_4) dans son écriture binaire :

$$N = b_4 + 2b_3 + 4b_2 + 8b_1.$$

Le tour déjoué

On a $\{0, \ldots, 15\} \overset{1:1}{\longleftrightarrow} \mathbf{F}_2^4$ par l'application qui à un entier N associe ses décimales (b_1, b_2, b_3, b_4) dans son écriture binaire :

$$N = b_4 + 2b_3 + 4b_2 + 8b_1.$$

$$b_1 = 0 \Longleftrightarrow N \leq 7$$

Le tour déjoué

On a $\{0, \ldots, 15\} \overset{1:1}{\longleftrightarrow} \mathbf{F}_2^4$ par l'application qui à un entier N associe ses décimales (b_1, b_2, b_3, b_4) dans son écriture binaire :

$$N = b_4 + 2b_3 + 4b_2 + 8b_1.$$

$$b_1 = 0 \iff N \leq 7$$
$$b_2 = 0 \iff N \in \{0, 1, 2, 3, 8, 9, 10, 11\}$$

Le tour déjoué

On a $\{0, \ldots, 15\} \overset{1:1}{\longleftrightarrow} \mathbf{F}_2^4$ par l'application qui à un entier N associe ses décimales (b_1, b_2, b_3, b_4) dans son écriture binaire :

$$N = b_4 + 2b_3 + 4b_2 + 8b_1.$$

$$b_1 = 0 \iff N \leq 7$$
$$b_2 = 0 \iff N \in \{0, 1, 2, 3, 8, 9, 10, 11\}$$
$$b_3 = 0 \iff N \in \{0, 1, 4, 5, 8, 9, 12, 13\}$$

Le tour déjoué

On a $\{0, \ldots, 15\} \overset{1:1}{\longleftrightarrow} \mathbf{F}_2^4$ par l'application qui à un entier N associe ses décimales (b_1, b_2, b_3, b_4) dans son écriture binaire :

$$N = b_4 + 2b_3 + 4b_2 + 8b_1.$$

$$\begin{aligned} b_1 = 0 &\iff N \leq 7 \\ b_2 = 0 &\iff N \in \{0, 1, 2, 3, 8, 9, 10, 11\} \\ b_3 = 0 &\iff N \in \{0, 1, 4, 5, 8, 9, 12, 13\} \\ b_4 = 0 &\iff N \text{ est pair} \end{aligned}$$

Le tour déjoué

On a $\{0, \ldots, 15\} \overset{1:1}{\longleftrightarrow} \mathbf{F}_2^4$ par l'application qui à un entier N associe ses décimales (b_1, b_2, b_3, b_4) dans son écriture binaire :

$$N = b_4 + 2b_3 + 4b_2 + 8b_1.$$

$$\begin{aligned} b_1 = 0 &\iff N \leq 7 \\ b_2 = 0 &\iff N \in \{0, 1, 2, 3, 8, 9, 10, 11\} \\ b_3 = 0 &\iff N \in \{0, 1, 4, 5, 8, 9, 12, 13\} \\ b_4 = 0 &\iff N \text{ est pair} \\ b_1 + b_2 + b_4 = 0 &\iff N \in \{0, 2, 5, 7, 9, 11, 12, 14\} \end{aligned}$$

Le tour déjoué

On a $\{0, \ldots, 15\} \overset{1:1}{\longleftrightarrow} \mathbf{F}_2^4$ par l'application qui à un entier N associe ses décimales (b_1, b_2, b_3, b_4) dans son écriture binaire :

$$N = b_4 + 2b_3 + 4b_2 + 8b_1.$$

$$\begin{aligned}
b_1 = 0 &\iff N \leq 7 \\
b_2 = 0 &\iff N \in \{0, 1, 2, 3, 8, 9, 10, 11\} \\
b_3 = 0 &\iff N \in \{0, 1, 4, 5, 8, 9, 12, 13\} \\
b_4 = 0 &\iff N \text{ est pair} \\
b_1 + b_2 + b_4 = 0 &\iff N \in \{0, 2, 5, 7, 9, 11, 12, 14\} \\
b_1 + b_3 + b_4 = 0 &\iff N \in \{0, 3, 4, 7, 9, 10, 13, 14\}
\end{aligned}$$

