# Codes correcteurs d'erreurs, formes quadratiques entières : des analogies inattendues

Michel Broué

Université Paris-Diderot Paris 7
CNRS–IMJ-PRG

École normale supérieure, 10 décembre 2014

# Codes correcteurs d'erreurs

# Codes correcteurs d'erreurs

*« Allo Papa Tango Charlie ? »* ...

# Codes correcteurs d'erreurs

« *Allo Papa Tango Charlie ?* » ... signifie « A P T C ».

# Codes correcteurs d'erreurs

« *Allo Papa Tango Charlie ?* » ... signifie « A P T C ».

= Le code consiste ici à « ajouter de la redondance à l'information ».

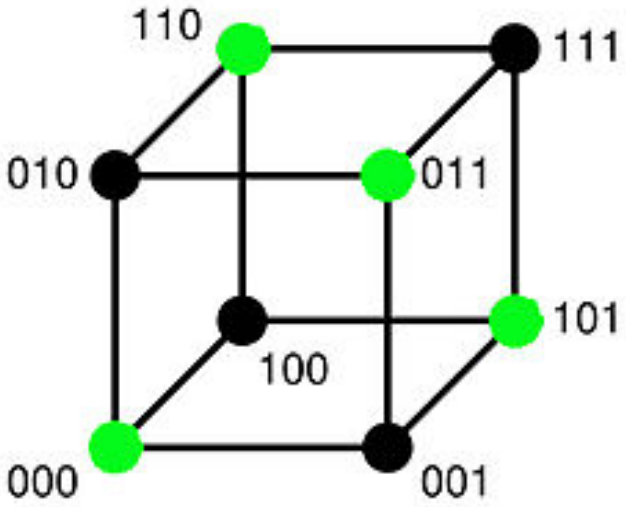
Une suite de n « 0 » et de « 1 » (ou de bips et non-bips) correspond

Une suite de n « 0 » et de « 1 » (ou de bips et non-bips) correspond

- à un vecteur de l'espace vectoriel $\mathbb{F}_2^n$ :

Une suite de n « 0 » et de « 1 » (ou de bips et non-bips) correspond

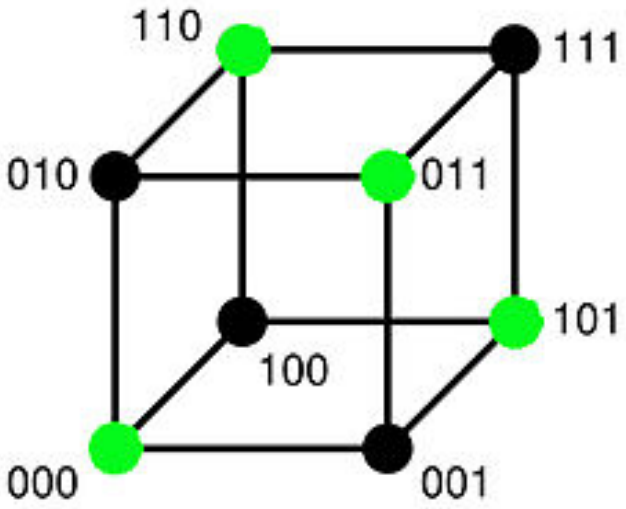
- à un vecteur de l'espace vectoriel $\mathbb{F}_2^n$ :




(ici $n = 3$)

Une suite de n « 0 » et de « 1 » (ou de bips et non-bips) correspond

- à un vecteur de l'espace vectoriel $\mathbb{F}_2^n$ :



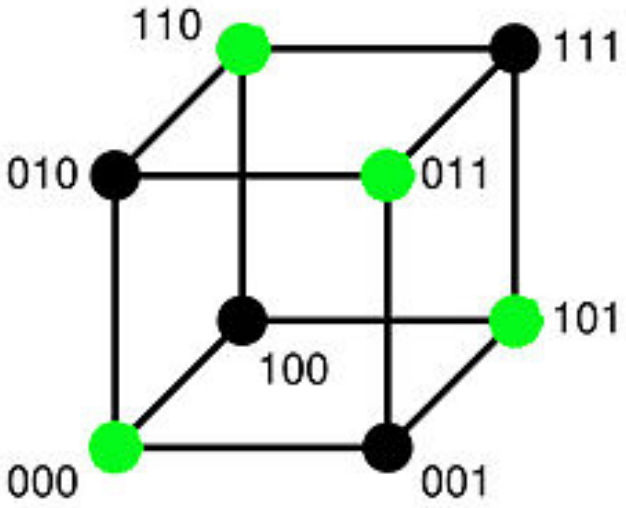

(ici $n = 3$)

en vert, les points de l'hyperplan noyau de la forme linéaire

$$s : \mathbb{F}_2^n \to \mathbb{F}_2 \ , \ \sum_{i=1}^{n} \lambda_i e_i \mapsto \sum_{i=1}^{n} \lambda_i \ ,$$

Une suite de n « 0 » et de « 1 » (ou de bips et non-bips) correspond

- à un vecteur de l'espace vectoriel $\mathbb{F}_2^n$ :




(ici $n = 3$)

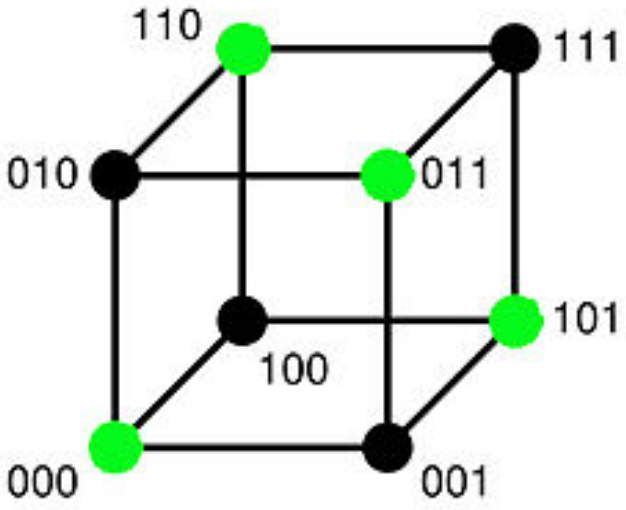
en vert, les points de l'hyperplan noyau de la forme linéaire

$$s : \mathbb{F}_2^n \to \mathbb{F}_2 \ , \ \sum_{i=1}^{n} \lambda_i e_i \mapsto \sum_{i=1}^{n} \lambda_i \ ,$$

- à un sous-ensemble d'un ensemble à n éléments :

Une suite de n « 0 » et de « 1 » (ou de bips et non-bips) correspond

- à un vecteur de l'espace vectoriel $\mathbb{F}_2^n$ :




(ici $n = 3$)

en vert, les points de l'hyperplan noyau de la forme linéaire

$$s : \mathbb{F}_2^n \to \mathbb{F}_2 \ , \ \sum_{i=1}^{n} \lambda_i e_i \mapsto \sum_{i=1}^{n} \lambda_i \ ,$$

- à un sous-ensemble d'un ensemble à n éléments :

en vert, l'ensemble des parties paires.

# Codes correcteurs

# Codes correcteurs

Soit $\Omega$ un ensemble fini de cardinal $n$. L'ensemble des parties de $\Omega$, muni de l'opération *différence symétrique*

$$x + y := (x \cup y) - (x \cap y)$$

est un espace vectoriel sur $\mathbb{F}_2$, naturellement isomorphe à $\mathbb{F}_2^{\Omega}$.

On le note $\mathcal{P}(\Omega)$.

# Codes correcteurs

Soit $\Omega$ un ensemble fini de cardinal $n$. L'ensemble des parties de $\Omega$, muni de l'opération *différence symétrique*

$$x + y := (x \cup y) - (x \cap y)$$

est un espace vectoriel sur $\mathbb{F}_2$, naturellement isomorphe à $\mathbb{F}_2^{\Omega}$.

On le note $\mathcal{P}(\Omega)$.

**(1)** Il existe une et une seule forme linéaire non triviale sur $\mathcal{P}(\Omega)$ invariante par l'action du groupe symétrique $\mathfrak{S}(\Omega)$, à savoir la forme

$$\boxed{s : \mathcal{P}(\Omega) \longrightarrow \mathbb{F}_2 \quad , \quad x \mapsto |x| \mod 2\,.}$$

# Codes correcteurs

Soit $\Omega$ un ensemble fini de cardinal $n$. L'ensemble des parties de $\Omega$, muni de l'opération *différence symétrique*

$$x + y := (x \cup y) - (x \cap y)$$

est un espace vectoriel sur $\mathbb{F}_2$, naturellement isomorphe à $\mathbb{F}_2^{\Omega}$.

On le note $\mathcal{P}(\Omega)$.

**(1)** Il existe une et une seule forme linéaire non triviale sur $\mathcal{P}(\Omega)$ invariante par l'action du groupe symétrique $\mathfrak{S}(\Omega)$, à savoir la forme

$$\boxed{s : \mathcal{P}(\Omega) \longrightarrow \mathbb{F}_2 \quad , \quad x \mapsto |x| \mod 2\,.}$$

Le noyau de $s$ est l'hyperplan $\mathcal{H}(\Omega)$, ensemble des parties de cardinal pair de $\Omega$.

# Codes correcteurs – suite

**(2)** Les *formes quadratiques* non nulles invariantes par $\mathfrak{S}(\Omega)$ ont toutes même restriction, notée $q$, à l'hyperplan $\mathcal{H}(\Omega)$, où

$$\boxed{q(x) = \frac{|x|}{2} \mod 2 \quad \text{pour tout } x \in \mathcal{H}(\Omega)\,,}$$

# Codes correcteurs – suite

**(2)** Les *formes quadratiques* non nulles invariantes par $\mathfrak{S}(\Omega)$ ont toutes même restriction, notée $q$, à l'hyperplan $\mathcal{H}(\Omega)$, où

$$\boxed{q(x) = \frac{|x|}{2} \mod 2 \quad \text{pour tout } x \in \mathcal{H}(\Omega)\,,}$$

et

$$\boxed{q(x+y) - q(x) - q(y) = |x \cap y| \mod 2 \quad \text{pour tous } x, y \in \mathcal{H}(\Omega)\,.}$$

# Codes correcteurs – suite

**(2)** Les *formes quadratiques* non nulles invariantes par $\mathfrak{S}(\Omega)$ ont toutes même restriction, notée $q$, à l'hyperplan $\mathcal{H}(\Omega)$, où

$$\boxed{q(x) = \frac{|x|}{2} \mod 2 \quad \text{pour tout } x \in \mathcal{H}(\Omega)\,,}$$

et

$$\boxed{q(x+y) - q(x) - q(y) = |x \cap y| \mod 2 \quad \text{pour tous } x, y \in \mathcal{H}(\Omega)\,.}$$

**(3)** C'est un exercice d'algèbre linéaire que de classifier $(\mathcal{H}(\Omega), q)$.

# Codes autoduaux pairs

# Codes autoduaux pairs

- Un *code correcteur d'erreurs* est un sous–espace vectoriel $\mathcal{E}$ de $\mathcal{P}(\Omega)$.

