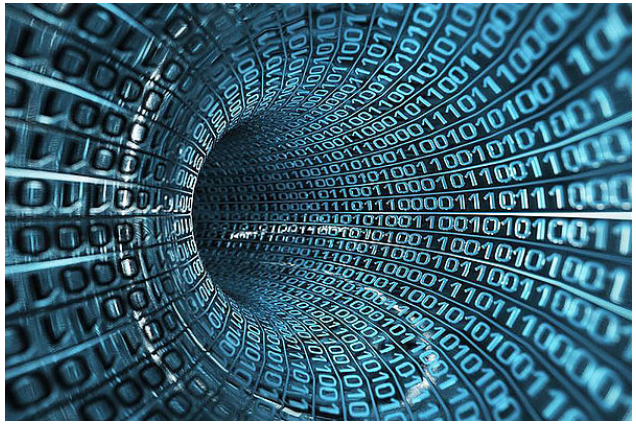
Les mathématiques et les communications numériques: des satellites aux réseaux

Alberto Ravagnani

University College Dublin



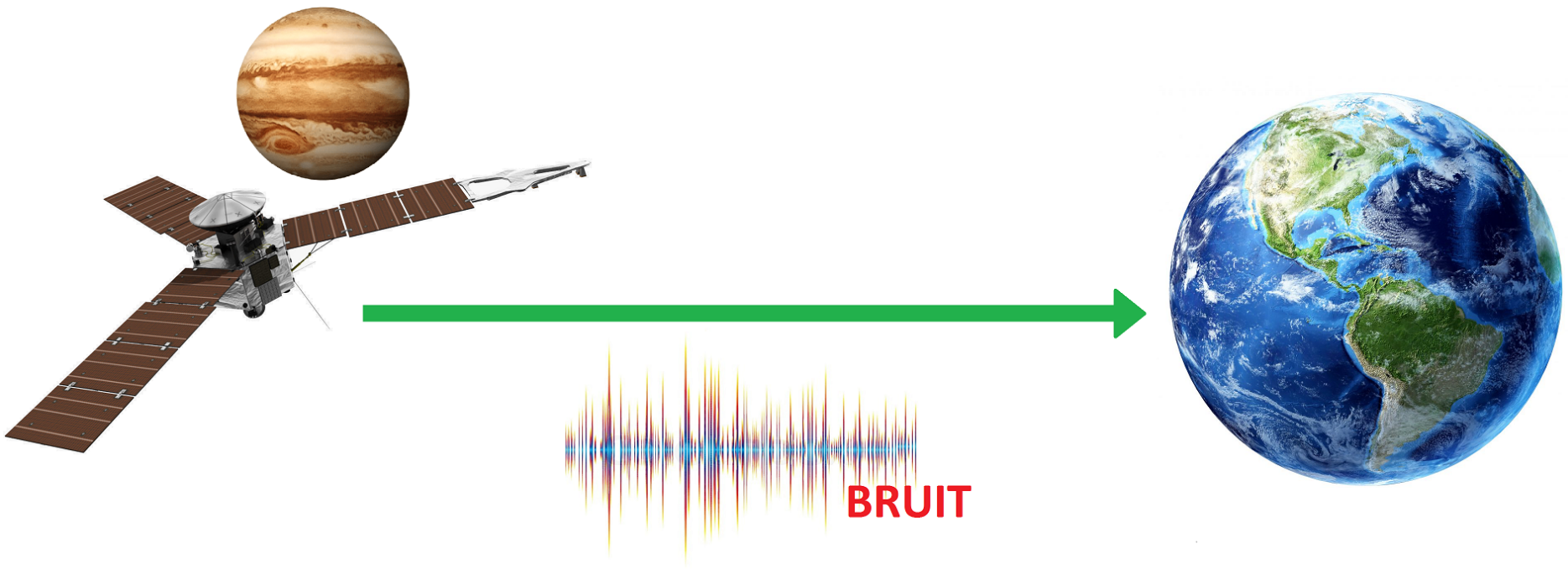
Théorie et pratique des codes correcteurs d'erreurs

– Université de Neuchâtel –

Qu'est-ce que la théorie des codes?

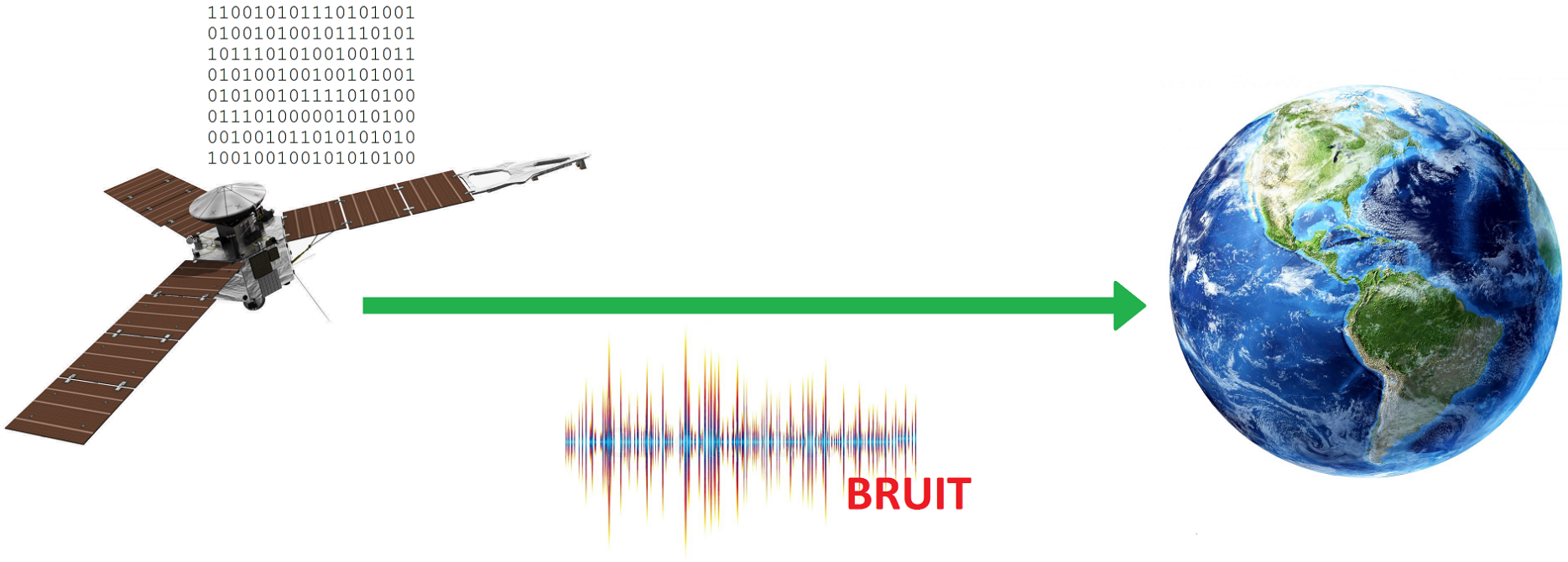
Qu'est-ce que la théorie des codes?

Un **code** (**correcteur**) est un objet mathématique qui corrige les erreurs dues à un bruit.



