Actions de groupes en théorie des codes

Martino Borello

Université Paris 8 - LAGA

Paris 13, 06.01.2017

Contexte

q une puissance d'un nombre premier.

Définitions de base

- Un **code linéaire** q**-aire** $\mathcal{C}$ de **longueur** n est un sous-espace de $\mathbb{F}_q^n$.
- Si $c = (c_1, \ldots, c_n) \in \mathcal{C}$ (**mot**), le **poids** (de Hamming) de c est

$$\mathrm{wt}(c) := \#\{i \in \{1, \ldots, n\} \mid c_i \neq 0\}$$

  $(\mathrm{wt}(\mathcal{C}) := \{\mathrm{wt}(c) \mid c \in \mathcal{C}\})$.
- $\mathrm{d}(\mathcal{C}) := \min_{c \in \mathcal{C}, c \neq 0} \mathrm{wt}(c)$ (**distance minimale**).
- Si $\langle \cdot, \cdot \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ est le produit scalaire standard,

$$\mathcal{C}^\perp := \{v \in \mathbb{F}_q^n \mid \langle v, c \rangle = 0, \text{ pour tout } c \in \mathcal{C}\} \quad (\textbf{dual de } \mathcal{C}).$$

- If $\mathcal{C} = \mathcal{C}^\perp$, le code $\mathcal{C}$ est appelé **autodual**.

Polynôme énumérateur

$$\mathcal{C} \subseteq \mathbb{F}_q^n \rightsquigarrow w_{\mathcal{C}}(x,y) := \sum_{c \in \mathcal{C}} x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)} = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

où $A_i := \#\{c \in \mathcal{C} \mid \mathrm{wt}(c) = i\}$.

$\mathcal{C}$ code linéaire **binaire**.

Conditions de divisibilité

- **Pair**: $\mathrm{wt}(\mathcal{C}) \subseteq 2\mathbb{Z} \Rightarrow w_{\mathcal{C}}(x,y) = w_{\mathcal{C}}(x,-y)$.
- **Doublement pair**: $\mathrm{wt}(\mathcal{C}) \subseteq 4\mathbb{Z} \Rightarrow w_{\mathcal{C}}(x,y) = w_{\mathcal{C}}(x,iy)$.

Identités de MacWilliams

- **Autodual** $\Rightarrow w_{\mathcal{C}}(x,y) = w_{\mathcal{C}}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)$.

Remarque: autodual $\Rightarrow$ pair.

L'action de $\mathrm{GL}_2(\mathbb{C})$ sur $\mathbb{C}[x,y]$

$\mathrm{GL}_2(\mathbb{C}) \curvearrowright \mathbb{C}[x,y]$:

$$\left(A := \begin{bmatrix} a & b \\ c & d \end{bmatrix}, p(x,y)\right) \mapsto p(x,y)^A := p(ax+by, cx+dy).$$

Pour $G \leqslant \mathrm{GL}_2(\mathbb{C})$, on appelle

$$\mathbb{C}[x,y]^G := \{p(x,y) \mid p(x,y)^A = p(x,y)\ \forall A \in G\}.$$

Exemple

$$G := \left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle \Rightarrow \mathbb{C}[x,y]^G = \mathbb{C}[x,y^2].$$

Le Théorème de Gleason

Théorème (Gleason '70)

Soit $\mathcal{C}$ un code linéaire binaire qui est autodual et doublement pair. Alors

$$w_{\mathcal{C}}(x,y) \in \mathbb{C}[f_1, f_2]$$

où $f_1 := w_{\hat{\mathcal{H}}_3}(x,y)$ et $f_2 := w_{\mathcal{G}_{24}}(x,y)$.