# Codes autoduaux pairs

- Un *code correcteur d'erreurs* est un sous–espace vectoriel $\mathcal{E}$ de $\mathcal{P}(\Omega)$.
- Un code $\mathcal{E}$ est dit *entier* s'il est contenu dans son orthogonal $\mathcal{E}^0$.
  Un code $\mathcal{E}$ est dit *autodual* s'il est égal son orthogonal $\mathcal{E}^0$.

# Codes autoduaux pairs

- Un *code correcteur d'erreurs* est un sous–espace vectoriel $\mathcal{E}$ de $\mathcal{P}(\Omega)$.
- Un code $\mathcal{E}$ est dit *entier* s'il est contenu dans son orthogonal $\mathcal{E}^0$.
  Un code $\mathcal{E}$ est dit *autodual* s'il est égal son orthogonal $\mathcal{E}^0$.

  Ainsi, un code $\mathcal{E}$ est entier si et seulement si, pour tous $x, y \in \mathcal{E}$, $|x \cap y|$ est pair. En particulier, on a $\mathcal{E} \subseteq \mathcal{H}(\Omega)$.

# Codes autoduaux pairs

- Un *code correcteur d'erreurs* est un sous–espace vectoriel $\mathcal{E}$ de $\mathcal{P}(\Omega)$.
- Un code $\mathcal{E}$ est dit *entier* s'il est contenu dans son orthogonal $\mathcal{E}^0$.
  Un code $\mathcal{E}$ est dit *autodual* s'il est égal son orthogonal $\mathcal{E}^0$.

  Ainsi, un code $\mathcal{E}$ est entier si et seulement si, pour tous $x, y \in \mathcal{E}$, $|x \cap y|$ est pair. En particulier, on a $\mathcal{E} \subseteq \mathcal{H}(\Omega)$.
- Un code $\mathcal{E}$ est dit *pair* si, pour tout $x \in \mathcal{E}$, $|x|$ est divisible par 4.

# Codes autoduaux pairs

- Un *code correcteur d'erreurs* est un sous–espace vectoriel $\mathcal{E}$ de $\mathcal{P}(\Omega)$.
- Un code $\mathcal{E}$ est dit *entier* s'il est contenu dans son orthogonal $\mathcal{E}^0$.
  Un code $\mathcal{E}$ est dit *autodual* s'il est égal son orthogonal $\mathcal{E}^0$.

  Ainsi, un code $\mathcal{E}$ est entier si et seulement si, pour tous $x, y \in \mathcal{E}$, $|x \cap y|$ est pair. En particulier, on a $\mathcal{E} \subseteq \mathcal{H}(\Omega)$.
- Un code $\mathcal{E}$ est dit *pair* si, pour tout $x \in \mathcal{E}$, $|x|$ est divisible par 4.

  Un code pair est contenu dans $\mathcal{H}(\Omega)$, et totalement singulier pour la forme quadratique $q$, donc il est entier.

# Un exemple de Codes autoduaux pairs

# Un exemple de Codes autoduaux pairs

- Supposons $n$ multiple de 4, posons $n = 2m$, et
$$\Omega := \{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_m\}.$$

# Un exemple de Codes autoduaux pairs

- Supposons $n$ multiple de 4, posons $n = 2m$, et
$$\Omega := \{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_m\}.$$
- Le code $\mathcal{E}_n$ est par définition le code engendré par tous les éléments de la forme
$$x_{i,j} := \{\alpha_i, \alpha_j, \beta_i, \beta_j\}_{1 \leq i \neq j \leq m} \quad \text{et} \quad \{\alpha_1, \alpha_2, \ldots, \alpha_m\}.$$

# Un exemple de Codes autoduaux pairs

- Supposons $n$ multiple de 4, posons $n = 2m$, et
$$\Omega := \{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_m\}.$$
- Le code $\mathcal{E}_n$ est par définition le code engendré par tous les éléments de la forme
$$x_{i,j} := \{\alpha_i, \alpha_j, \beta_i, \beta_j\}_{1 \leq i \neq j \leq m} \quad \text{et} \quad \{\alpha_1, \alpha_2, \ldots, \alpha_m\}.$$

## Exercice

1. $\mathcal{E}_n$ est entier, et autodual si $m$ est pair.
2. Il est pair et autodual si $m$ est multiple de 4, *i.e.*,

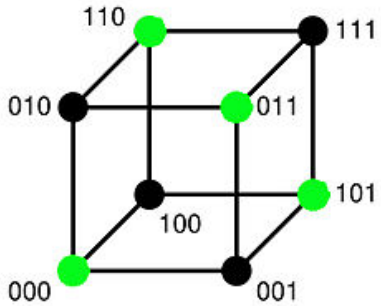
si $n$ est multiple de 8.

# Si $n$ est multiple de 8

Cas particulier : Pour $n = 8$, considérant $\Omega$ comme l'ensemble sous-jacent à l'espace affine de dimension 3 sur le corps $\mathbb{F}_2$, le code $\mathcal{E}_8$ est formé de $\Omega$, $\emptyset$, et des 14 plans affines.

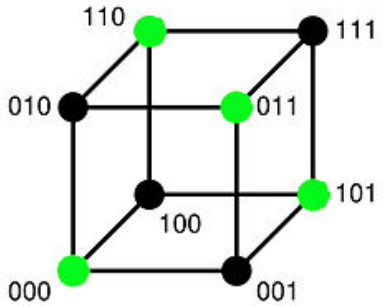
# Si $n$ est multiple de 8

Cas particulier : Pour $n = 8$, considérant $\Omega$ comme l'ensemble sous-jacent à l'espace affine de dimension 3 sur le corps $\mathbb{F}_2$, le code $\mathcal{E}_8$ est formé de $\Omega$, $\emptyset$, et des 14 plans affines.



# Si $n$ est multiple de 8

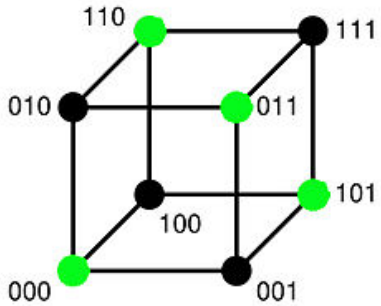
Cas particulier : Pour $n = 8$, considérant $\Omega$ comme l'ensemble sous-jacent à l'espace affine de dimension 3 sur le corps $\mathbb{F}_2$, le code $\mathcal{E}_8$ est formé de $\Omega$, $\emptyset$, et des 14 plans affines.




Le résultat suivant se déduit de la classification des paires $(\mathcal{H}(\Omega), q)$.

# Si $n$ est multiple de 8

Cas particulier : Pour $n = 8$, considérant $\Omega$ comme l'ensemble sous-jacent à l'espace affine de dimension 3 sur le corps $\mathbb{F}_2$, le code $\mathcal{E}_8$ est formé de $\Omega$, $\emptyset$, et des 14 plans affines.




Le résultat suivant se déduit de la classification des paires $(\mathcal{H}(\Omega), q)$.

**Théorème**

Il existe un code autodual et pair dans $\mathcal{P}(\Omega)$ si et seulement si

$$n \equiv 0 \mod 8 .$$

# Réseaux

- $\mathbb{Q}^n$ est muni de son produit scalaire naturel $(x, y) \mapsto \langle x, y \rangle$.

# Réseaux

- $\mathbb{Q}^n$ est muni de son produit scalaire naturel $(x, y) \mapsto \langle x, y \rangle$.
  On pose $x^2 := \langle x, x \rangle$.

# Réseaux

- $\mathbb{Q}^n$ est muni de son produit scalaire naturel $(x, y) \mapsto \langle x, y \rangle$.
  On pose $x^2 := \langle x, x \rangle$.
- Un *réseau $L$ de $\mathbb{Q}^n$* est un sous–groupe additif de $\mathbb{Q}^n$ engendré par une base de $\mathbb{Q}^n$.

# Réseaux

- $\mathbb{Q}^n$ est muni de son produit scalaire naturel $(x, y) \mapsto \langle x, y \rangle$.
  On pose $x^2 := \langle x, x \rangle$.
- Un *réseau $L$ de $\mathbb{Q}^n$* est un sous–groupe additif de $\mathbb{Q}^n$ engendré par une base de $\mathbb{Q}^n$.
- Le *réseau dual $L^0$ de $L$* est l'ensemble des éléments $y \in \mathbb{Q}^n$ tels que $\langle x, y \rangle \in \mathbb{Z}$ pour tout $x \in L$.

# Réseaux

- $\mathbb{Q}^n$ est muni de son produit scalaire naturel $(x, y) \mapsto \langle x, y \rangle$.
  On pose $x^2 := \langle x, x \rangle$.
- Un *réseau $L$ de $\mathbb{Q}^n$* est un sous–groupe additif de $\mathbb{Q}^n$ engendré par une base de $\mathbb{Q}^n$.
- Le *réseau dual $L^0$ de $L$* est l'ensemble des éléments $y \in \mathbb{Q}^n$ tels que $\langle x, y \rangle \in \mathbb{Z}$ pour tout $x \in L$.
  On a $L^{00} = L$.

# Réseaux

- $\mathbb{Q}^n$ est muni de son produit scalaire naturel $(x, y) \mapsto \langle x, y \rangle$.
  On pose $x^2 := \langle x, x \rangle$.
- Un *réseau $L$ de $\mathbb{Q}^n$* est un sous–groupe additif de $\mathbb{Q}^n$ engendré par une base de $\mathbb{Q}^n$.
- Le *réseau dual $L^0$ de $L$* est l'ensemble des éléments $y \in \mathbb{Q}^n$ tels que $\langle x, y \rangle \in \mathbb{Z}$ pour tout $x \in L$.
  On a $L^{00} = L$.
- Le volume $\mathrm{vol}(L)$ de $L$ est la valeur absolue du déterminant d'une base de $L$ par rapport à une base orthonormale de $\mathbb{Q}^n$.

# Réseaux

- $\mathbb{Q}^n$ est muni de son produit scalaire naturel $(x, y) \mapsto \langle x, y \rangle$.
  On pose $x^2 := \langle x, x \rangle$.
- Un *réseau $L$ de $\mathbb{Q}^n$* est un sous–groupe additif de $\mathbb{Q}^n$ engendré par une base de $\mathbb{Q}^n$.
- Le *réseau dual $L^0$ de $L$* est l'ensemble des éléments $y \in \mathbb{Q}^n$ tels que $\langle x, y \rangle \in \mathbb{Z}$ pour tout $x \in L$.
  On a $L^{00} = L$.
- Le volume $\mathrm{vol}(L)$ de $L$ est la valeur absolue du déterminant d'une base de $L$ par rapport à une base orthonormale de $\mathbb{Q}^n$.
  On a
$$\mathrm{vol}(L)\mathrm{vol}(L^0) = 1\,.$$

# Réseaux et formes quadratiques entières

# Réseaux et formes quadratiques entières

- Un réseau $L$ est dit *entier* si $L \subseteq L^0$.

# Réseaux et formes quadratiques entières

- Un réseau $L$ est dit *entier* si $L \subseteq L^0$.

  Les réseaux entiers définissent des formes quadratiques entières.

# Réseaux et formes quadratiques entières

- Un réseau $L$ est dit *entier* si $L \subseteq L^0$.

  Les réseaux entiers définissent des formes quadratiques entières.

- $L$ est dit *unimodulaire* si $L = L^0$.