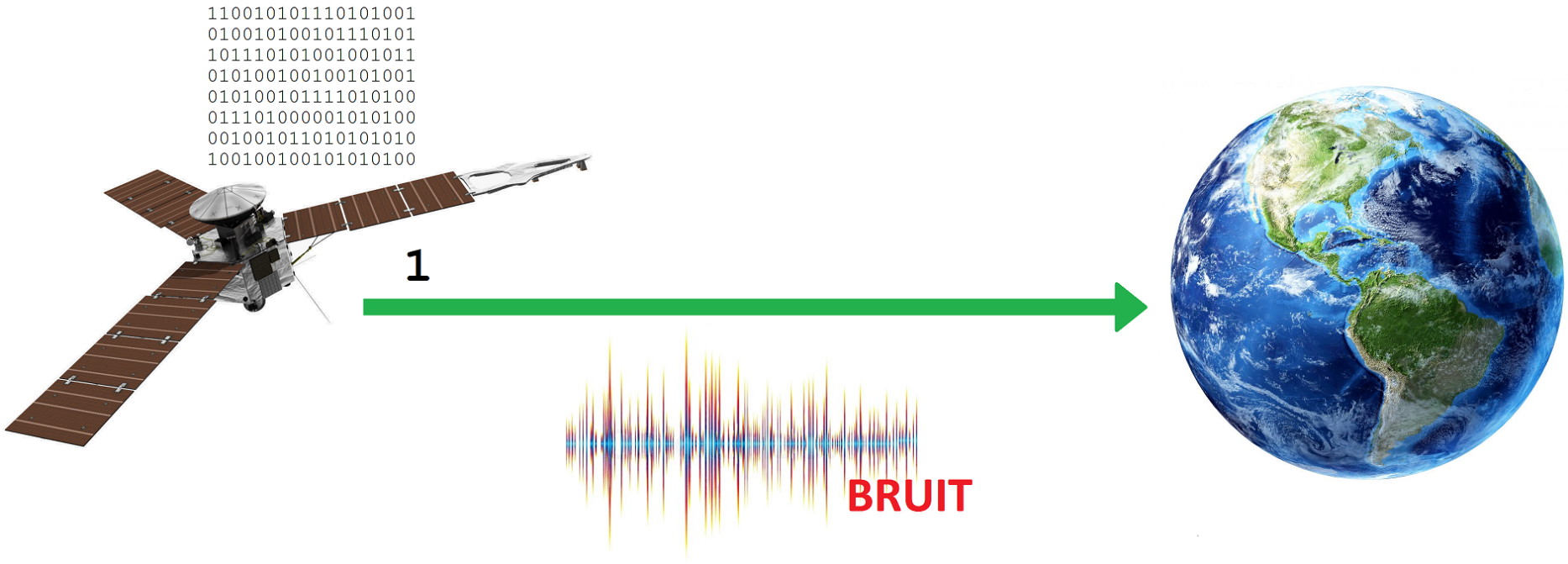
Qu'est-ce que la théorie des codes?

Un **code** (**correcteur**) est un objet mathématique qui corrige les erreurs dues à un bruit.



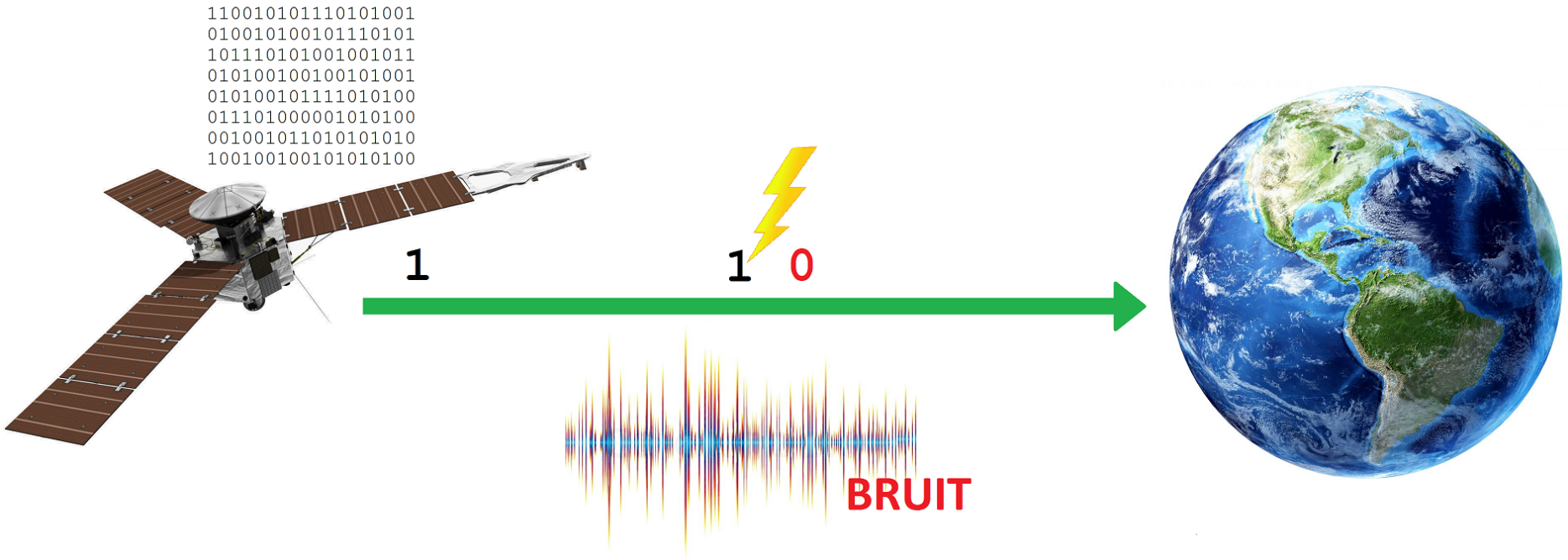
Qu'est-ce que la théorie des codes?

Un **code** (**correcteur**) est un objet mathématique qui corrige les erreurs dues à un bruit.



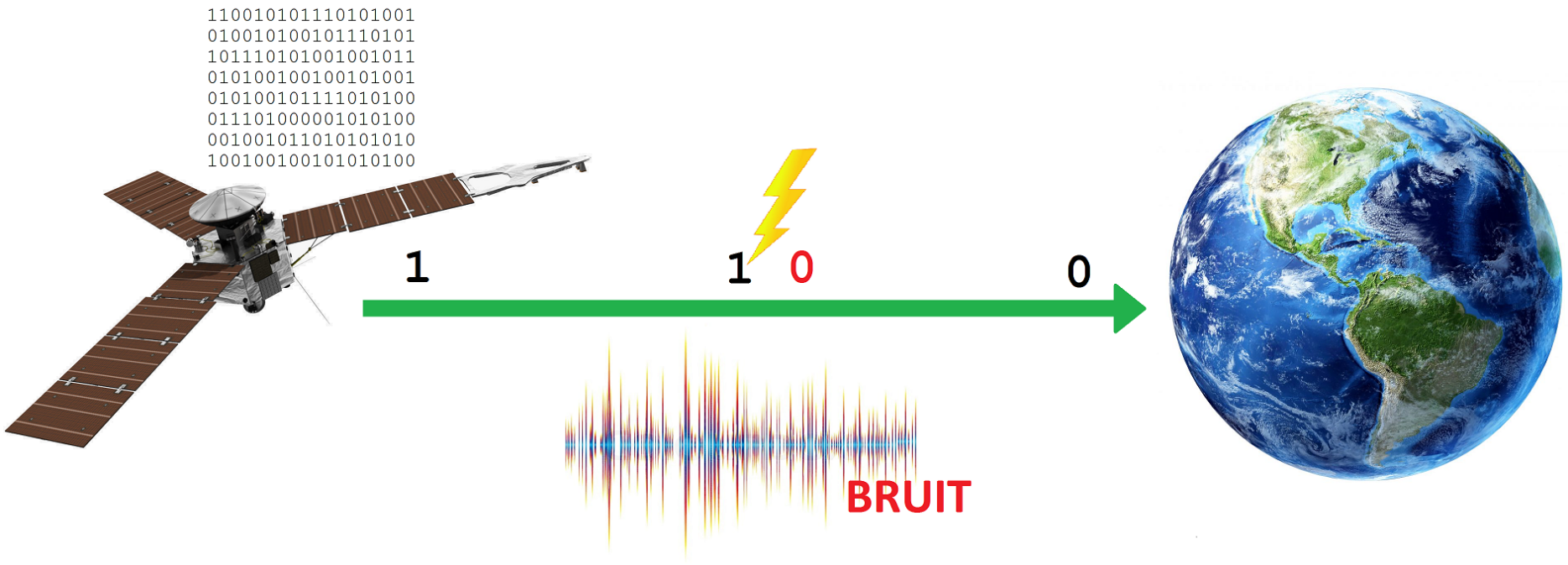
Qu'est-ce que la théorie des codes?

Un **code** (**correcteur**) est un objet mathématique qui corrige les erreurs dues à un bruit.