- $\mathcal{C}$ autodual $\Rightarrow w_{\mathcal{C}}(x,y) = w_{\mathcal{C}}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)$,
- $\mathcal{C}$ doublement pair $\Rightarrow w_{\mathcal{C}}(x,y) = w_{\mathcal{C}}(x, iy)$,
- $G := \left\langle \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \right\rangle \Rightarrow \mathbb{C}[x,y]^G = \mathbb{C}[f_1, f_2]$.

$\mathcal{C} \subseteq \mathbb{F}_2^n$ autodual et doublement pair.

Conséquences

- $8 \mid n$ (Gleason '71).
- $\mathrm{d}(\mathcal{C}) \leqslant 4\left\lfloor \frac{n}{24} \right\rfloor + 4$ (Mallows et Sloane '73).

Lorsque cette borne est atteinte $\mathcal{C}$ est dit **extrémal**.

- extrémal $\Rightarrow n \leqslant 3928$ (Zhang '99).
- $\underbrace{24 \mid n \text{ et extrémal}}_{\Downarrow}$

  Tous les mots d'un poids donné supportent un **5-design** (Assmus et Mattson '69)

Codes extrémaux

Codes extrémaux de longueur $24m$

$\mathcal{C} \subseteq \mathbb{F}_2^{24m}$ linéaire tel que

- $\mathcal{C} = \mathcal{C}^\perp \Rightarrow \dim \mathcal{C} = 12m$,
- $\{\mathrm{wt}(c) \mid c \in \mathcal{C}\} \subseteq \mathbf{4}\mathbb{Z}$,
- $\mathrm{d}(\mathcal{C}) = 4m + 4$.

Donc paramètres $[24m, 12m, 4m + 4]$.

- $\mathcal{G}_{24}$ (**le code de Golay**), l'unique (à équivalence près) de paramètres $[24, 12, 8]$;
- XQR_{48} (**code à résidus quadratiques étendu**), l'unique (à équivalence près) de paramètres $[48, 24, 12]$.

Un problème ouvert de longue date

Y a-t-il un code autodual de paramètres $[72, 36, 16]$? (Sloane '73)

Théorème (Pless, Conway, ..., Bouyuklieva, O'Brien, Willems, Feulner, Nebe)

Soit $\mathcal{C}$ un code autodual de paramètres $[72, 36, 16]$.
Le groupe $\mathrm{Aut}(\mathcal{C})$ est soit trivial soit isomorphe à l'un des groupes ci-dessous:

- Ordre 2: C_2;
- Ordre 3: C_3;
- Ordre 4: $C_2 \times C_2$ ou C_4;
- Ordre 5: C_5;
- Ordre 6: $\mathcal{S}_3$ ou C_6;
- Ordre 8: $C_2 \times C_2 \times C_2$ ou $\mathcal{D}_8$;
- Ordre 12: $\mathcal{A}_4$, C_{12}, $C_6 \times C_2$, $\mathcal{D}_{12}$ ou $C_3 \rtimes C_4$;
- Ordre 24: $\mathcal{S}_4$, $\mathcal{D}_{24}$, $(C_6 \times C_2) : C_2$, $\mathcal{D}_8 \times C_3$, $\mathcal{A}_4 \times C_2$, $\mathcal{D}_{12} \times C_2$ ou $C_6 \times C_2 \times C_2$.

Théorème (Pless, Conway, ..., Bouyuklieva, O'Brien, Willems, Feulner, Nebe, Borello, Dalla Volta, Yorgov's)

Soit $\mathcal{C}$ un code autodual de paramètres $[72, 36, 16]$.
Le groupe $\mathrm{Aut}(\mathcal{C})$ est soit trivial soit isomorphe à l'un des groupes ci-dessous:

- Ordre 2: C_2;
- Ordre 3: C_3;
- Ordre 4: $C_2 \times C_2$ ou C_4;
- Ordre 5: C_5;
- Ordre 6: $\mathcal{S}_3$ ou C_6;
- Ordre 8: $C_2 \times C_2 \times C_2$ ou $\mathcal{D}_8$;
- Ordre 12: $\mathcal{A}_4$, C_{12}, $C_6 \times C_2$, $\mathcal{D}_{12}$ ou $C_3 \rtimes C_4$;
- Ordre 24: $\mathcal{S}_4$, $\mathcal{D}_{24}$, $(C_6 \times C_2) : C_2$, $\mathcal{D}_8 \times C_3$, $\mathcal{A}_4 \times C_2$, $\mathcal{D}_{12} \times C_2$ ou $C_6 \times C_2 \times C_2$.