# Réseaux et formes quadratiques entières

- Un réseau $L$ est dit *entier* si $L \subseteq L^0$.

  Les réseaux entiers définissent des formes quadratiques entières.

- $L$ est dit *unimodulaire* si $L = L^0$.

- Il est dit *pair* si $x^2 \in 2\mathbb{Z}$ pour tout $x \in L$ (un réseau pair est entier).

# Réseaux et formes quadratiques entières

- Un réseau $L$ est dit *entier* si $L \subseteq L^0$.

  Les réseaux entiers définissent des formes quadratiques entières.

- $L$ est dit *unimodulaire* si $L = L^0$.

- Il est dit *pair* si $x^2 \in 2\mathbb{Z}$ pour tout $x \in L$ (un réseau pair est entier).

**Rappel : Théorème**

Il existe un code autodual et pair dans $\mathcal{P}(\Omega)$ si et seulement si

$$n \equiv 0 \mod 8\,.$$

# Réseaux et formes quadratiques entières

- Un réseau $L$ est dit *entier* si $L \subseteq L^0$.

  Les réseaux entiers définissent des formes quadratiques entières.

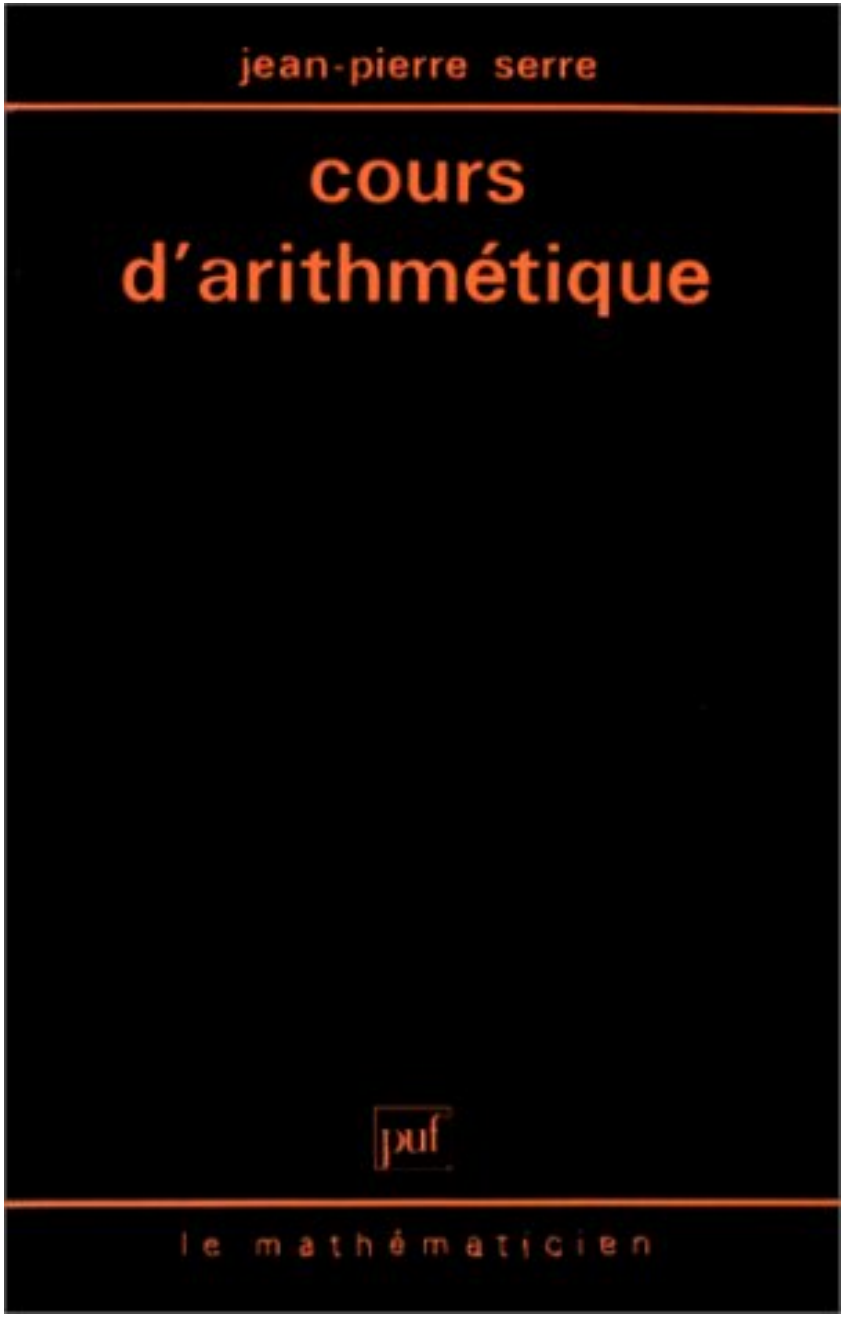
- $L$ est dit *unimodulaire* si $L = L^0$.

- Il est dit *pair* si $x^2 \in 2\mathbb{Z}$ pour tout $x \in L$ (un réseau pair est entier).

**Théorème : si $n$ est multiple de 8**

Il existe un réseau unimodulaire pair dans $\mathbb{Q}^n$ si et seulement si

$$n \equiv 0 \mod 8\,.$$


jean-pierre serre
cours
d'arithmétique
puf
le mathématicien

# Un exemple de réseau unimodulaire pair

# Un exemple de réseau unimodulaire pair

- Supposons $n \equiv 0 \bmod 4$.

# Un exemple de réseau unimodulaire pair

- Supposons $n \equiv 0 \bmod 4$.
- Soit $(v_1, v_2, \ldots, v_n)$ une base orthogonale avec $v_i^2 = 1/4$, et soit $R$ le réseau de base $(v_1, v_2, \ldots, v_n)$.

# Un exemple de réseau unimodulaire pair

- Supposons $n \equiv 0 \mod 4$.
- Soit $(v_1, v_2, \ldots, v_n)$ une base orthogonale avec $v_i^2 = 1/4$, et soit $R$ le réseau de base $(v_1, v_2, \ldots, v_n)$.
- Le réseau $\Lambda_n \subset R$ est

$$\Lambda_n := \left\{ \sum_{i=1}^{i=n} a_i v_i \mid (\forall i,\ a_i \equiv a_1 \mod 2) \text{ et } (\sum_i a_i \equiv 0 \mod 4) \right\} .$$

# Un exemple de réseau unimodulaire pair

- Supposons $n \equiv 0 \mod 4$.
- Soit $(v_1, v_2, \ldots, v_n)$ une base orthogonale avec $v_i^2 = 1/4$, et soit $R$ le réseau de base $(v_1, v_2, \ldots, v_n)$.
- Le réseau $\Lambda_n \subset R$ est

$$\Lambda_n := \left\{ \sum_{i=1}^{i=n} a_i v_i \mid (\forall i,\ a_i \equiv a_1 \mod 2) \text{ et } (\sum_i a_i \equiv 0 \mod 4) \right\}.$$

## Exercice

1. Le réseau $\Lambda_n$ est unimodulaire.
2. Si de plus $n$ est divisible par 8, le réseau $\Lambda_n$ est pair.

# Polynôme des poids d'un code

# Polynôme des poids d'un code

Le *polynôme des poids* d'un code $\mathcal{E}$ est par définition

$$P_{\mathcal{E}}(X,Y) := \sum_{x \in \mathcal{E}} X^{|x|} Y^{n-|x|} = \sum_{j=0}^{n} |\mathcal{E}_k|(\mathcal{E}) X^k Y^{n-k} .$$

# Polynôme des poids d'un code

Le *polynôme des poids* d'un code $\mathcal{E}$ est par définition

$$P_{\mathcal{E}}(X,Y) := \sum_{x\in\mathcal{E}} X^{|x|}\,Y^{n-|x|} = \sum_{j=0}^{n} |\mathcal{E}_k|(\mathcal{E})X^k\,Y^{n-k}\,.$$

## Théorème : Formule de MacWilliams

Supposons $n = 2m$, où $m$ est un entier. Pour tout code $\mathcal{E}$ dans $\mathcal{P}(\Omega)$,

$$P_{\mathcal{E}^0}(X,Y) = 2^{m-\dim\mathcal{E}}\,P_{\mathcal{E}}((-X+Y)/\sqrt{2},(X+Y)/\sqrt{2})\,.$$

# Polynôme des poids d'un code

Le *polynôme des poids* d'un code $\mathcal{E}$ est par définition

$$P_{\mathcal{E}}(X,Y) := \sum_{x\in\mathcal{E}} X^{|x|}\,Y^{n-|x|} = \sum_{j=0}^{n} |\mathcal{E}_k|(\mathcal{E})X^k\,Y^{n-k}\,.$$

## Théorème : Formule de MacWilliams

Supposons $n = 2m$, où $m$ est un entier. Pour tout code $\mathcal{E}$ dans $\mathcal{P}(\Omega)$,

$$P_{\mathcal{E}^0}(X,Y) = 2^{m-\dim\mathcal{E}}\,P_{\mathcal{E}}((-X+Y)/\sqrt{2},(X+Y)/\sqrt{2})\,.$$

Si $P(X,Y)\in\mathbb{C}[X,Y]$ et si $g := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est une matrice à coefficients complexes, on note $P\cdot g$ le polynôme défini par

$$(P\cdot g)(X,Y) := P(aX+bY, cX+dY)\,.$$

# Algèbre des polynômes des poids

## Corollaire

Si $\mathcal{E}$ est un code autodual pair, alors son polynôme des poids est invariant par l'action (à droite) du sous–groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par les deux matrices

$$\rho := \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \sigma := \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

# Algèbre des polynômes des poids

## Corollaire

Si $\mathcal{E}$ est un code autodual pair, alors son polynôme des poids est invariant par l'action (à droite) du sous–groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par les deux matrices

$$\rho := \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \sigma := \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} .$$

- Les deux matrices $\rho$ et $\sigma$ représentent des *pseudo–réflexions* (*i.e.*,des automorphismes d'ordre fini dont l'espace des points fixes est un hyperplan),

# Algèbre des polynômes des poids

## Corollaire

Si $\mathcal{E}$ est un code autodual pair, alors son polynôme des poids est invariant par l'action (à droite) du sous–groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par les deux matrices

$$\rho := \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \sigma := \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

- Les deux matrices $\rho$ et $\sigma$ représentent des *pseudo–réflexions* (*i.e.*,des automorphismes d'ordre fini dont l'espace des points fixes est un hyperplan),
- le groupe $W$ qu'elles engendrent est un groupe *fini* : c'est un *groupe de réflexions complexes* d'ordre 192

# Algèbre des polynômes des poids

## Corollaire

Si $\mathcal{E}$ est un code autodual pair, alors son polynôme des poids est invariant par l'action (à droite) du sous–groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par les deux matrices

$$\rho := \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \sigma := \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

- Les deux matrices $\rho$ et $\sigma$ représentent des *pseudo–réflexions* (*i.e.*,des automorphismes d'ordre fini dont l'espace des points fixes est un hyperplan),
- le groupe $W$ qu'elles engendrent est un groupe *fini* : c'est un *groupe de réflexions complexes* d'ordre 192 ($192 = 8 \times 24$).