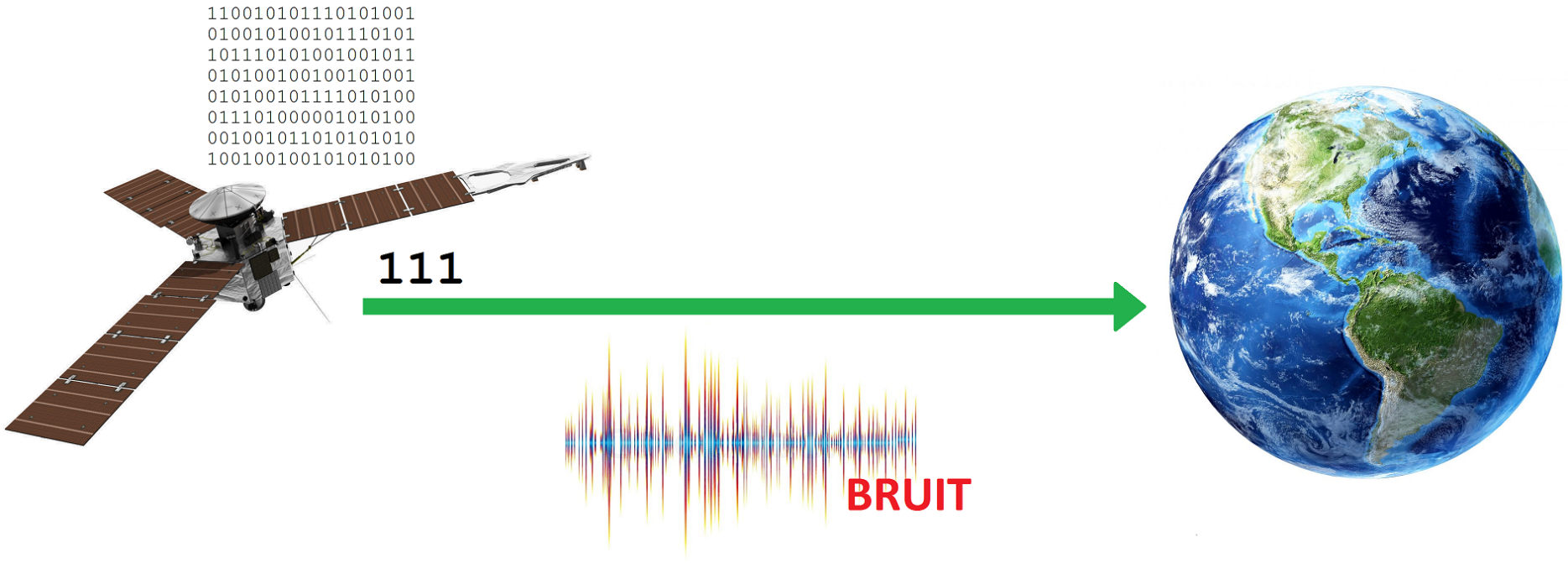
Qu'est-ce que la théorie des codes?

Un **code** (**correcteur**) est un objet mathématique qui corrige les erreurs dues à un bruit.



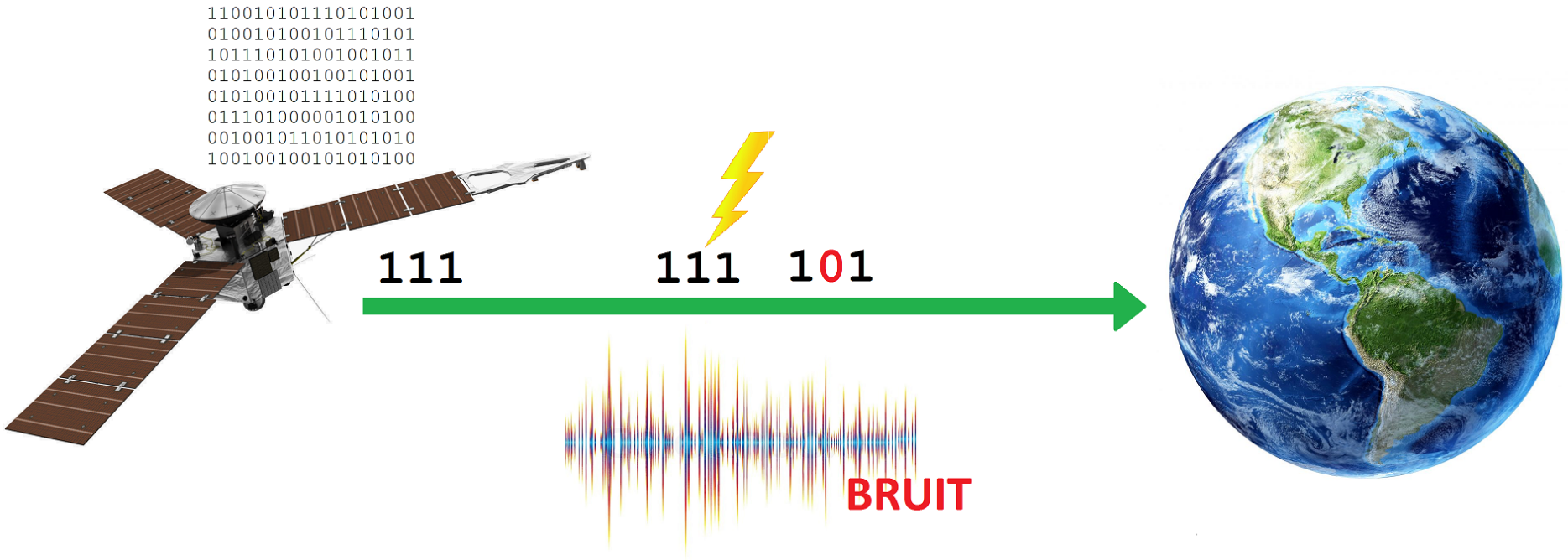
Qu'est-ce que la théorie des codes?

Un **code** (**correcteur**) est un objet mathématique qui corrige les erreurs dues à un bruit.



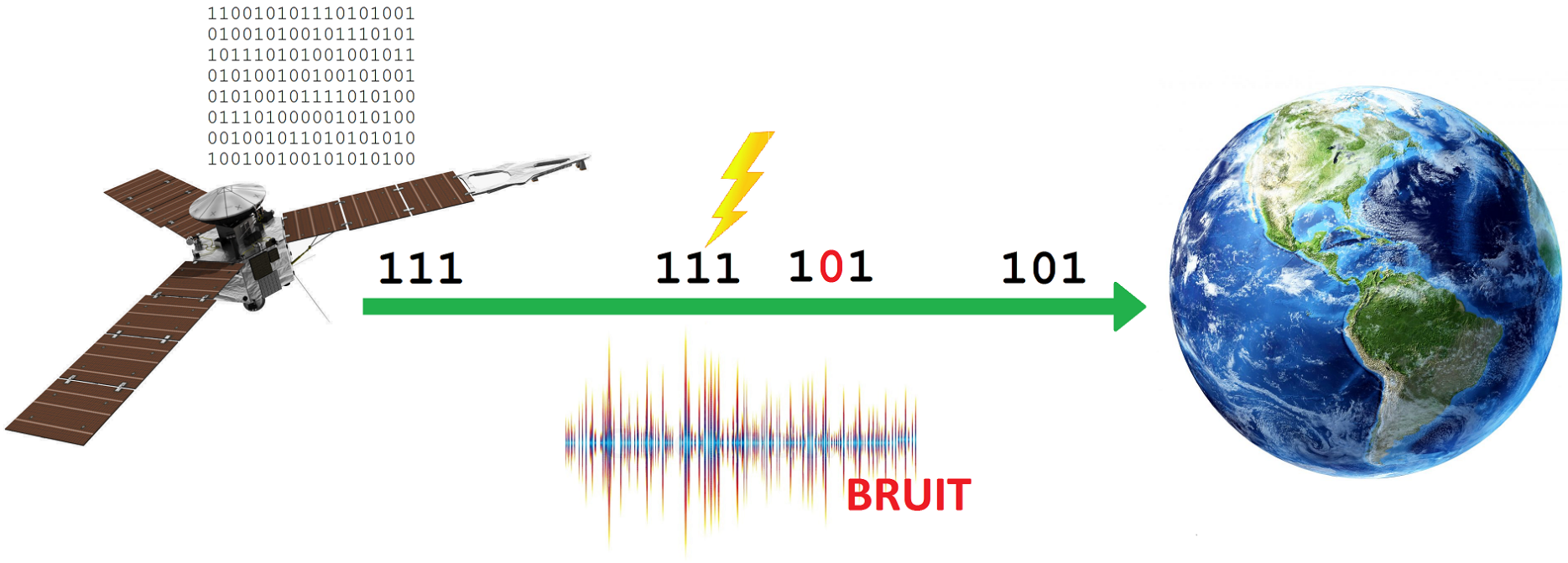
Qu'est-ce que la théorie des codes?