Théorème (Pless, Conway, ..., Bouyuklieva, O'Brien, Willems, Feulner, Nebe, Borello, Dalla Volta, Yorgov's)

Soit $\mathcal{C}$ un code autodual de paramètres $[72, 36, 16]$.
Le groupe $\mathrm{Aut}(\mathcal{C})$ est soit trivial soit isomorphe à l'un des groupes ci-dessous:

- Ordre 2: C_2;
- Ordre 3: C_3;
- Ordre 4: $C_2 \times C_2$;
- Ordre 5: C_5.

Généralisations

Différentes généralisations du théorème de Gleason.

G. Nebe, E.M. Rains, N.J.A. Sloane. **Self-dual codes and invariant theory**. Vol. 17. Berlin: Springer, 2006.

Idée:
propriétés de familles de codes (autoduaux) $\rightsquigarrow$ **symétries** des polynômes énumérateurs $\rightsquigarrow$ nouvelles **propriétés**.

Nos questions

- Étant donné un polynôme énumérateur, quelles sont ses symétries ?
- Sont-elles partagées par toute la famille de ce code ?
- Quels sont les groupes de symétries possibles ?
- Peut-on déterminer avec ces informations des polynômes énumérateurs inconnus ?

Symétries possibles

Pour $p(x,y) \in \mathbb{C}[x,y]_h$ (h=homogène), on appelle

$$S(p(x,y)) := \{A \in \mathrm{GL}_2(\mathbb{C}) \mid p(x,y)^A = p(x,y)\} \leqslant \mathrm{GL}_2(\mathbb{C}).$$

$\pi : S(p(x,y)) \leqslant \mathrm{GL}_2(\mathbb{C}) \mapsto \overline{S}(p(x,y)) \leqslant \mathrm{PGL}_2(\mathbb{C})$.

$$\begin{array}{ccccc} & & \mathrm{PGL}_2(\mathbb{C}) & \circlearrowright & \mathbb{P}^1(\mathbb{C}) \\ \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}, (x:y)\right) & \mapsto & (ax+by : cx+dy) & & \end{array}$$

simplement 3-transitive

induit

$$\overline{S}(p(x,y)) \circlearrowright V(p(x,y)) := \{(x:y) \in \mathbb{P}^1(\mathbb{C}) \mid p(x,y) = 0\}.$$

Théorème (B.,Mila)

$$\#S(p(x,y)) < \infty \Leftrightarrow \#V(p(x,y)) \geqslant 3.$$

Théorème (Blichfeldt 1917)

Si $H \leqslant \mathrm{PGL}_2(\mathbb{C})$ est fini, alors H est conjugué à l'un des groupes suivants:

- $\left\langle \left[\begin{smallmatrix} 1 & 0 \\ 0 & \zeta_m \end{smallmatrix}\right] \right\rangle \simeq C_m$ pour un certain $m \in \mathbb{N}$.
- $\left\langle \left[\begin{smallmatrix} 1 & 0 \\ 0 & \zeta_m \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \right\rangle \simeq D_m$ pour un certain $m \in \mathbb{N}$.
- $\left\langle \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} i & i \\ 1 & -1 \end{smallmatrix}\right] \right\rangle \simeq A_4$.
- $\left\langle \left[\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right], \left[\begin{smallmatrix} i & i \\ 1 & -1 \end{smallmatrix}\right] \right\rangle \simeq S_4$.
- $\left\langle \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} i & i \\ 1 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 2 & -\omega \\ \omega & -2 \end{smallmatrix}\right] \right\rangle \simeq A_5$ où $\omega = (1-\sqrt{5})i - (1+\sqrt{5})$.