# Algèbre des polynômes des poids

## Corollaire

Si $\mathcal{E}$ est un code autodual pair, alors son polynôme des poids est invariant par l'action (à droite) du sous–groupe de $\mathrm{GL}_2(\mathbb{C})$ engendré par les deux matrices

$$\rho := \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \sigma := \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} .$$

- Les deux matrices $\rho$ et $\sigma$ représentent des *pseudo–réflexions* (*i.e.*,des automorphismes d'ordre fini dont l'espace des points fixes est un hyperplan),
- le groupe $W$ qu'elles engendrent est un groupe *fini* : c'est un *groupe de réflexions complexes* d'ordre 192 ($192 = 8 \times 24$).

$\rightsquigarrow$ GROUPES DE RÉFLEXIONS ...

# Groupes de réflexions

Soit $G$ un sous-groupe fini de $\mathrm{GL}_r(\mathbb{C})$, qui opère sur $\mathbb{C}[X_1, \ldots, X_r]$ :

# Groupes de réflexions

Soit $G$ un sous-groupe fini de $\mathrm{GL}_r(\mathbb{C})$, qui opère sur $\mathbb{C}[X_1, \ldots, X_r]$ :

$$P \cdot (a_{i,j})(X_1, \ldots, X_r) := P(\sum_j a_{1,j} X_j, \ldots, \sum_j a_{r,j} X_j)\,.$$

# Groupes de réflexions

Soit $G$ un sous-groupe fini de $\mathrm{GL}_r(\mathbb{C})$, qui opère sur $\mathbb{C}[X_1, \ldots, X_r]$ :

$$P \cdot (a_{i,j})(X_1, \ldots, X_r) := P(\sum_j a_{1,j} X_j, \ldots, \sum_j a_{r,j} X_j)\,.$$

## Théorème (Shephard–Todd, Chevalley, Serre)

Les assertions suivantes sont équivalentes :

# Groupes de réflexions

Soit $G$ un sous-groupe fini de $\mathrm{GL}_r(\mathbb{C})$, qui opère sur $\mathbb{C}[X_1, \ldots, X_r]$ :

$$P \cdot (a_{i,j})(X_1, \ldots, X_r) := P(\sum_j a_{1,j} X_j, \ldots, \sum_j a_{r,j} X_j)\,.$$

## Théorème (Shephard–Todd, Chevalley, Serre)

Les assertions suivantes sont équivalentes :

(i) $G$ est engendré par des pseudo-réflexions.

# Groupes de réflexions

Soit $G$ un sous-groupe fini de $\mathrm{GL}_r(\mathbb{C})$, qui opère sur $\mathbb{C}[X_1, \ldots, X_r]$ :

$$P \cdot (a_{i,j})(X_1, \ldots, X_r) := P(\sum_j a_{1,j} X_j, \ldots, \sum_j a_{r,j} X_j)\,.$$

## Théorème (Shephard–Todd, Chevalley, Serre)

Les assertions suivantes sont équivalentes :

(i) $G$ est engendré par des pseudo-réflexions.

(ii) La sous-algèbre $\mathbb{C}^G[X_1, \ldots, X_r]$ des polynômes fixes par l'action de $G$ est isomorphe à une algèbre de polynômes.

# Groupes de réflexions

Soit $G$ un sous-groupe fini de $\mathrm{GL}_r(\mathbb{C})$, qui opère sur $\mathbb{C}[X_1, \ldots, X_r]$ :

$$P \cdot (a_{i,j})(X_1, \ldots, X_r) := P(\sum_j a_{1,j} X_j, \ldots, \sum_j a_{r,j} X_j)\,.$$

## Théorème (Shephard–Todd, Chevalley, Serre)

Les assertions suivantes sont équivalentes :

(i) $G$ est engendré par des pseudo-réflexions.

(ii) La sous-algèbre $\mathbb{C}^G[X_1, \ldots, X_r]$ des polynômes fixes par l'action de $G$ est isomorphe à une algèbre de polynômes.

Alors

# Groupes de réflexions

Soit $G$ un sous-groupe fini de $\mathrm{GL}_r(\mathbb{C})$, qui opère sur $\mathbb{C}[X_1, \ldots, X_r]$ :

$$P \cdot (a_{i,j})(X_1, \ldots, X_r) := P(\sum_j a_{1,j} X_j, \ldots, \sum_j a_{r,j} X_j)\,.$$

## Théorème (Shephard–Todd, Chevalley, Serre)

Les assertions suivantes sont équivalentes :

(i) $G$ est engendré par des pseudo-réflexions.

(ii) La sous-algèbre $\mathbb{C}^G[X_1, \ldots, X_r]$ des polynômes fixes par l'action de $G$ est isomorphe à une algèbre de polynômes.

Alors

1. Il existe $r$ éléments homogènes algébriquement indépendants $I_1, \ldots, I_r$ de $\mathbb{C}^G[X_1, \ldots, X_r]$ tels que $\mathbb{C}^G[X_1, \ldots, X_r] = \mathbb{C}[I_1, \ldots, I_r]$,

# Groupes de réflexions

Soit $G$ un sous-groupe fini de $\mathrm{GL}_r(\mathbb{C})$, qui opère sur $\mathbb{C}[X_1, \ldots, X_r]$ :

$$P \cdot (a_{i,j})(X_1, \ldots, X_r) := P(\sum_j a_{1,j} X_j, \ldots, \sum_j a_{r,j} X_j)\,.$$

## Théorème (Shephard–Todd, Chevalley, Serre)

Les assertions suivantes sont équivalentes :

(i) $G$ est engendré par des pseudo-réflexions.

(ii) La sous-algèbre $\mathbb{C}^G[X_1, \ldots, X_r]$ des polynômes fixes par l'action de $G$ est isomorphe à une algèbre de polynômes.

Alors

1. Il existe $r$ éléments homogènes algébriquement indépendants $I_1, \ldots, I_r$ de $\mathbb{C}^G[X_1, \ldots, X_r]$ tels que $\mathbb{C}^G[X_1, \ldots, X_r] = \mathbb{C}[I_1, \ldots, I_r]$,
2. si $d_1, \ldots, d_r$ sont les degrés respectifs de $I_1, \ldots, I_r$, on a $|G| = d_1 \cdots d_r$.

# Algèbre des polynômes des poids – suite

- $|W| = 192 = 8 \times 24$, et l'algèbre $\mathbb{C}^W[X, Y]$ des polynômes invariants par l'action de $W$ est une *algèbre de polynômes*, engendrée par deux éléments algébriquement indépendants, homogènes et de degrés respectifs 8 et 24.

# Algèbre des polynômes des poids – suite

- $|W| = 192 = 8 \times 24$, et l'algèbre $\mathbb{C}^W[X, Y]$ des polynômes invariants par l'action de $W$ est une *algèbre de polynômes*, engendrée par deux éléments algébriquement indépendants, homogènes et de degrés respectifs 8 et 24.
- La dimension de l'espace vectoriel des polynômes homogènes de degré $n$ invariants par $W$ est $1 + [n/24]$.

# Algèbre des polynômes des poids – suite

- $|W| = 192 = 8 \times 24$, et l'algèbre $\mathbb{C}^W[X, Y]$ des polynômes invariants par l'action de $W$ est une *algèbre de polynômes*, engendrée par deux éléments algébriquement indépendants, homogènes et de degrés respectifs 8 et 24.
- La dimension de l'espace vectoriel des polynômes homogènes de degré $n$ invariants par $W$ est $1 + [n/24]$.

## Théorème : Où vit le polynôme des poids

# Algèbre des polynômes des poids – suite

- $|W| = 192 = 8 \times 24$, et l'algèbre $\mathbb{C}^W[X, Y]$ des polynômes invariants par l'action de $W$ est une *algèbre de polynômes*, engendrée par deux éléments algébriquement indépendants, homogènes et de degrés respectifs 8 et 24.
- La dimension de l'espace vectoriel des polynômes homogènes de degré $n$ invariants par $W$ est $1 + [n/24]$.

## Théorème : Où vit le polynôme des poids

1. Le polynôme des poids d'un code autodual pair appartient à l'algèbre $\mathbb{Z}^W[X, Y]$ des polynômes à coefficients *entiers* et invariants par $W$,

# Algèbre des polynômes des poids – suite

- $|W| = 192 = 8 \times 24$, et l'algèbre $\mathbb{C}^W[X, Y]$ des polynômes invariants par l'action de $W$ est une *algèbre de polynômes*, engendrée par deux éléments algébriquement indépendants, homogènes et de degrés respectifs 8 et 24.
- La dimension de l'espace vectoriel des polynômes homogènes de degré $n$ invariants par $W$ est $1 + [n/24]$.

## Théorème : Où vit le polynôme des poids

1. Le polynôme des poids d'un code autodual pair appartient à l'algèbre $\mathbb{Z}^W[X, Y]$ des polynômes à coefficients *entiers* et invariants par $W$,
2. On a $\mathbb{Z}^W[X, Y] = \mathbb{Z}[A(X, Y), D(X, Y])$ où

$$A(X, Y) := X^8 + 14X^4Y^4 + Y^8 \quad \text{et} \quad D(X, Y) := X^4Y^4(X^4 - Y^4)^4 .$$

## Corollaire

## Corollaire

1. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual et pair en dimension 8, à savoir le polynôme

$$A(X, Y) = X^8 + 14X^4Y^4 + Y^8 .$$

## Corollaire

1. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual et pair en dimension 8, à savoir le polynôme
$$A(X,Y) = X^8 + 14X^4Y^4 + Y^8 .$$
2. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual et pair en dimension 24 ne contenant aucun vecteur de poids 4, à savoir le polynôme
$$B(X,Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24} .$$

## Corollaire

1. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual et pair en dimension 8, à savoir le polynôme
$$A(X,Y) = X^8 + 14X^4Y^4 + Y^8 .$$
2. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual et pair en dimension 24 ne contenant aucun vecteur de poids 4, à savoir le polynôme
$$B(X,Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24} .$$

## Théorème : Existence des codes « sans petits vecteurs »

## Corollaire

1. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual et pair en dimension 8, à savoir le polynôme
$$A(X,Y) = X^8 + 14X^4Y^4 + Y^8 .$$
2. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual et pair en dimension 24 ne contenant aucun vecteur de poids 4, à savoir le polynôme
$$B(X,Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24} .$$

## Théorème : Existence des codes « sans petits vecteurs »

1. Il existe un et un seul (à isomorphisme près) code autodual pair en dimension 8, de polynôme des poids $A(X,Y) = X^8 + 14X^4Y^4 + Y^8$ .

## Corollaire

1. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual et pair en dimension 8, à savoir le polynôme
$$A(X,Y) = X^8 + 14X^4Y^4 + Y^8 .$$
2. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual et pair en dimension 24 ne contenant aucun vecteur de poids 4, à savoir le polynôme
$$B(X,Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24} .$$

## Théorème : Existence des codes « sans petits vecteurs »

1. Il existe un et un seul (à isomorphisme près) code autodual pair en dimension 8, de polynôme des poids $A(X,Y) = X^8 + 14X^4Y^4 + Y^8$ .
2. Il existe un et un seul (à isomorphisme près) code autodual pair en dimension 24, de polynôme des poids
$$B(X,Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24} .$$
appelé le *Code de Golay*.