Un **code** (**correcteur**) est un objet mathématique qui corrige les erreurs dues à un bruit.



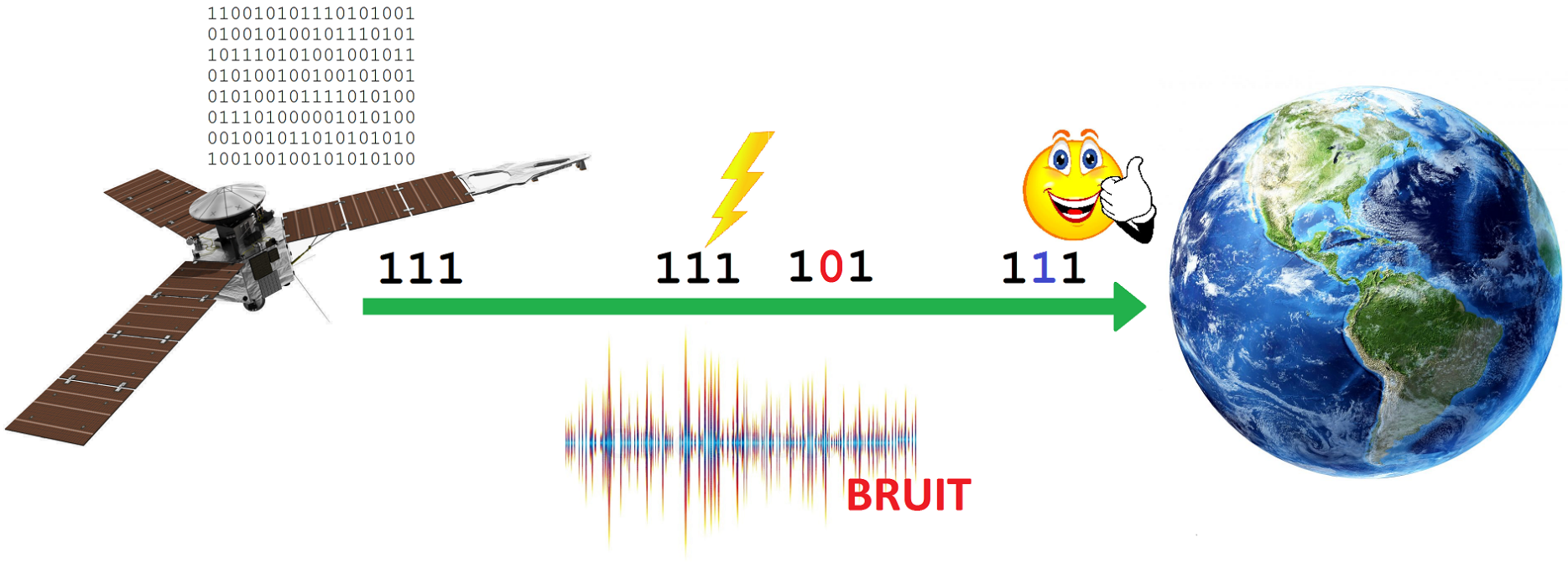
Qu'est-ce que la théorie des codes?

Un **code** (**correcteur**) est un objet mathématique qui corrige les erreurs dues à un bruit.



Qu'est-ce que la théorie des codes?

Un **code** (**correcteur**) est un objet mathématique qui corrige les erreurs dues à un bruit.



Qu'est-ce que la théorie des codes?

IDÉE DE BASE de la théorie des codes: ajouter de la **redondance**.

Qu'est-ce que la théorie des codes?

IDÉE DE BASE de la théorie des codes: ajouter de la **redondance**.

En langage mathématique...

Définition

Soit $\mathbb{F}_q$ le corps fini avec q éléments.

- La **distance de Hamming** entre $v, w \in \mathbb{F}_q^n$ est $d_{\mathrm{H}}(v, w) = \#\{1 \leq i \leq n \mid v_i \neq w_i\}$.
- Un **code** est un sous-espace $\mathscr{C} \subseteq \mathbb{F}_q^n$, $\mathscr{C} \neq \{0\}$.
- Les éléments de $\mathscr{C}$ s'appellent les **mots** du code.
- La **distance minimale** de $\mathscr{C}$ est $d_{\mathrm{H}}(\mathscr{C}) = \min\{d_{\mathrm{H}}(v, w) \mid v, w \in \mathscr{C},\ v \neq w\}$.

Qu'est-ce que la théorie des codes?

IDÉE DE BASE de la théorie des codes: ajouter de la **redondance**.

En langage mathématique...

Définition

Soit $\mathbb{F}_q$ le corps fini avec q éléments.

- La **distance de Hamming** entre $v, w \in \mathbb{F}_q^n$ est $d_{\mathrm{H}}(v, w) = \#\{1 \leq i \leq n \mid v_i \neq w_i\}$.
- Un **code** est un sous-espace $\mathscr{C} \subseteq \mathbb{F}_q^n$, $\mathscr{C} \neq \{0\}$.
- Les éléments de $\mathscr{C}$ s'appellent les **mots** du code.
- La **distance minimale** de $\mathscr{C}$ est $d_{\mathrm{H}}(\mathscr{C}) = \min\{d_{\mathrm{H}}(v, w) \mid v, w \in \mathscr{C},\ v \neq w\}$.

Proposition

La capacité de correction d'un code est mesurée par sa distance minimale.

Qu'est-ce que la théorie des codes?

IDÉE DE BASE de la théorie des codes: ajouter de la **redondance**.

En langage mathématique...

Définition

Soit $\mathbb{F}_q$ le corps fini avec q éléments.

- La **distance de Hamming** entre $v, w \in \mathbb{F}_q^n$ est $d_{\mathrm{H}}(v, w) = \#\{1 \leq i \leq n \mid v_i \neq w_i\}$.
- Un **code** est un sous-espace $\mathscr{C} \subseteq \mathbb{F}_q^n$, $\mathscr{C} \neq \{0\}$.
- Les éléments de $\mathscr{C}$ s'appellent les **mots** du code.
- La **distance minimale** de $\mathscr{C}$ est $d_{\mathrm{H}}(\mathscr{C}) = \min\{d_{\mathrm{H}}(v, w) \mid v, w \in \mathscr{C},\ v \neq w\}$.

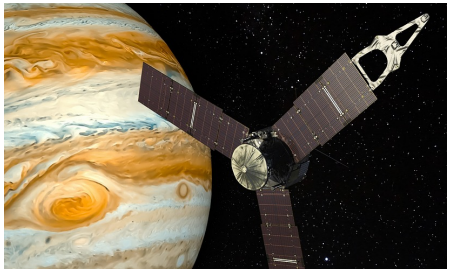
Proposition

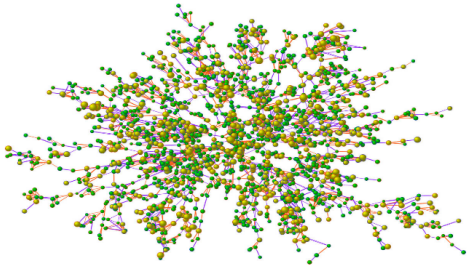
La capacité de correction d'un code est mesurée par sa distance minimale.

Autrement dit, un code de dimension k est un plongement $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^n$ $\rightsquigarrow$ **redondance**.

Applications

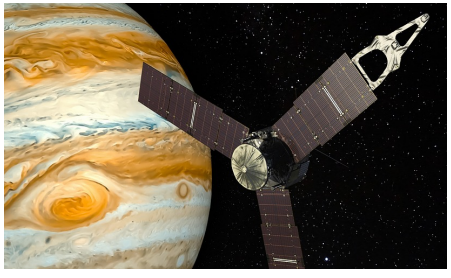
- Satellites
- Sondes spatiales (photos des planètes et des lunes)
- Trains
- CDs, DVDs, mémoires flash, ...
- Code QR
- Code ISBN
- Communications sur un réseau (web, téléphones mobiles, ...)