Le tour déjoué

On a $\{0, \ldots, 15\} \overset{1:1}{\longleftrightarrow} \mathbf{F}_2^4$ par l'application qui à un entier N associe ses décimales (b_1, b_2, b_3, b_4) dans son écriture binaire :

$$N = b_4 + 2b_3 + 4b_2 + 8b_1.$$

$$\begin{aligned}
b_1 = 0 &\iff N \leq 7 \\
b_2 = 0 &\iff N \in \{0, 1, 2, 3, 8, 9, 10, 11\} \\
b_3 = 0 &\iff N \in \{0, 1, 4, 5, 8, 9, 12, 13\} \\
b_4 = 0 &\iff N \text{ est pair} \\
b_1 + b_2 + b_4 = 0 &\iff N \in \{0, 2, 5, 7, 9, 11, 12, 14\} \\
b_1 + b_3 + b_4 = 0 &\iff N \in \{0, 3, 4, 7, 9, 10, 13, 14\} \\
b_2 + b_3 + b_4 = 0 &\iff N \in \{0, 3, 5, 6, 8, 11, 13, 14\}
\end{aligned}$$

Sommaire

- Michel Demazure. *Cours d'algèbre. Primalité. Divisibilité. Codes.* Cassini, Paris, 1997. xviii+302 pp.
- Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier, Sébastien Varrette. *Théorie des codes. Compression, cryptage, correction*. Dunod, 2013 - 2ème édition - 384 p.
- http ://www.sagemath.org/

- Michel Demazure. *Cours d'algèbre. Primalité. Divisibilité. Codes.* Cassini, Paris, 1997. xviii+302 pp.
- Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier, Sébastien Varrette. *Théorie des codes. Compression, cryptage, correction*. Dunod, 2013 - 2ème édition - 384 p.
- http ://www.sagemath.org/

1. Pour tout entier $r \geq 2$, il existe un code binaire, linéaire, 1-correcteur parfait de paramètres $[2^r - 1, 2^r - r - 1, 3]$.

- Michel Demazure. *Cours d'algèbre. Primalité. Divisibilité. Codes.* Cassini, Paris, 1997. xviii+302 pp.
- Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier, Sébastien Varrette. *Théorie des codes. Compression, cryptage, correction*. Dunod, 2013 - 2ème édition - 384 p.
- http ://www.sagemath.org/

1. Pour tout entier $r \geq 2$, il existe un code binaire, linéaire, 1-correcteur parfait de paramètres $[2^r - 1, 2^r - r - 1, 3]$.
2. Il existe un seul code t-correcteur parfait avec $t > 1$: le code de Golay G_{23} (de longueur 23, dimension 12 avec $d_H(G_{23}) = 7$).

- Michel Demazure. *Cours d'algèbre. Primalité. Divisibilité. Codes.* Cassini, Paris, 1997. xviii+302 pp.
- Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier, Sébastien Varrette. *Théorie des codes. Compression, cryptage, correction*. Dunod, 2013 - 2ème édition - 384 p.
- http ://www.sagemath.org/

1. Pour tout entier $r \geq 2$, il existe un code binaire, linéaire, 1-correcteur parfait de paramètres $[2^r - 1, 2^r - r - 1, 3]$.
2. Il existe un seul code t-correcteur parfait avec $t > 1$: le code de Golay G_{23} (de longueur 23, dimension 12 avec $d_H(G_{23}) = 7$).
3. Il existe une notion de code sur tout corps fini.

- Michel Demazure. *Cours d'algèbre. Primalité. Divisibilité. Codes.* Cassini, Paris, 1997. xviii+302 pp.
- Jean-Guillaume Dumas, Jean-Louis Roch, Eric Tannier, Sébastien Varrette. *Théorie des codes. Compression, cryptage, correction*. Dunod, 2013 - 2ème édition - 384 p.
- http ://www.sagemath.org/

1. Pour tout entier $r \geq 2$, il existe un code binaire, linéaire, 1-correcteur parfait de paramètres $[2^r - 1, 2^r - r - 1, 3]$.
2. Il existe un seul code t-correcteur parfait avec $t > 1$: le code de Golay G_{23} (de longueur 23, dimension 12 avec $d_H(G_{23}) = 7$).
3. Il existe une notion de code sur tout corps fini.
4. Les codes de Reed-Solomon sont utilisés pour les transmissions par satellite ou la lecture des codes QR.