## Corollaire

1. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual et pair en dimension 8, à savoir le polynôme
$$A(X,Y) = X^8 + 14X^4Y^4 + Y^8 .$$
2. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual et pair en dimension 24 ne contenant aucun vecteur de poids 4, à savoir le polynôme
$$B(X,Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24} .$$

## Théorème : Existence des codes « sans petits vecteurs »

1. Il existe un et un seul (à isomorphisme près) code autodual pair en dimension 8, de polynôme des poids $A(X,Y) = X^8 + 14X^4Y^4 + Y^8$ .
2. Il existe un et un seul (à isomorphisme près) code autodual pair en dimension 24, de polynôme des poids
$$B(X,Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24} .$$
appelé le *Code de Golay*. (Nous y reviendrons plus loin)

# Fonction thêta d'un réseau

# Fonction thêta d'un réseau

La fonction thêta d'un réseau $L$ de $\mathbb{Q}^n$ est par définition la fonction définie sur le demi–plan de Poincaré $\{z \in \mathbb{C} \mid (\mathrm{im}\,(z) > 0)\}$ par

$$\boxed{\Theta_L(z) := \sum_{x \in L} e^{\pi i x^2 z}\,.}$$

# Fonction thêta d'un réseau

La fonction thêta d'un réseau $L$ de $\mathbb{Q}^n$ est par définition la fonction définie sur le demi–plan de Poincaré $\{z \in \mathbb{C} \mid (\mathrm{im}\,(z) > 0)\}$ par

$$\boxed{\Theta_L(z) := \sum_{x \in L} e^{\pi i x^2 z}\,.}$$

En particulier, si $L$ est pair, on pose $q := e^{2\pi i z}$ et on a

$$\boxed{\Theta_L(z) = \sum_{r \geq 0} |L_{2r}|\, q^r\,,}$$

où on désigne par $L_{2r}$ l'ensemble des vecteurs de $L$ de carré $2r$.

# Fonction thêta d'un réseau : un exemple

# Fonction thêta d'un réseau : un exemple

- Pour $k \in \mathbb{N}$, on définit

$$\sigma_k(r) := \sum_{\{d|(d|r)\}} d^k \, .$$

# Fonction thêta d'un réseau : un exemple

- Pour $k \in \mathbb{N}$, on définit

$$\sigma_k(r) := \sum_{\{d|(d|r)\}} d^k \, .$$

- Pour $n = 2m = 4k$, et $q := \exp(2\pi i z)$, on définit la $k$-ième *fonction d'Eisenstein* par

$$E_k(z) := 1 + (-1)^k \frac{n}{B_k} \sum_{r=1}^{\infty} \sigma_{m-1}(r) q^r \, .$$

# Fonction thêta d'un réseau : un exemple

- Pour $k \in \mathbb{N}$, on définit

$$\sigma_k(r) := \sum_{\{d|(d|r)\}} d^k \, .$$

- Pour $n = 2m = 4k$, et $q := \exp(2\pi i z)$, on définit la $k$-ième *fonction d'Eisenstein* par

$$E_k(z) := 1 + (-1)^k \frac{n}{B_k} \sum_{r=1}^{\infty} \sigma_{m-1}(r) q^r \, .$$

- La fonction thêta du réseau $\Lambda_8$ défini ci-dessus est

$$E_2(z) = 1 + 240 \sum_{r \geq 1} \sigma_3(r) q^r = 1 + 240q + 2160q^2 + 6720q^3 + \cdots \, .$$

# Formule de Poisson

On a l'analogue suivant de la formule de Mac Williams.

# Formule de Poisson

## Rappel : Théorème : Formule de MacWilliams

Supposons $n = 2m$, où $m$ est un entier. Pour tout code $\mathcal{E}$ dans $\mathcal{P}(\Omega)$,

$$\boxed{P_{\mathcal{E}^0}(X, Y) = 2^{m-\dim \mathcal{E}}\, P_{\mathcal{E}}((-X+Y)/\sqrt{2}, (X+Y)/\sqrt{2})\,.}$$

# Formule de Poisson

## Théorème : Formule de Poisson

Supposons $n = 2m$, où $m$ est un entier. Pour tout réseau $L$ de $\mathbb{Q}^n$,

$$\boxed{\Theta_{L^0}(z) = (z/i)^m \mathrm{vol}(L)\Theta_L(-1/z)\,.}$$

# Formule de Poisson

## Théorème : Formule de Poisson

Supposons $n = 2m$, où $m$ est un entier. Pour tout réseau $L$ de $\mathbb{Q}^n$,

$$\boxed{\Theta_{L^0}(z) = (z/i)^m \mathrm{vol}(L)\Theta_L(-1/z)\,.}$$

De même que pour les codes auto-orthogonaux pairs, on en déduit

# Formule de Poisson

## Théorème : Formule de Poisson

Supposons $n = 2m$, où $m$ est un entier. Pour tout réseau $L$ de $\mathbb{Q}^n$,

$$\boxed{\Theta_{L^0}(z) = (z/i)^m \mathrm{vol}(L)\Theta_L(-1/z)\,.}$$

De même que pour les codes auto-orthogonaux pairs, on en déduit

- une propriété d'invariance des fonctions thêta des réseaux unimodulaires pairs,

# Formule de Poisson

## Théorème : Formule de Poisson

Supposons $n = 2m$, où $m$ est un entier. Pour tout réseau $L$ de $\mathbb{Q}^n$,

$$\boxed{\Theta_{L^0}(z) = (z/i)^m \mathrm{vol}(L)\Theta_L(-1/z)\,.}$$

De même que pour les codes auto-orthogonaux pairs, on en déduit

- une propriété d'invariance des fonctions thêta des réseaux unimodulaires pairs,
- qui implique leur appartenance à une algèbre graduée engendrée par deux éléments

# Formule de Poisson

## Théorème : Formule de Poisson

Supposons $n = 2m$, où $m$ est un entier. Pour tout réseau $L$ de $\mathbb{Q}^n$,

$$\boxed{\Theta_{L^0}(z) = (z/i)^m \mathrm{vol}(L)\Theta_L(-1/z)\,.}$$

De même que pour les codes auto-orthogonaux pairs, on en déduit

- une propriété d'invariance des fonctions thêta des réseaux unimodulaires pairs,
- qui implique leur appartenance à une algèbre graduée engendrée par deux éléments homogènes de degrés respectifs 8 et 24.

# Formule de Poisson

## Théorème : Formule de Poisson

Supposons $n = 2m$, où $m$ est un entier. Pour tout réseau $L$ de $\mathbb{Q}^n$,

$$\boxed{\Theta_{L^0}(z) = (z/i)^m \mathrm{vol}(L)\Theta_L(-1/z)\,.}$$

De même que pour les codes auto-orthogonaux pairs, on en déduit

- une propriété d'invariance des fonctions thêta des réseaux unimodulaires pairs,
- qui implique leur appartenance à une algèbre graduée engendrée par deux éléments homogènes de degrés respectifs 8 et 24.

$\rightsquigarrow$ FORMES MODULAIRES ...

# Formes Modulaires

Une *forme modulaire de degré n* est une fonction $\theta$ holomorphe sur le demi–plan de Poincaré, vérifiant les propriétés suivantes.

# Formes Modulaires

Une *forme modulaire de degré n* est une fonction $\theta$ holomorphe sur le demi–plan de Poincaré, vérifiant les propriétés suivantes.

- *Invariance* :

$$\theta(z+1) = \theta(z) \text{ et } \theta(z) = z^n \theta(-1/z)\,.$$

# Formes Modulaires

Une *forme modulaire de degré n* est une fonction $\theta$ holomorphe sur le demi–plan de Poincaré, vérifiant les propriétés suivantes.

- *Invariance* :

$$\theta(z+1) = \theta(z) \text{ et } \theta(z) = z^n \theta(-1/z)\,.$$

- *Holomorphie à l'infini* :

$$\text{si } q := \exp(2i\pi z)\,, \text{ on a } \theta(z) = \sum_{r \geq 0} a_r q^r$$

où la série entière $\sum_{r\geq 0} a_r q^r$ converge pour $|q| < 1$.

# Formes Modulaires

Une *forme modulaire de degré n* est une fonction $\theta$ holomorphe sur le demi–plan de Poincaré, vérifiant les propriétés suivantes.

- *Invariance* :

$$\theta(z+1) = \theta(z) \text{ et } \theta(z) = z^n \theta(-1/z)\,.$$

- *Holomorphie à l'infini* :

$$\text{si } q := \exp(2i\pi z)\,, \text{ on a } \theta(z) = \sum_{r \geq 0} a_r q^r$$

où la série entière $\sum_{r\geq 0} a_r q^r$ converge pour $|q| < 1$.

On dit que la forme $\theta$ est *à coefficients entiers* si ses coefficients de Fourier $a_r$ sont entiers.

# Algèbre des formes modulaires

# Algèbre des formes modulaires

- Pour $n = 2m = 4k$, la fonction $E_k(z) := 1 + (-1)^k \frac{n}{B_k} \sum_{r=1}^{\infty} \sigma_{m-1}(r) q^r$ est une forme modulaire de degré n.

# Algèbre des formes modulaires

- Pour $n = 2m = 4k$, la fonction $E_k(z) := 1 + (-1)^k \dfrac{n}{B_k} \sum_{r=1}^{\infty} \sigma_{m-1}(r) q^r$

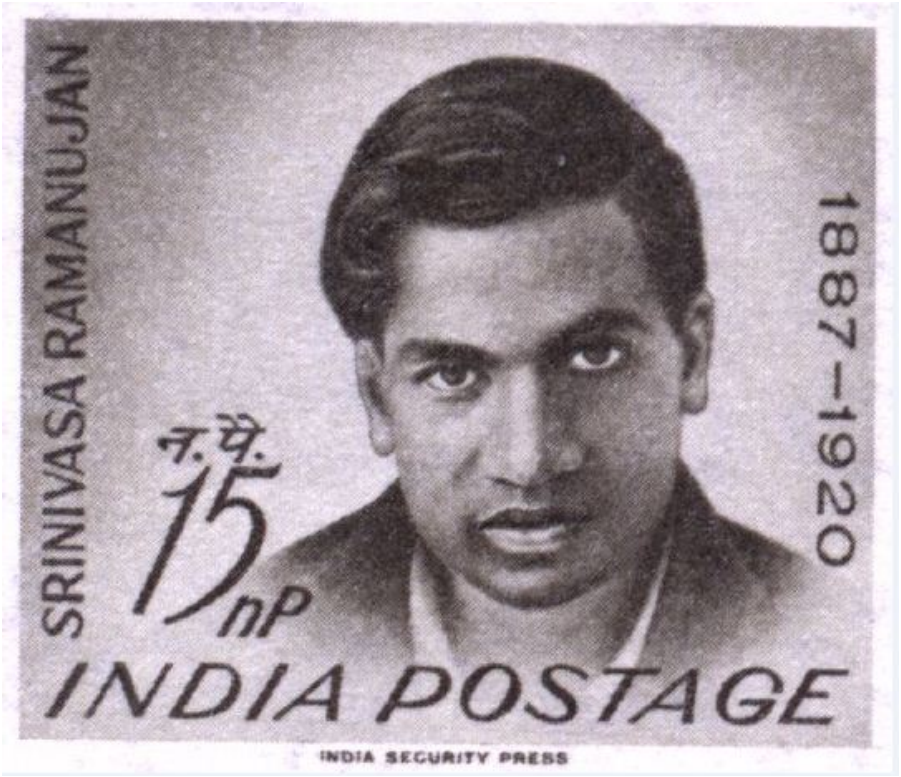
est une forme modulaire de degré n.