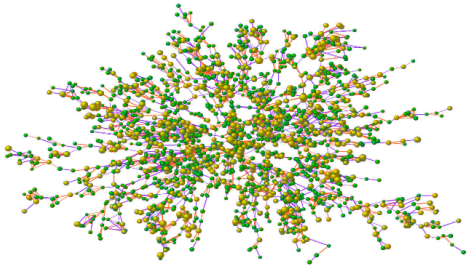




Applications

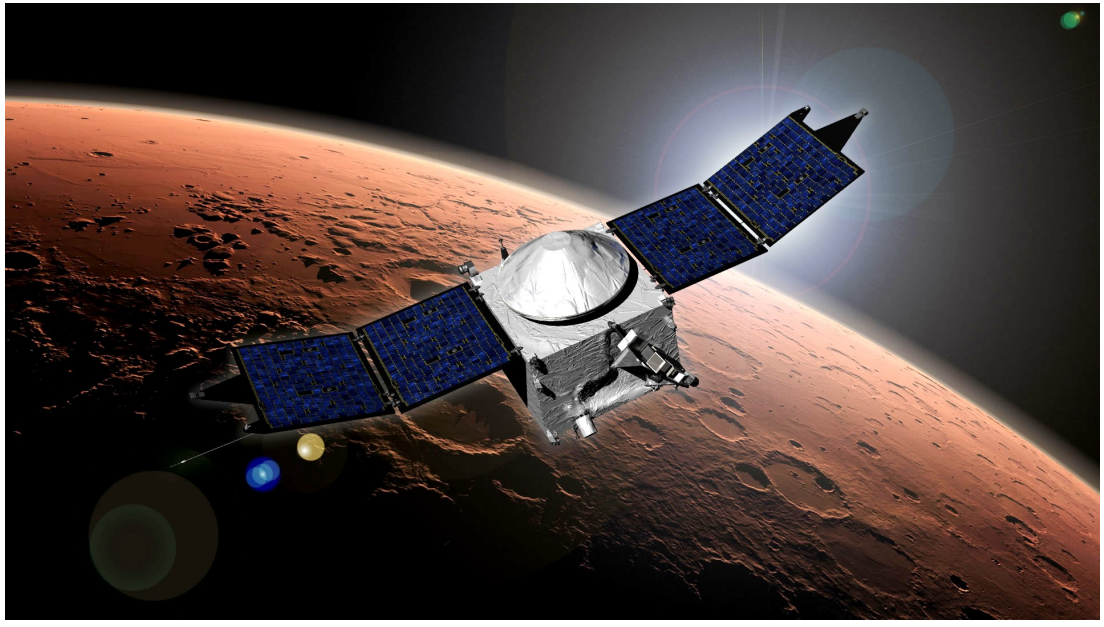
- Satellites
- Sondes spatiales (photos des planètes et des lunes) ◀
- Trains
- CDs, DVDs, mémoires flash, ...
- Code QR
- Code ISBN
- Communications sur un réseau (web, téléphones mobiles, ...) ◀





Les sondes spatiales

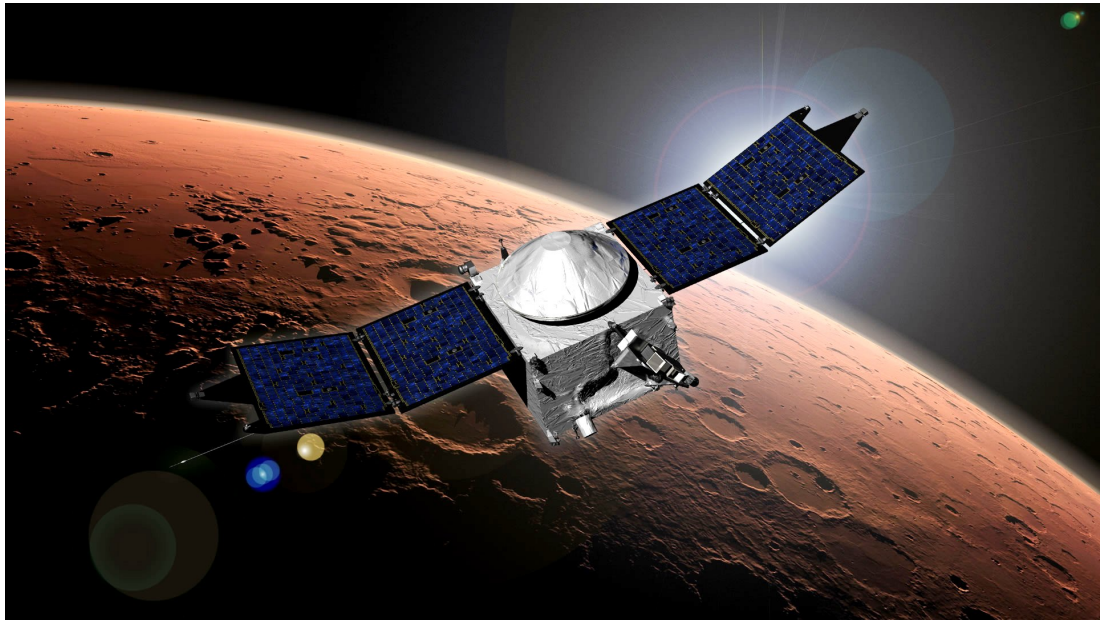
1972: la sonde *Mariner 9* prend des photos de Mars.



- Photos en 64 nuances de gris
- En moyenne, 26% de chaque image était corrompu (vent solaire, atmosphère)

Les sondes spatiales

1972: la sonde *Mariner 9* prend des photos de Mars.

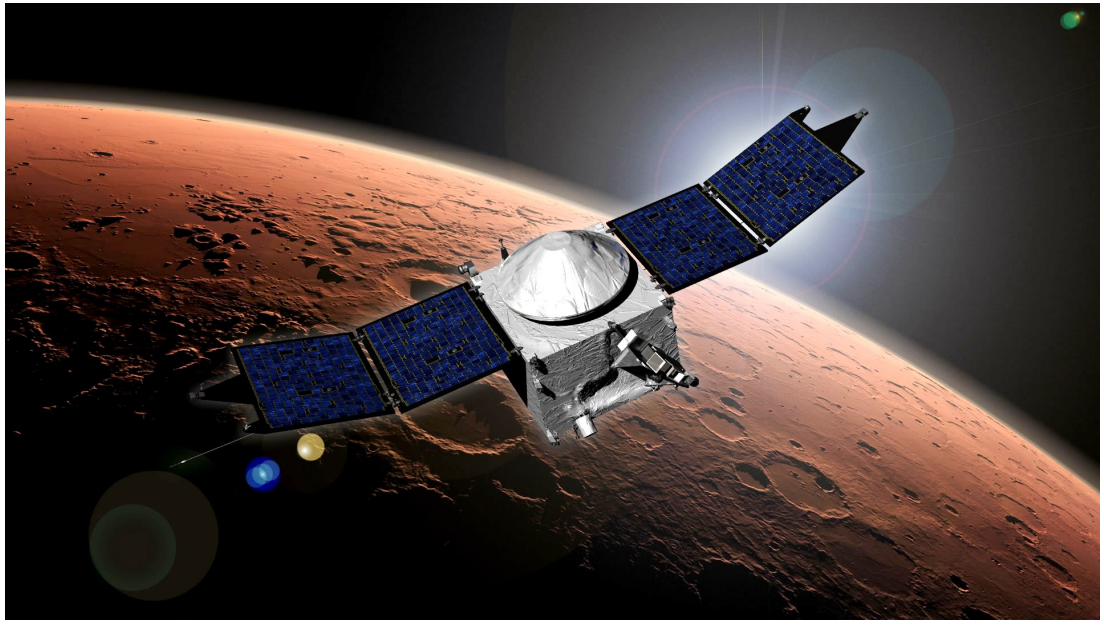


- Photos en 64 nuances de gris
- En moyenne, 26% de chaque image était corrompu (vent solaire, atmosphère)

Code utilisé pour la correction: **Reed-Muller** RM(1,5)

Les sondes spatiales

1972: la sonde *Mariner 9* prend des photos de Mars.