Corollaire

Si $\#V(p(x,y)) \geqslant 3$, alors $\exists A \in \mathrm{GL}_2(\mathbb{C})$ t.q. $S(p(x,y)^A)$ est une extension centrale de l'un des groupes énumérés ci-dessus.

Exemple (Code de répétition)

$\mathcal{C}$ le code binaire $[12, 2, 6]$ dont la matrice génératrice est

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

$w_{\mathcal{C}}(x, y) = x^{12} + 2x^6y^6 + y^{12} \rightsquigarrow \overline{S}(w_{\mathcal{C}}(x, y)) \simeq D_6.$

Exemple (Code de Golay ternaire)

$\mathcal{C}$ le code ternaire $[12, 6, 6]_3$ dont la matrice génératrice est

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 0 \end{bmatrix}$$

$w_{\mathcal{C}}(x, y) = x^{12} + 264x^6y^6 + 440x^3y^9 + 24y^{12} \rightsquigarrow \overline{S}(w_{\mathcal{C}}(x, y)) \simeq A_4.$

Exemple (Code de Hamming)

$\mathcal{C}$ le code binaire $[8,4,4]$ dont la matrice génératrice est

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

$w_{\mathcal{C}}(x,y) = x^8 + 14x^4y^4 + y^8 \rightsquigarrow \overline{S}(w_{\mathcal{C}}(x,y)) \simeq S_4$.

Exemple

$f_1(x,y) := x^{20} + 228x^{15}y^5 + 494x^{10}y^{10} - 228x^5y^{15} + y^{20}$;
$f_2(x,y) := x^{30} - 522x^{25}y^5 - 10005x^{20}y^{10} - 10005x^{10}y^{20} + 522x^5y^{25} + y^{30}$.

$$p(x,y) \in \mathbb{C}[f_1(x,y), f_2(x,y)] \Rightarrow \overline{S}(p(x,y)) \simeq A_5.$$

Problème ouvert

Y a-t-il un code $\mathcal{C}$ t.q. $\overline{S}(w_{\mathcal{C}}(x,y)) \simeq A_5$?

L'algorithme

Input: $p(x,y) \in \mathbb{C}[x,y]_h$ de degré n t.q. $p(1,0) \neq 0$.

1. $G := \varnothing$.
2. $V :=$`RootsOf`$(p(x,1)) = \{x_1, \ldots, x_m\}$.
3. `If` $m < 3$, `then print`("Groupe infini") `and break; else`
   $V_3 :=$ {tous les sous-ensembles ordonnés de cardinal 3 de V}.
4. `For` $\{x'_1, x'_2, x'_3\} \in V_3$:

   4A. `Solve` $\begin{cases} x_1 a + b - x'_1 x_1 c - x'_1 d = 0 \\ x_2 a + b - x'_2 x_2 c - x'_2 d = 0 \\ x_3 a + b - x'_3 x_3 c - x'_3 d = 0 \end{cases}$ (les inconnues sont a, b, c, d).

   On appelle $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ l'une des ∞^1 solutions.

   4B. `If` $\left\{ \frac{\underline{a}x+\underline{b}}{\underline{c}x+\underline{d}} \mid x \in V \right\} = V$, `then`

   4BI. $A := \begin{bmatrix} \underline{a} & \underline{b} \\ \underline{c} & \underline{d} \end{bmatrix}$.

   4BII. $\lambda := \frac{p(\underline{a},\underline{c})}{p(\underline{1},\underline{0})}$. $B := \lambda^{-1/n} A$.

   4BIII. `If` $p(x,y)^B = p(x,y)$, `then` $G := G \cup \{\zeta_n B \mid \zeta_n \in \mathbb{C}$ s.t. $\zeta_n^n = 1\}$.