- La *fonction de Ramanujan*, définie par

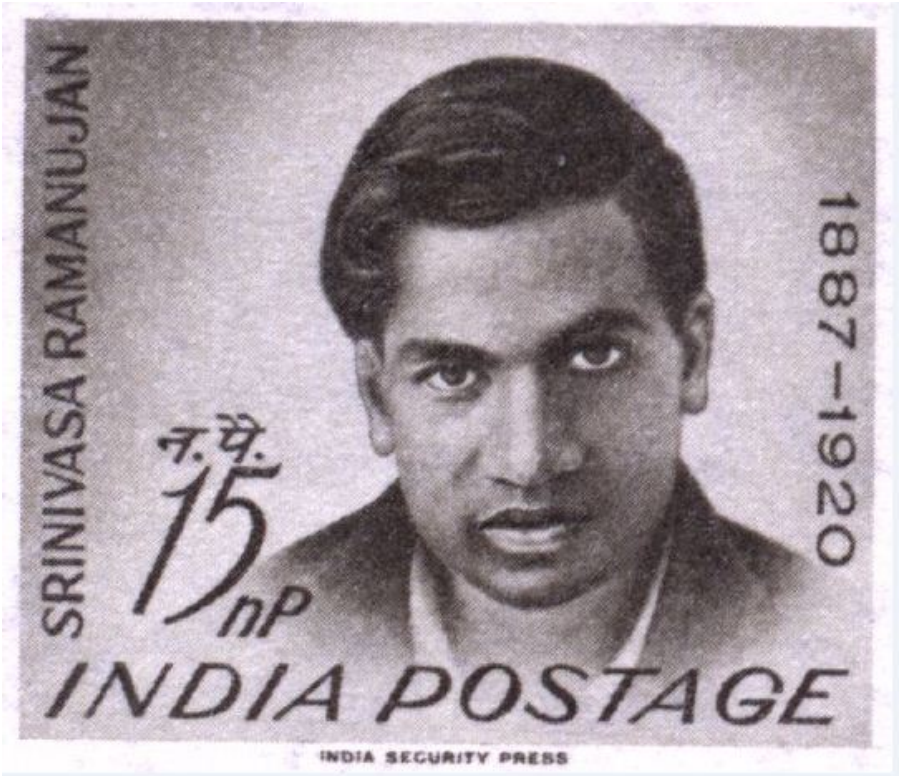
$$\Delta(z) := q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_{n \geq 1} \tau(n) q^n \, ,$$

est une forme modulaire de degré 24.

# Ramanujan !

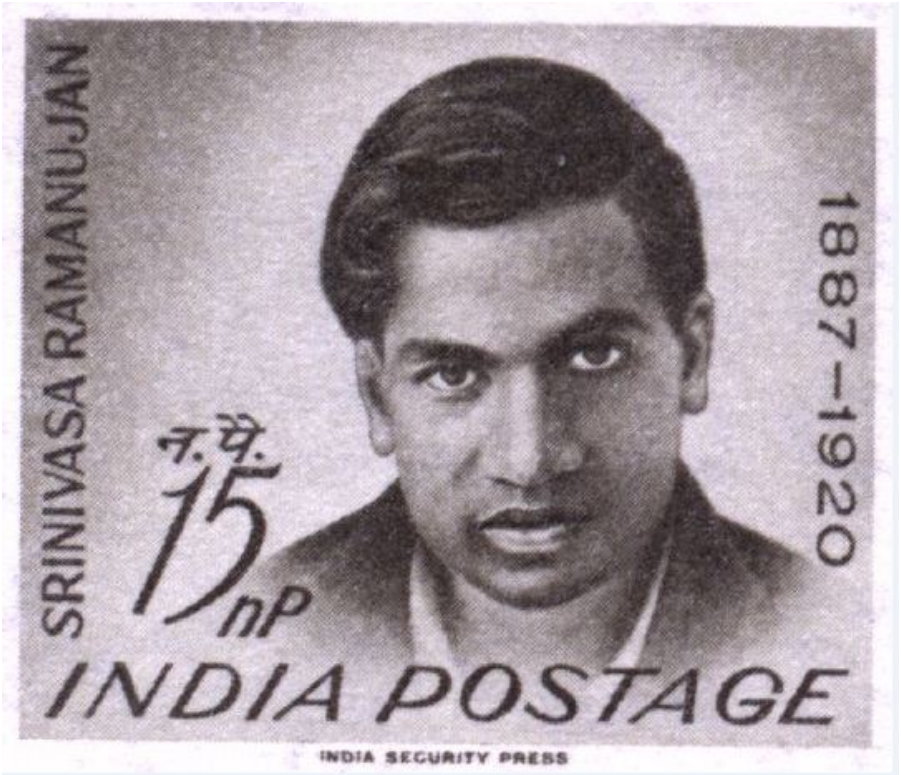

SRINIVASA RAMANUJAN
1887–1920
15 nP
INDIA POSTAGE
INDIA SECURITY PRESS

# Ramanujan !




$$\Delta(z) := q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n$$

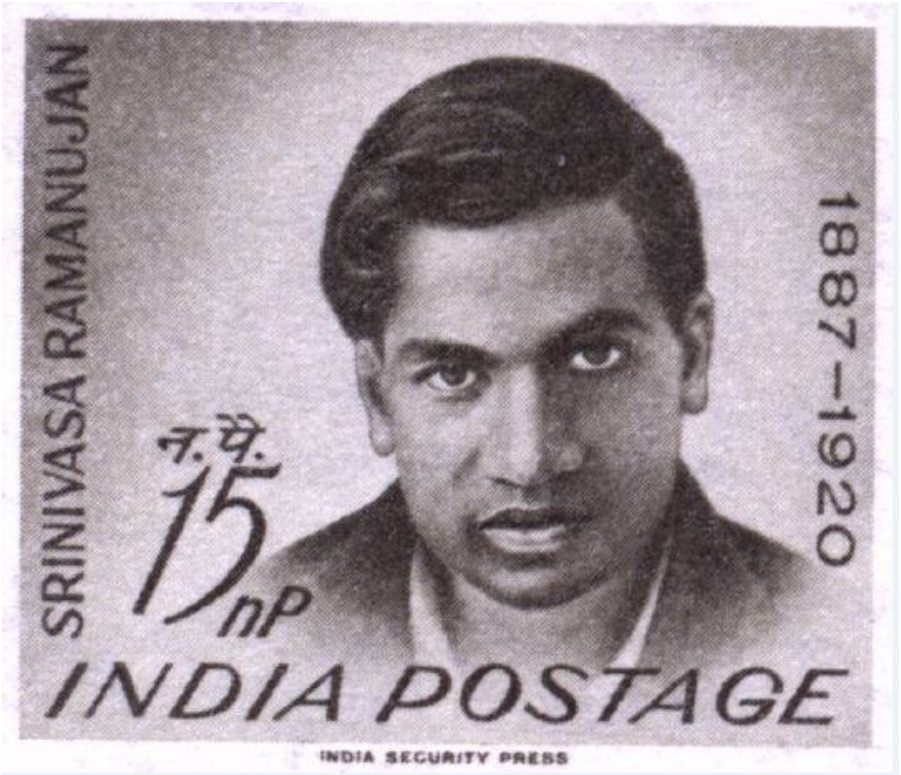
# Ramanujan !




$$\Delta(z) := q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n$$

$$|\tau(p) \leq 2\sqrt{p^{11}}\ ?$$

# Ramanujan !




$$\Delta(z) := q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}\tau(n)q^n$$

$|\tau(p) \leq 2\sqrt{p^{11}}$ ? (Deligne, 1964)

# Algèbre des formes modulaires

# Algèbre des formes modulaires

- L'ensemble $\mathcal{M} = \bigoplus \mathcal{M}_n$ des formes modulaires forme une algèbre graduée.

# Algèbre des formes modulaires

- L'ensemble $\mathcal{M} = \bigoplus \mathcal{M}_n$ des formes modulaires forme une algèbre graduée.
- On a $\mathcal{M} = \mathbb{C}[E_2, E_3]$ où $E_2$ et $E_3$ sont respectivement de degrés 8 et 24.

# Algèbre des formes modulaires

- L'ensemble $\mathcal{M} = \bigoplus \mathcal{M}_n$ des formes modulaires forme une algèbre graduée.
- On a $\mathcal{M} = \mathbb{C}[E_2, E_3]$ où $E_2$ et $E_3$ sont respectivement de degrés 8 et 24.

## Rappel – Théorème : Où vit le polynôme des poids

1. Le polynôme des poids d'un code autodual pair appartient à l'algèbre $\mathbb{Z}^W[X, Y]$ des polynômes à coefficients *entiers* et invariants par $W$,
2. On a $\mathbb{Z}^W[X, Y] = \mathbb{Z}[A(X, Y), D(X, Y)]$ où

$$A(X, Y) := X^8 + 14X^4Y^4 + Y^8 \quad \text{et} \quad D(X, Y) := X^4Y^4(X^4 - Y^4)^4 .$$

# Algèbre des formes modulaires

- L'ensemble $\mathcal{M} = \bigoplus \mathcal{M}_n$ des formes modulaires forme une algèbre graduée.
- On a $\mathcal{M} = \mathbb{C}[E_2, E_3]$ où $E_2$ et $E_3$ sont respectivement de degrés 8 et 24.

## Théorème : Où vit la fonction thêta

# Algèbre des formes modulaires

- L'ensemble $\mathcal{M} = \bigoplus \mathcal{M}_n$ des formes modulaires forme une algèbre graduée.
- On a $\mathcal{M} = \mathbb{C}[E_2, E_3]$ où $E_2$ et $E_3$ sont respectivement de degrés 8 et 24.

## Théorème : Où vit la fonction thêta

1. L'algèbre des formes modulaire entières est $\mathbb{Z}[E_2, \Delta]$.

# Algèbre des formes modulaires

- L'ensemble $\mathcal{M} = \bigoplus \mathcal{M}_n$ des formes modulaires forme une algèbre graduée.
- On a $\mathcal{M} = \mathbb{C}[E_2, E_3]$ où $E_2$ et $E_3$ sont respectivement de degrés 8 et 24.

**Théorème : Où vit la fonction thêta**

1. L'algèbre des formes modulaire entières est $\mathbb{Z}[E_2, \Delta]$.
2. La fonction $\theta_L$ d'un réseau unimodulaire pair de rang $n$ est un élément de degré $n$ de $\mathbb{Z}[E_2, \Delta]$.