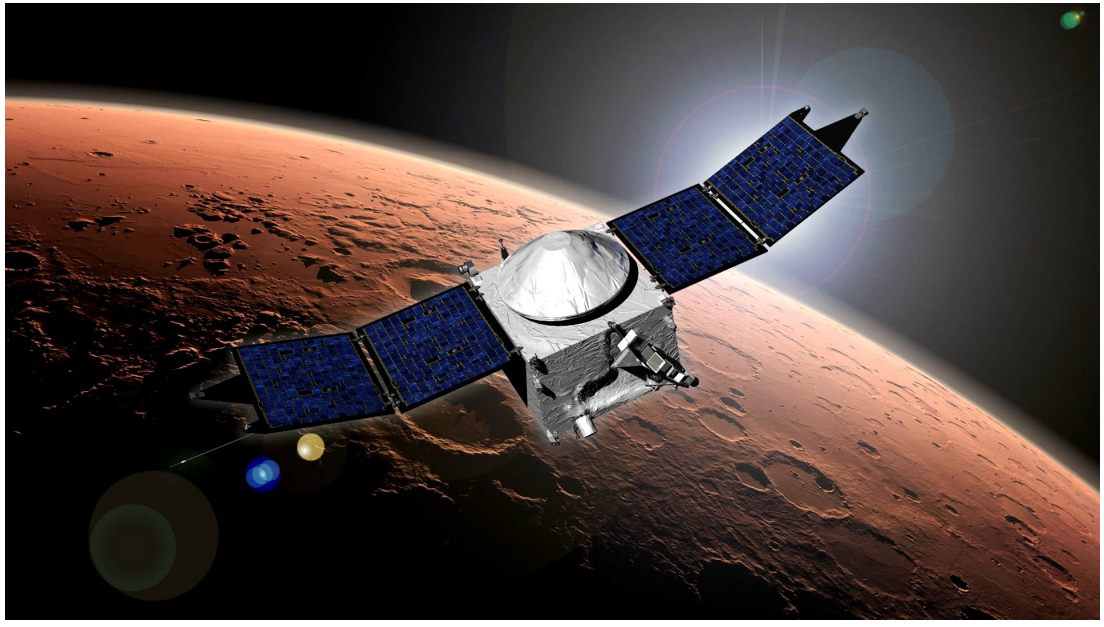


- Photos en 64 nuances de gris
- En moyenne, 26% de chaque image était corrompu (vent solaire, atmosphère)

Code utilisé pour la correction: **Reed-Muller** $\mathrm{RM}(1,5) \subseteq \mathbb{F}_2^{32}$

Les sondes spatiales

1972: la sonde *Mariner 9* prend des photos de Mars.



- Photos en 64 nuances de gris
- En moyenne, 26% de chaque image était corrompu (vent solaire, atmosphère)

Code utilisé pour la correction: **Reed-Muller** $\mathrm{RM}(1,5) \subseteq \mathbb{F}_2^{32}$ de dimension 6.

Les codes de Reed-Muller

$\mathrm{RM}(1,5) \subseteq \mathbb{F}_2^{32}$ est l'espace engendré par les lignes de la matrice

$$\begin{pmatrix}
1&0&0&1&0&1&1&0&0&1&1&0&1&0&0&1&0&1&1&0&1&0&0&1&1&0&0&1&0&1&1&0\\
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{pmatrix}$$

Cette matrice nous a permis de voir les premières photos rapprochées de Mars.

Les codes de Reed-Muller

$\mathrm{RM}(1,5) \subseteq \mathbb{F}_2^{32}$ est l'espace engendré par les lignes de la matrice

$$\begin{pmatrix}
1&0&0&1&0&1&1&0&0&1&1&0&1&0&0&1&0&1&1&0&1&0&0&1&1&0&0&1&0&1&1&0\\
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{pmatrix}$$

Cette matrice nous a permis de voir les premières photos rapprochées de Mars.

Définition

Soient $0 \leq r \leq m$ des entiers. Le **code de Reed-Muller** $\mathrm{RM}(r,m) \subseteq \mathbb{F}_2^{2^m}$ est donné par

$$\begin{cases}
\mathrm{RM}(m,m) = \mathbb{F}_2^{2^m}, \\
\mathrm{RM}(-1,m) = \{0\}, \\
\mathrm{RM}(r,m) = \{(u, u+v) \mid u \in \mathrm{RM}(r,m-1),\ v \in \mathrm{RM}(r-1,m-1)\}.
\end{cases}$$

Les codes de Reed-Muller

$\mathrm{RM}(1,5) \subseteq \mathbb{F}_2^{32}$ est l'espace engendré par les lignes de la matrice

$$\begin{pmatrix}
1&0&0&1&0&1&1&0&0&1&1&0&1&0&0&1&0&1&1&0&1&0&0&1&1&0&0&1&0&1&1&0\\
0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\
0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\
0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\
0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{pmatrix}$$

Cette matrice nous a permis de voir les premières photos rapprochées de Mars.

Définition

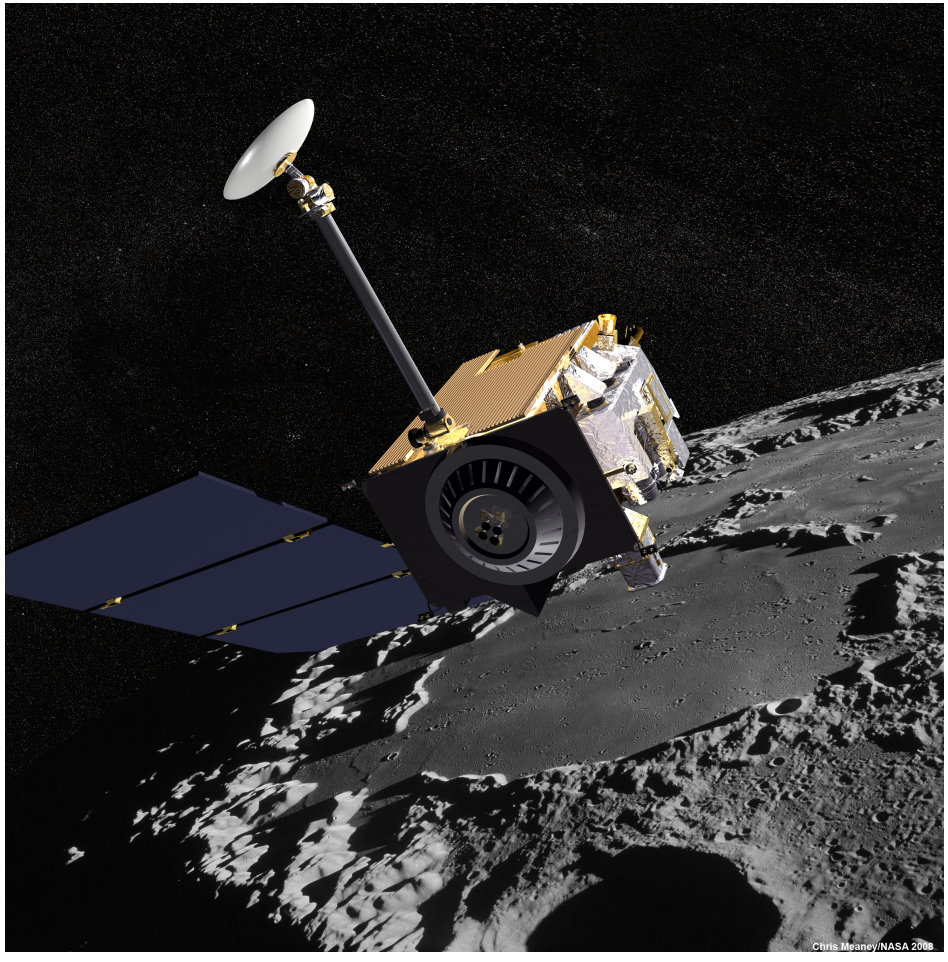
Soient $0 \leq r \leq m$ des entiers. Le **code de Reed-Muller** $\mathrm{RM}(r,m) \subseteq \mathbb{F}_2^{2^m}$ est donné par

$$\begin{cases}
\mathrm{RM}(m,m) = \mathbb{F}_2^{2^m}, \\
\mathrm{RM}(-1,m) = \{0\}, \\
\mathrm{RM}(r,m) = \{(u, u+v) \mid u \in \mathrm{RM}(r,m-1),\ v \in \mathrm{RM}(r-1,m-1)\}.
\end{cases}$$

D'autres codes peuvent être construits en utilisant, par exemple, les **polynômes** (codes de Reed-Solomon), les **séries de Laurent** (codes convolution), ...