Output: $G = S(p(x,y))$.

L'algorithme

Input: $p(x,y) \in \mathbb{C}[x,y]_h$ de degré n t.q. $p(1,0) \neq 0$.

1. $G := \varnothing$.
2. $V :=$ `RootsOf`$(p(x,1)) = \{x_1, \ldots, x_m\}$. (Où ?)
3. `If` $m < 3$, `then print`("Groupe infini") `and break; else`
   $V_3 := \{$tous les sous-ensembles ordonnés de cardinal 3 de $V\}$.
4. `For` $\{x'_1, x'_2, x'_3\} \in V_3$:

   4A. `Solve` $\begin{cases} x_1 a + b - x'_1 x_1 c - x'_1 d = 0 \\ x_2 a + b - x'_2 x_2 c - x'_2 d = 0 \\ x_3 a + b - x'_3 x_3 c - x'_3 d = 0 \end{cases}$ (les inconnues sont a, b, c, d).

   On appelle $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ l'une des ∞^1 solutions. (simplement 3-transitive)

   4B. `If` $\left\{ \frac{\underline{a}x+\underline{b}}{\underline{c}x+\underline{d}} \mid x \in V \right\} = V$, `then`

   4BI. $A := \begin{bmatrix} \underline{a} & \underline{b} \\ \underline{c} & \underline{d} \end{bmatrix}$.

   4BII. $\lambda := \frac{p(\underline{a},\underline{c})}{p(1,0)}$. $B := \lambda^{-1/n} A$.

   4BIII. `If` $p(x,y)^B = p(x,y)$, `then` $G := G \cup \{\zeta_n B \mid \zeta_n \in \mathbb{C}$ s.t. $\zeta_n^n = 1\}$.

Output: $G = S(p(x,y))$.

Codes de Reed-Müller

- $\mathcal{RM}_q(r,m) := \{(f(\underline{a}))_{\underline{a}\in\mathbb{F}_q^m} \mid f \in \mathbb{F}_q[x_1,\ldots,x_m] \text{ de degré } \leqslant r\} \subseteq \mathbb{F}_q^{q^n}$.

Dimension et distance minimale connue.

Polynôme énumérator d'un code $\mathcal{RM}_q(r,m)$ $\leftrightsquigarrow$ **Comptage de points $\mathbb{F}_q$-rationnels** des hypersurfaces dans $\mathbb{A}^m(\mathbb{F}_q)$

N. Kaplan. **Rational Point Counts for del Pezzo Surfaces over Finite Fields and Coding Theory**. 2013. Thesis (Ph.D.) - Harvard University

Théorème (B.,Mila)

Si $q = 2$ et $m \geqslant 3r + 1$ ou $q \in \{3, 4, 5\}$ et $m \geqslant 2r + 1$ ou $q > 5$ et $m \geqslant r + 1$, alors $\overline{S}(w_{\mathcal{RM}_q(r,m)}(x, y))$ est soit cyclique soit dihedral.

Théorème (B.,Mila)

Si $m \geqslant 2$, alors

$$\begin{bmatrix} u & u-1 \\ u-1 & u \end{bmatrix} \in \overline{S}(w_{\mathcal{RM}_2(m-1,m)}(x, y)),$$

où $u := \frac{\zeta+1}{2}$ (ζ est une racine primitive 2^m-ième de l'unité).

Théorème (B.,Mila)

Si $\mathcal{C} \in \{\mathcal{RM}_4(2, 2), \mathcal{RM}_4(3, 2), \mathcal{RM}_5(2, 2)\}$, alors $\overline{S}(w_{\mathcal{C}}(x, y)) = \{\mathrm{Id}\}$.

Problème ouvert

Comprendre le **comportement général** et déduire propriétés et **nouveaux polynômes énumérateurs**.

Merci beaucoup pour l'attention !