# Algèbre des formes modulaires

## Rappel :Corollaire

1. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual pair en dimension 8 : le polynôme
$$A(X,Y) = X^8 + 14X^4Y^4 + Y^8 .$$
2. Il y a un seul polynôme qui peut être le polynôme des poids d'un code autodual pair en dimension 24 sans vecteur de poids 4 : le polynôme
$$B(X,Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24} .$$

## Rappel :Théorème : Existence des codes « sans petits vecteurs »

1. Il existe un et un seul (à isomorphisme près) code autodual pair en dimension 8, de polynôme des poids $A(X,Y) = X^8 + 14X^4Y^4 + Y^8$ .
2. Il existe un et un seul (à isomorphisme près) code autodual pair en dimension 24, de polynôme des poids
$$B(X,Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24} ,$$
appelé le *Code de Golay* (Nous y reviendrons plus loin)

## Corollaire

1. Il y a une seule fonction qui peut être la fonction thêta d'un réseau unimodulaire pair en dimension 8, à savoir la fonction $E_2$.
2. Il y a une seule fonction qui peut être la fonction thêta d'un réseau unimodulaire pair en dimension 24 ne contenant aucun vecteur de carré 2, à savoir

$$\Theta_{24} = 1 + (65520/691) \sum_{n \geq 1} (\sigma_{11}(n) - \tau(n)) q^n = 1 + 196560\, q^2 + 16773120\, q^3 + 398034000\, q^4 + \cdots .$$

## Théorème : Existence des réseaux « sans petits vecteurs »

1. Il existe un et un seul (à isomorphisme près) réseau unimodulaire pair en dimension 8, le réseau $\Lambda_8$.
2. Il existe un et un seul (à isomorphisme près) réseau unimodulaire pair en dimension 24, de fonction thêta $\Theta_{24}$, appelé le *réseau de Leech*. (Nous y revenons ci-dessous)

# En dimension 24

**Du côté codes :**

# En dimension 24

## Du côté codes :

- Le code de Golay est engendré par les « cellules » d'un *système de Steiner* $\mathrm{St}(5, 8, 24)$.

# En dimension 24

**Du côté codes :**

- Le code de Golay est engendré par les « cellules » d'un *système de Steiner* $\mathrm{St}(5, 8, 24)$.
- Le groupe des automorphismes d'un tel système de Steiner (et du code de Golay) est *le groupe de Mathieu* $M_{24}$,

# En dimension 24

## Du côté codes :

- Le code de Golay est engendré par les « cellules » d'un *système de Steiner* $\mathrm{St}(5, 8, 24)$.
- Le groupe des automorphismes d'un tel système de Steiner (et du code de Golay) est *le groupe de Mathieu* $M_{24}$, groupe 5 fois transitif sur 24 lettres, d'ordre $(24 \times 23 \times 22 \times 21 \times 22) \times 48$.

# En dimension 24

**Du côté codes :**

- Le code de Golay est engendré par les « cellules » d'un *système de Steiner* $\mathrm{St}(5, 8, 24)$.
- Le groupe des automorphismes d'un tel système de Steiner (et du code de Golay) est *le groupe de Mathieu* $M_{24}$, groupe 5 fois transitif sur 24 lettres, d'ordre $(24 \times 23 \times 22 \times 21 \times 22) \times 48$.

  $\rightsquigarrow$ GROUPES DE MATHIEU ET GROUPES SIMPLES ...

# En dimension 24

**Du côté codes :**

- Le code de Golay est engendré par les « cellules » d'un *système de Steiner* $\mathrm{St}(5, 8, 24)$.
- Le groupe des automorphismes d'un tel système de Steiner (et du code de Golay) est *le groupe de Mathieu* $M_{24}$, groupe 5 fois transitif sur 24 lettres, d'ordre $(24 \times 23 \times 22 \times 21 \times 22) \times 48$.

  $\rightsquigarrow$ GROUPES DE MATHIEU ET GROUPES SIMPLES ...

**Du côté réseaux :**

# En dimension 24

## Du côté codes :

- Le code de Golay est engendré par les « cellules » d'un *système de Steiner* $\mathrm{St}(5, 8, 24)$.
- Le groupe des automorphismes d'un tel système de Steiner (et du code de Golay) est *le groupe de Mathieu* $M_{24}$, groupe 5 fois transitif sur 24 lettres, d'ordre $(24 \times 23 \times 22 \times 21 \times 22) \times 48$.

  $\rightsquigarrow$ GROUPES DE MATHIEU ET GROUPES SIMPLES ...

## Du côté réseaux :

- Le réseau de Leech, fantastique réseau en dimension 24 !

# En dimension 24

## Du côté codes :

- Le code de Golay est engendré par les « cellules » d'un *système de Steiner* $\mathrm{St}(5, 8, 24)$.
- Le groupe des automorphismes d'un tel système de Steiner (et du code de Golay) est *le groupe de Mathieu* $M_{24}$, groupe 5 fois transitif sur 24 lettres, d'ordre $(24 \times 23 \times 22 \times 21 \times 22) \times 48$.

  $\rightsquigarrow$ GROUPES DE MATHIEU ET GROUPES SIMPLES ...

## Du côté réseaux :

- Le réseau de Leech, fantastique réseau en dimension 24 !
- Le groupe des automorphismes du réseau de Leech est *le groupe de Conway*, dont le quotient par le centre est un *groupe simple sporadique*.

# En dimension 24

## Du côté codes :

- Le code de Golay est engendré par les « cellules » d'un *système de Steiner* $\mathrm{St}(5, 8, 24)$.
- Le groupe des automorphismes d'un tel système de Steiner (et du code de Golay) est *le groupe de Mathieu* $M_{24}$, groupe 5 fois transitif sur 24 lettres, d'ordre $(24 \times 23 \times 22 \times 21 \times 22) \times 48$.

  $\rightsquigarrow$ GROUPES DE MATHIEU ET GROUPES SIMPLES ...

## Du côté réseaux :

- Le réseau de Leech, fantastique réseau en dimension 24 !
- Le groupe des automorphismes du réseau de Leech est *le groupe de Conway*, dont le quotient par le centre est un *groupe simple sporadique*.

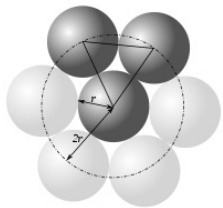
  $\rightsquigarrow$ RÉSEAU DE LEECH, GROUPE DE CONWAY, MONSTRE ...

# Réseau de Leech etc.

- Chaque boule unité centrée en un point du réseau n'en intersecte aucune autre, et est tangente à 196560 autres telles boules...

# Réseau de Leech etc.

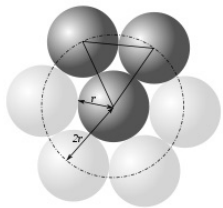
- Chaque boule unité centrée en un point du réseau n'en intersecte aucune autre, et est tangente à 196560 autres telles boules...



(le nombre maximal possible, comme 6 en dimension 2).

# Réseau de Leech etc.

- Chaque boule unité centrée en un point du réseau n'en intersecte aucune autre, et est tangente à 196560 autres telles boules...



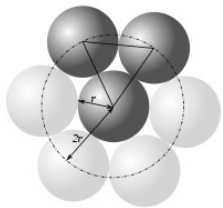
(le nombre maximal possible, comme 6 en dimension 2).

- Le groupe de Conway, groupe des automorphismes du réseau de Leech, est un groupe « presque simple », d'ordre

$$8315553613086720000$$

# Réseau de Leech etc.

- Chaque boule unité centrée en un point du réseau n'en intersecte aucune autre, et est tangente à 196560 autres telles boules...



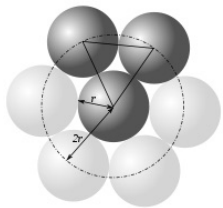
(le nombre maximal possible, comme 6 en dimension 2).

- Le groupe de Conway, groupe des automorphismes du réseau de Leech, est un groupe « presque simple », d'ordre

$$8315553613086720000 = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23\,.$$

# Réseau de Leech etc.

- Chaque boule unité centrée en un point du réseau n'en intersecte aucune autre, et est tangente à 196560 autres telles boules...



(le nombre maximal possible, comme 6 en dimension 2).

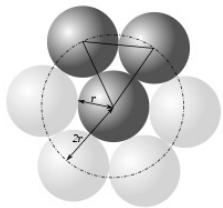
- Le groupe de Conway, groupe des automorphismes du réseau de Leech, est un groupe « presque simple », d'ordre

$$8315553613086720000 = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23\,.$$

- Le groupe de Mathieu $M_{24}$ est une sorte de squelette pour le groupe de Conway.

# Réseau de Leech etc.

- Chaque boule unité centrée en un point du réseau n'en intersecte aucune autre, et est tangente à 196560 autres telles boules...



(le nombre maximal possible, comme 6 en dimension 2).

- Le groupe de Conway, groupe des automorphismes du réseau de Leech, est un groupe « presque simple », d'ordre

$$8315553613086720000 = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23\,.$$

- Le groupe de Mathieu $M_{24}$ est une sorte de squelette pour le groupe de Conway.
  Le groupe de Conway est à son tour une espèce de squelette dans le «Monstre», le plus grand des groupes finis simples sporadiques, d'ordre

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \simeq 8 \cdot 10^{53}\,.$$

# Ponts entre les deux mondes

À un code $\mathcal{E}$ dans $\mathcal{P}(\Omega)$, on associe un réseau $L(\mathcal{E})$ dans $\mathbb{Q}^{\Omega}$ :

# Ponts entre les deux mondes

À un code $\mathcal{E}$ dans $\mathcal{P}(\Omega)$, on associe un réseau $L(\mathcal{E})$ dans $\mathbb{Q}^\Omega$ :

- Soit $R$ le réseau de base

$$(v_i)_{i\in\Omega} \text{ orthogonale et telle que } v_i^2 = 1/2.$$

# Ponts entre les deux mondes

À un code $\mathcal{E}$ dans $\mathcal{P}(\Omega)$, on associe un réseau $L(\mathcal{E})$ dans $\mathbb{Q}^\Omega$ :

- Soit $R$ le réseau de base

$$(v_i)_{i\in\Omega} \text{ orthogonale et telle que } v_i^2 = 1/2.$$

- L'application $v_i \mapsto \{i\}$ induit un isomorphisme $R/2R \xrightarrow{\sim} \mathcal{P}(\Omega)$.

# Ponts entre les deux mondes

À un code $\mathcal{E}$ dans $\mathcal{P}(\Omega)$, on associe un réseau $L(\mathcal{E})$ dans $\mathbb{Q}^\Omega$ :

- Soit $R$ le réseau de base

$$(v_i)_{i\in\Omega} \text{ orthogonale et telle que } v_i^2 = 1/2.$$

- L'application $v_i \mapsto \{i\}$ induit un isomorphisme $R/2R \xrightarrow{\sim} \mathcal{P}(\Omega)$.
- On désigne par $L(\mathcal{E})$ l'image réciproque de $\mathcal{E}$.

# Ponts entre les deux mondes

À un code $\mathcal{E}$ dans $\mathcal{P}(\Omega)$, on associe un réseau $L(\mathcal{E})$ dans $\mathbb{Q}^\Omega$ :

- Soit $R$ le réseau de base
$$(v_i)_{i\in\Omega} \text{ orthogonale et telle que } v_i^2 = 1/2.$$
- L'application $v_i \mapsto \{i\}$ induit un isomorphisme $R/2R \xrightarrow{\sim} \mathcal{P}(\Omega)$.
- On désigne par $L(\mathcal{E})$ l'image réciproque de $\mathcal{E}$.