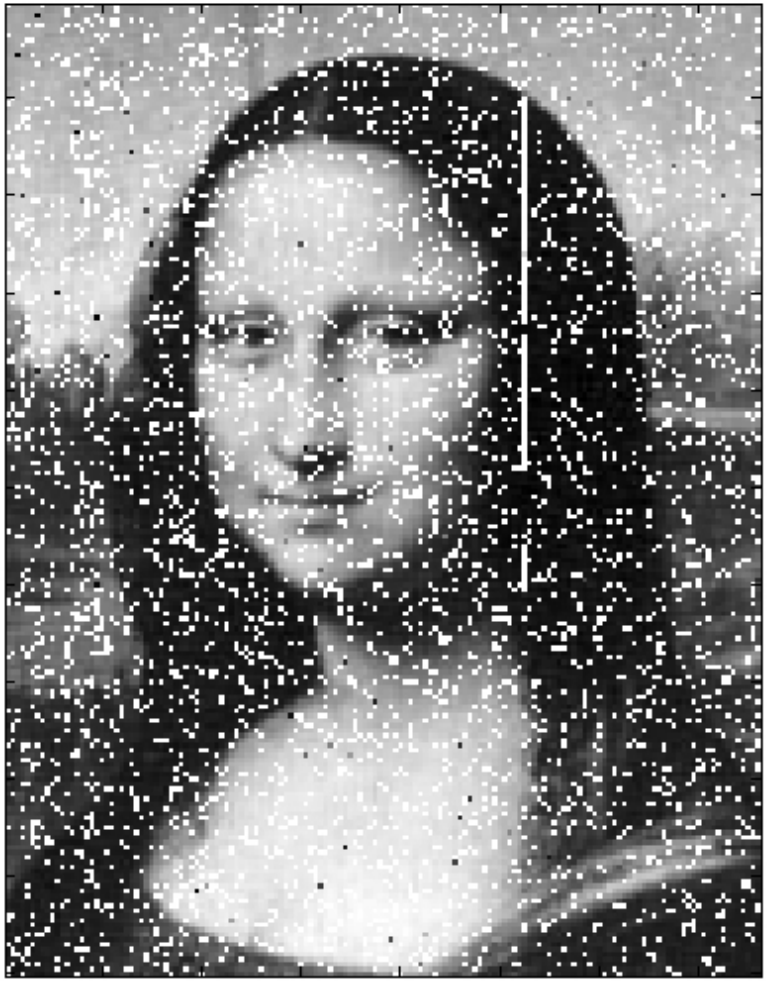
Ça marche!

2009: le LRO (Lunar Reconnaissance Orbiter) prend des photos de la surface de la Lune.



Ça marche!

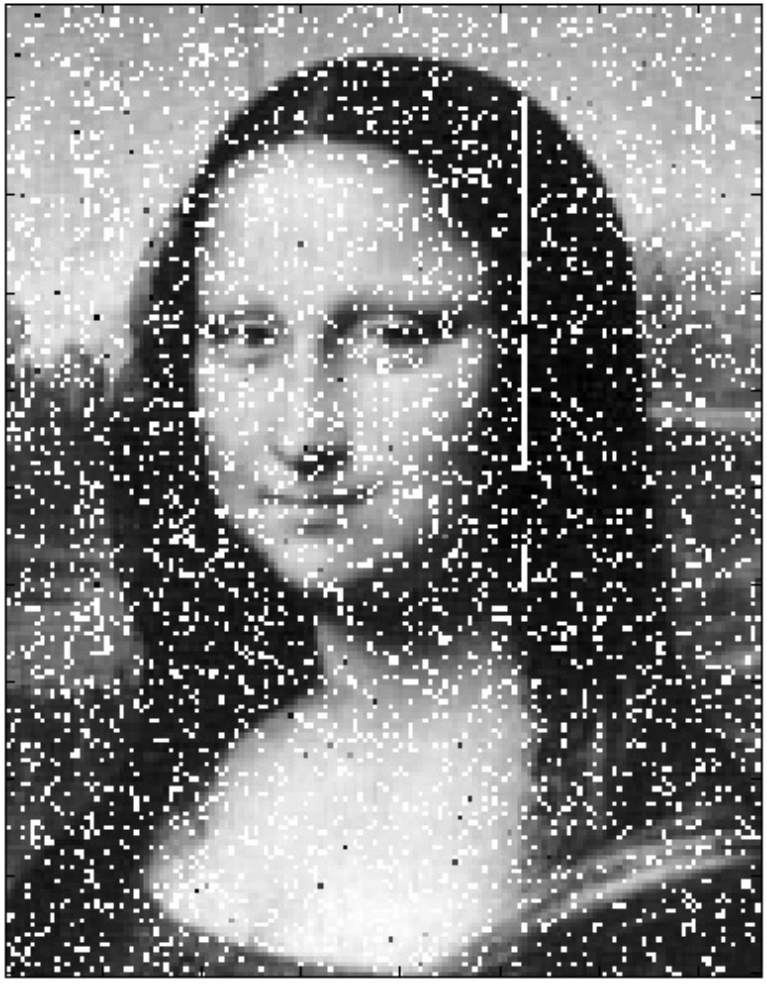
Test de la transmission d'images:



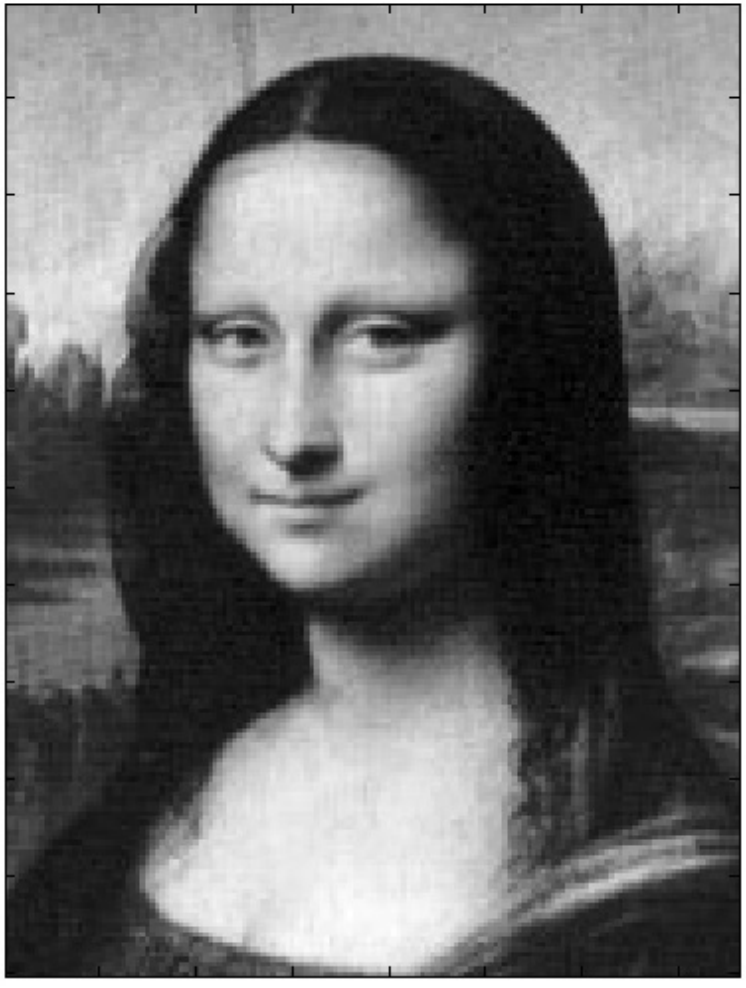
sans codage

Ça marche!