## Le pont trivial

# Ponts entre les deux mondes

À un code $\mathcal{E}$ dans $\mathcal{P}(\Omega)$, on associe un réseau $L(\mathcal{E})$ dans $\mathbb{Q}^\Omega$ :

- Soit $R$ le réseau de base
$$(v_i)_{i\in\Omega} \text{ orthogonale et telle que } v_i^2 = 1/2.$$
- L'application $v_i \mapsto \{i\}$ induit un isomorphisme $R/2R \xrightarrow{\sim} \mathcal{P}(\Omega)$.
- On désigne par $L(\mathcal{E})$ l'image réciproque de $\mathcal{E}$.

## Le pont trivial

1. $L(\mathcal{E}^0) = L(\mathcal{E})^0$,

# Ponts entre les deux mondes

À un code $\mathcal{E}$ dans $\mathcal{P}(\Omega)$, on associe un réseau $L(\mathcal{E})$ dans $\mathbb{Q}^\Omega$ :

- Soit $R$ le réseau de base
$$(v_i)_{i\in\Omega} \text{ orthogonale et telle que } v_i^2 = 1/2.$$
- L'application $v_i \mapsto \{i\}$ induit un isomorphisme $R/2R \xrightarrow{\sim} \mathcal{P}(\Omega)$.
- On désigne par $L(\mathcal{E})$ l'image réciproque de $\mathcal{E}$.

## Le pont trivial

1. $L(\mathcal{E}^0) = L(\mathcal{E})^0$,
2. $L(\mathcal{E})$ est unimodulaire pair si et seulement si $\mathcal{E}$ est autodual pair.

# Isomorphisme entre les algèbres

# Isomorphisme entre les algèbres

On considère les fonctions de Jacobi définies par

$$\varphi_2(z) := \sum_{n\in\mathbb{Z}} \exp(2\pi i(n+(1/2))^2 z)\,,$$

$$\varphi_3(z) := \sum_{n\in\mathbb{Z}} \exp(2\pi i n^2 z)\,.$$

# Isomorphisme entre les algèbres

On considère les fonctions de Jacobi définies par

$$\varphi_2(z) := \sum_{n\in\mathbb{Z}} \exp(2\pi i(n+(1/2))^2 z)\,,$$

$$\varphi_3(z) := \sum_{n\in\mathbb{Z}} \exp(2\pi i n^2 z)\,.$$

## Proposition

# Isomorphisme entre les algèbres

On considère les fonctions de Jacobi définies par

$$\varphi_2(z) := \sum_{n\in\mathbb{Z}} \exp(2\pi i(n+(1/2))^2 z)\,,$$
$$\varphi_3(z) := \sum_{n\in\mathbb{Z}} \exp(2\pi i n^2 z)\,.$$

## Proposition

1. L'application $P(X,Y) \mapsto P(\varphi_2,\varphi_3)$ définit un isomorphisme entre l'algèbre des polynômes $W$-invariants $\mathbb{Q}^W(X,Y)$ et l'algèbre des formes modulaires à coefficients rationnels.

# Isomorphisme entre les algèbres

On considère les fonctions de Jacobi définies par

$$\varphi_2(z) := \sum_{n\in\mathbb{Z}} \exp(2\pi i(n+(1/2))^2 z)\,,$$
$$\varphi_3(z) := \sum_{n\in\mathbb{Z}} \exp(2\pi i n^2 z)\,.$$

## Proposition

1. L'application $P(X,Y) \mapsto P(\varphi_2,\varphi_3)$ définit un isomorphisme entre l'algèbre des polynômes $W$-invariants $\mathbb{Q}^W(X,Y)$ et l'algèbre des formes modulaires à coefficients rationnels.
2. Pour tout code audodual pair $\mathcal{E}$, on a $\theta_{L(\mathcal{E})} = P_{\mathcal{E}}(\varphi_2,\varphi_3)$.

# Mais...

- *Via* le pont trivial, le code de Golay ne s'envoie pas sur le réseau de Leech.

# Mais...

- *Via* le pont trivial, le code de Golay ne s'envoie pas sur le réseau de Leech.
  Leur relation est un peu plus subtile

# Mais...

- *Via* le pont trivial, le code de Golay ne s'envoie pas sur le réseau de Leech.
  Leur relation est un peu plus subtile... mais très étroite.

# Mais...

- *Via* le pont trivial, le code de Golay ne s'envoie pas sur le réseau de Leech.
  Leur relation est un peu plus subtile... mais très étroite.
- Bien d'autres analogies ne sont pas (encore ?) reliées par un pont.

# Mais...

- *Via* le pont trivial, le code de Golay ne s'envoie pas sur le réseau de Leech.
  Leur relation est un peu plus subtile... mais très étroite.
- Bien d'autres analogies ne sont pas (encore ?) reliées par un pont.
  Par exemple, les *formules des masses* (ici, $n = 2m$ et $m$ est pair) :

# Mais...

- *Via* le pont trivial, le code de Golay ne s'envoie pas sur le réseau de Leech.
  Leur relation est un peu plus subtile... mais très étroite.
- Bien d'autres analogies ne sont pas (encore ?) reliées par un pont.
  Par exemple, les *formules des masses* (ici, $n = 2m$ et $m$ est pair) :
  - $\sum_{\mathcal{E}} \frac{P_{\mathcal{E}}(X,Y)}{|\mathrm{Aut}(\mathcal{E})|} =$ (un polynôme explicite qui ne dépend que de $n$),

# Mais...

- *Via* le pont trivial, le code de Golay ne s'envoie pas sur le réseau de Leech.
  Leur relation est un peu plus subtile... mais très étroite.
- Bien d'autres analogies ne sont pas (encore ?) reliées par un pont.

  Par exemple, les *formules des masses* (ici, $n = 2m$ et $m$ est pair) :

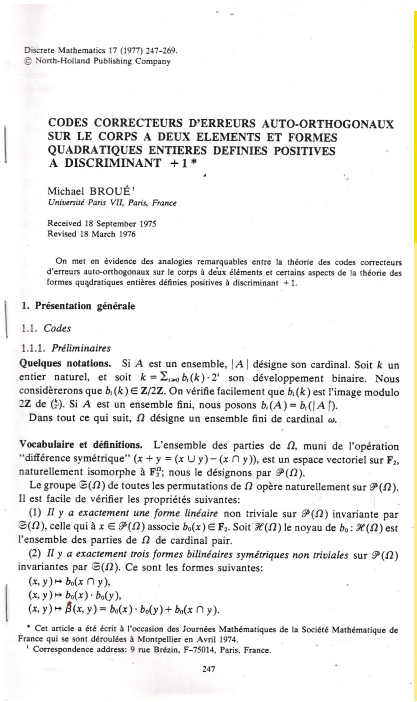
  - $\sum_{\mathcal{E}} \frac{P_{\mathcal{E}}(X,Y)}{|\mathrm{Aut}(\mathcal{E})|} = (\text{un polynôme explicite qui ne dépend que de } n)\,,$
  - $\sum_{L} \frac{\theta_L}{|\mathrm{Aut}(L)|} = \left( \frac{1}{2^{n-1}} \frac{B_{m/2}}{m!} \prod_{j=1}^{m-1} B_j \right) E_m\,,$

# Mais...

- *Via* le pont trivial, le code de Golay ne s'envoie pas sur le réseau de Leech.
  Leur relation est un peu plus subtile... mais très étroite.
- Bien d'autres analogies ne sont pas (encore ?) reliées par un pont.
  Par exemple, les *formules des masses* (ici, $n = 2m$ et $m$ est pair) :
  - $\sum_{\mathcal{E}} \frac{P_{\mathcal{E}}(X,Y)}{|\mathrm{Aut}(\mathcal{E})|} =$ (un polynôme explicite qui ne dépend que de $n$),
  - $\sum_{L} \frac{\theta_L}{|\mathrm{Aut}(L)|} = \left( \frac{1}{2^{n-1}} \frac{B_{m/2}}{m!} \prod_{j=1}^{m-1} B_j \right) E_m$, où

$$E_m(z) = \frac{1}{2\zeta(m)} \sum_{\substack{(a,b)\neq(0,0) \\ (a,b)\in\mathbb{Z}^2}} \frac{1}{(az+b)^m} .$$

# Bibliographie



Discrete Mathematics 17 (1977) 247–269.
© North-Holland Publishing Company

**CODES CORRECTEURS D'ERREURS AUTO-ORTHOGONAUX SUR LE CORPS A DEUX ELEMENTS ET FORMES QUADRATIQUES ENTIERES DEFINIES POSITIVES A DISCRIMINANT +1 ***

Michael BROUÉ [1]
*Université Paris VII, Paris, France*

Received 18 September 1975
Revised 18 March 1976

On met en évidence des analogies remarquables entre la théorie des codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux éléments et certains aspects de la théorie des formes quadratiques entières définies positives à discriminant +1.

**1. Présentation générale**

1.1. *Codes*

1.1.1. *Préliminaires*

**Quelques notations.** Si $A$ est un ensemble, $|A|$ désigne son cardinal. Soit $k$ un entier naturel, et soit $k = \sum_{i\geq 0} b_i(k)\cdot 2^i$ son développement binaire. Nous considérerons que $b_i(k) \in \mathbf{Z}/2\mathbf{Z}$. On vérifie facilement que $b_i(k)$ est l'image modulo $2\mathbf{Z}$ de $\left[\frac{k}{2^i}\right]$. Si $A$ est un ensemble fini, nous posons $b_i(A) = b_i(|A|)$.

Dans tout ce qui suit, $\Omega$ désigne un ensemble fini de cardinal $\omega$.

**Vocabulaire et définitions.** L'ensemble des parties de $\Omega$, muni de l'opération "différence symétrique" $(x + y = (x \cup y) - (x \cap y))$, est un espace vectoriel sur $\mathbf{F}_2$, naturellement isomorphe à $\mathbf{F}_2^\omega$; nous le désignons par $\mathcal{P}(\Omega)$.

Le groupe $\mathfrak{S}(\Omega)$ de toutes les permutations de $\Omega$ opère naturellement sur $\mathcal{P}(\Omega)$. Il est facile de vérifier les propriétés suivantes:

(1) *Il y a exactement une forme linéaire* non triviale sur $\mathcal{P}(\Omega)$ invariante par $\mathfrak{S}(\Omega)$, celle qui à $x \in \mathcal{P}(\Omega)$ associe $b_0(x) \in \mathbf{F}_2$. Soit $\mathcal{H}(\Omega)$ le noyau de $b_0 : \mathcal{H}(\Omega)$ est l'ensemble des parties de $\Omega$ de cardinal pair.

(2) *Il y a exactement trois formes bilinéaires symétriques non triviales* sur $\mathcal{P}(\Omega)$ invariantes par $\mathfrak{S}(\Omega)$. Ce sont les formes suivantes:

$(x, y) \mapsto b_0(x \cap y)$,
$(x, y) \mapsto b_0(x)\cdot b_0(y)$,
$(x, y) \mapsto \beta(x, y) = b_0(x)\cdot b_0(y) + b_0(x \cap y)$.

* Cet article a été écrit à l'occasion des Journées Mathématiques de la Société Mathématique de France qui se sont déroulées à Montpellier en Avril 1974.

[1] Correspondence address: 9 rue Brézin, F–75014, Paris, France.