Test de la transmission d'images:



sans codage



avec codage

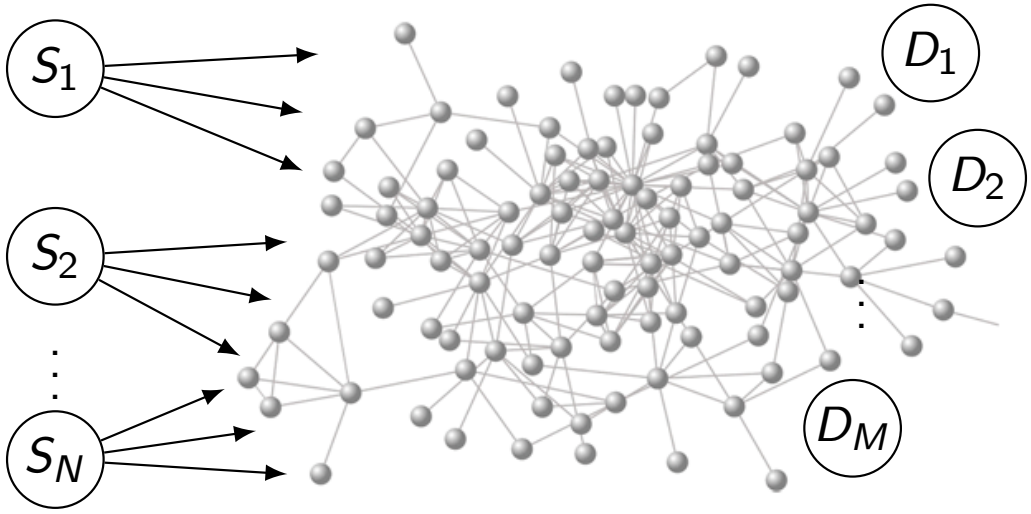
Les communications sur les réseaux

Théorie “classique” des codes : **une** source d’information, **un** destinataire.

Les communications sur les réseaux

Théorie "classique" des codes : **une** source d'information, **un** destinataire.

Théorie "réseaux" des codes : **plusieurs** sources d'information, **plusieurs** destinataires.



Applications: LTE (téléphones mobiles), distributed storage, peer-to-peer, streaming,...

Les communications sur les réseaux

On travaille avec des **nouvelles définitions** et objets mathématiques:

- Codes réseaux (Ahlswede, Cai, Li, Yeung, Kötter, Médard)
- Codes avec la métrique du rang (Delsarte, Gabidulin, Kötter, Kschischang)
- Codes "subspace" (Kötter, Kschischang)

$\rightsquigarrow$ **Nouveaux outils mathématiques** pour étudier les communications sur un réseau.

Les communications sur les réseaux

On travaille avec des **nouvelles définitions** et objets mathématiques:

- Codes réseaux (Ahlswede, Cai, Li, Yeung, Kötter, Médard)
- Codes avec la métrique du rang (Delsarte, Gabidulin, Kötter, Kschischang)
- Codes "subspace" (Kötter, Kschischang)

$\rightsquigarrow$ **Nouveaux outils mathématiques** pour étudier les communications sur un réseau.

Nouveaux problèmes mathématiques:

- Espaces de matrices avec la métrique du rang
- Problèmes de "packing" dans une Grassmannienne sur $\mathbb{F}_q$
- Problèmes en Théorie des Graphes

Les communications sur les réseaux

On travaille avec des **nouvelles définitions** et objets mathématiques:

- Codes réseaux (Ahlswede, Cai, Li, Yeung, Kötter, Médard)
- Codes avec la métrique du rang (Delsarte, Gabidulin, Kötter, Kschischang)
- Codes "subspace" (Kötter, Kschischang)

$\rightsquigarrow$ **Nouveaux outils mathématiques** pour étudier les communications sur un réseau.

Nouveaux problèmes mathématiques:

- Espaces de matrices avec la métrique du rang ◀
- Problèmes de "packing" dans une Grassmannienne sur $\mathbb{F}_q$
- Problèmes en Théorie des Graphes

La conjecture de Etzion et Silberstein

Soient $1 \leq n \leq m$ des entiers, et soit $\mathscr{P} \subseteq \{1,...,n\} \times \{1,...,m\}$ un ensemble (**profil**). Définissons

$$\mathbb{F}_q^{n \times m}[\mathscr{P}] = \{M \in \mathbb{F}_q^{n \times m} \mid M_{ij} = 0 \text{ pour tout } (i,j) \notin \mathscr{P}\}.$$

La conjecture de Etzion et Silberstein

Soient $1 \leq n \leq m$ des entiers, et soit $\mathscr{P} \subseteq \{1,...,n\} \times \{1,...,m\}$ un ensemble (**profil**). Définissons

$$\mathbb{F}_q^{n \times m}[\mathscr{P}] = \{M \in \mathbb{F}_q^{n \times m} \mid M_{ij} = 0 \text{ pour tout } (i,j) \notin \mathscr{P}\}.$$

$$n \left\{ \underbrace{\begin{array}{cccccc} \bullet & \bullet & 0 & \bullet & \bullet & \bullet \\ 0 & \bullet & \bullet & \bullet & 0 & \bullet \\ \bullet & \bullet & 0 & 0 & \bullet & 0 \\ \bullet & \bullet & \bullet & \bullet & 0 & \bullet \end{array}}_{m} \right.$$

$$\mathscr{P} = \{\bullet\} \subseteq \{1,...,n\} \times \{1,...,m\}.$$

La conjecture de Etzion et Silberstein

Soient $1 \leq n \leq m$ des entiers, et soit $\mathscr{P} \subseteq \{1,...,n\} \times \{1,...,m\}$ un ensemble (**profil**). Définissons

$$\mathbb{F}_q^{n\times m}[\mathscr{P}] = \{M \in \mathbb{F}_q^{n\times m} \mid M_{ij} = 0 \text{ pour tout } (i,j) \notin \mathscr{P}\}.$$

$$\underbrace{\begin{pmatrix} \bullet & \bullet & 0 & \bullet & \bullet & \bullet \\ 0 & \bullet & \bullet & \bullet & 0 & \bullet \\ \bullet & \bullet & 0 & 0 & \bullet & 0 \\ \bullet & \bullet & \bullet & \bullet & 0 & \bullet \end{pmatrix}}_{m} \Big\} n \qquad \mathscr{P} = \{\bullet\} \subseteq \{1,...,n\} \times \{1,...,m\}.$$

Proposition (Etzion-Silberstein 2009)

Soit $1 \leq \delta \leq n$ un entier, et soit $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}[\mathscr{P}]$ un sous-espace tel que

$$\text{rang}(M) \geq \delta \text{ pour toute } M \in \mathscr{C},\ M \neq 0.$$

Supposons que $\mathscr{P} = \mathscr{F}$ est un diagramme de Ferrers. Alors $\dim_{\mathbb{F}_q}(\mathscr{C}) \leq \mathrm{C}_\delta(\mathscr{F})$, où $\mathrm{C}_\delta(\mathscr{F})$ est un invariant combinatoire attaché à $(\mathscr{F}, \delta)$.

Conjecture de E-S: la borne est exacte.

La conjecture de Etzion et Silberstein

La conjecture est vraie dans les cas les plus importants pour les applications.

La conjecture de Etzion et Silberstein

La conjecture est vraie dans les cas les plus importants pour les applications.

Théorème (Gorla-Ravagnani)

Soit $\mathscr{F}$ un diagramme de Ferrers où les lignes ont cardinalité $r_1, r_2, ..., r_n$. La conjecture de Etzion-Silberstein est vraie dans les cas suivants:

- $r_{\delta-1} \geq n$,
- $\delta = n = m$ sont pairs et $C_n(\mathscr{F}) = n/2$,
- $\delta = n = m$ et $C_n(\mathscr{F}) = n-1$,
- $r_i \geq m-i+1$ pour $i = 1, ..., \delta$ et $r_i \leq m-i+1$ pour $i = \delta, ..., n$ et $q = |\mathbb{F}_q| \geq n-1$.

$\rightsquigarrow$ construction **explicite** de codes correcteurs "subspace" avec des bonnes propriétés.

La conjecture de Etzion et Silberstein

La conjecture est vraie dans les cas les plus importants pour les applications.

Théorème (Gorla-Ravagnani)

Soit $\mathscr{F}$ un diagramme de Ferrers où les lignes ont cardinalité $r_1, r_2, ..., r_n$. La conjecture de Etzion-Silberstein est vraie dans les cas suivants:

- $r_{\delta-1} \geq n$,
- $\delta = n = m$ sont pairs et $C_n(\mathscr{F}) = n/2$,
- $\delta = n = m$ et $C_n(\mathscr{F}) = n-1$,
- $r_i \geq m-i+1$ pour $i = 1, ..., \delta$ et $r_i \leq m-i+1$ pour $i = \delta, ..., n$ et $q = |\mathbb{F}_q| \geq n-1$.

$\rightsquigarrow$ construction **explicite** de codes correcteurs "subspace" avec des bonnes propriétés.

Merci beaucoup!