Codes cycliques tordus sur les anneaux de Galois

Delphine Boucher, Patrick Solé, Felix Ulmer

IRMAR, UMR 6625, Université de Rennes 1,
I3S, UMR 6070, Université de Nice Sophia antipolis

Conférence C2, Mars 2008

Représentation polynomiale des codes cycliques

$$
\begin{array}{rcl}
(\mathbb{F}_q)^n & \leftrightsquigarrow & \mathbb{F}_q[x]/(x^n-1) \\
a=(a_0,a_1,\ldots,a_{n-1}) & \leftrightsquigarrow & a(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1} \\
C & \leftrightsquigarrow & \mathcal{C} \;=\; (g)/(x^n-1) \text{ avec } x^n-1=h\cdot g
\end{array}
$$

C est cyclique ssi $\mathcal{C}$ est un idéal de l'anneau $\mathbb{F}_q[x]/(x^n-1)$

$$(a_0,a_1,\ldots,a_{n-2},a_{n-1})\in\mathcal{C}\Rightarrow(a_{n-1},a_0,a_1,\ldots,a_{n-2})\in\mathcal{C}$$

Représentation polynomiale des codes cycliques

$$
\begin{array}{rcl}
(\mathbb{F}_q)^n & \leftrightsquigarrow & \mathbb{F}_q[x]/(x^n-1) \\
a=(a_0,a_1,\ldots,a_{n-1}) & \leftrightsquigarrow & a(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1} \\
C & \leftrightsquigarrow & \mathcal{C} \;=\; (g)/(x^n-1) \text{ avec } x^n-1=h\cdot g
\end{array}
$$

C est cyclique ssi $\mathcal{C}$ est un idéal de l'anneau $\mathbb{F}_q[x]/(x^n-1)$

$$(a_0,a_1,\ldots,a_{n-2},a_{n-1})\in\mathcal{C}\Rightarrow(a_{n-1},a_0,a_1,\ldots,a_{n-2})\in\mathcal{C}$$

Dualité des codes cycliques

Code Dual :

$$\mathcal{C}^{\perp} = \{b \in (\mathbb{F}_q)^n \mid \forall a \in \mathcal{C}, < a, b >= 0\}.$$

$x^n - 1 = h \cdot g \in \mathbb{F}_q[x]$ avec $h = h_0 + h_1 x + \ldots + x^k$ le polynôme de contrôle

$\Rightarrow (g)^{\perp}$ est aussi un code cyclique engendré par le réciproque de h qui est $h_0 x^k + h_1 x^{k-1} + \ldots + 1$

Anneaux de polynômes tordus (avec automorphisme)

Soit R un anneau et $\theta \in \mathrm{Aut}(R)$:

$$R[X,\theta] = \{a_0 + a_1X + \ldots + a_nX^n \mid a_i \in R \text{ et } n \in \mathbb{N}\}.$$

1. **addition :** comme dans $R[X]$ coeff par coeff
2. **multiplication :** pour $a \in R$ on a $X \cdot a = \theta(a) \cdot X$ et on distribue ...

Exemple : $R = \mathbb{F}_q$ un corps fini. $\Rightarrow \mathbb{F}_q[X,\theta]$ euclidien à droite et à gauche

Anneaux de polynômes tordus (avec automorphisme)

Soit R un anneau et $\theta \in \mathrm{Aut}(R)$:

$$R[X,\theta] = \{a_0 + a_1X + \ldots + a_nX^n \mid a_i \in R \text{ et } n \in \mathbb{N}\}.$$

1. **addition :** comme dans $R[X]$ coeff par coeff
2. **multiplication :** pour $a \in R$ on a $X \cdot a = \theta(a) \cdot X$ et on distribue ...

Exemple : $R = \mathbb{F}_q$ un corps fini. $\Rightarrow \mathbb{F}_q[X,\theta]$ euclidien à droite et à gauche

Idéaux des Anneaux de polynômes tordus sur $\mathbb{F}_q$

Les idéaux bilatères sont engendrés par $X^t \cdot f$ avec $f \in (\mathbb{F}_q)^\theta[X^{|\theta|}]$ avec $|\theta| =$ ordre de θ dans $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$.

$$\begin{array}{rcl} (\mathbb{F}_q)^n & \leftrightsquigarrow & \mathbb{F}_q[X,\theta]/(f) \\ a = (a_0, a_1, \ldots, a_{n-1}) & \leftrightsquigarrow & a(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} \\ C & \leftrightsquigarrow & \mathcal{C} = (g)/(f) \text{ avec } f = h \cdot g \end{array}$$

non unicité de la factorisation $\Rightarrow$ beaucoup de codes

$$f = X^n - 1 = h \cdot g \Rightarrow \; h^\perp = \theta^k(h_0)X^k + \theta^{k-1}(h_1)X^{k-1} + \ldots + 1$$

Idéaux des Anneaux de polynômes tordus sur $\mathbb{F}_q$

Les idéaux bilatères sont engendrés par $X^t \cdot f$ avec $f \in (\mathbb{F}_q)^\theta[X^{|\theta|}]$ avec $|\theta| =$ ordre de θ dans $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$.

$$\begin{aligned} (\mathbb{F}_q)^n &\leftrightsquigarrow \mathbb{F}_q[X,\theta]/(f) \\ a = (a_0, a_1, \ldots, a_{n-1}) &\leftrightsquigarrow a(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} \\ C &\leftrightsquigarrow \mathcal{C} = (g)/(f) \text{ avec } f = h \cdot g \end{aligned}$$

non unicité de la factorisation $\Rightarrow$ beaucoup de codes

$$f = X^n - 1 = h \cdot g \Rightarrow \; h^\perp = \theta^k(h_0)X^k + \theta^{k-1}(h_1)X^{k-1} + \ldots + 1$$

Idéaux des Anneaux de polynômes tordus sur $\mathbb{F}_q$

Les idéaux bilatères sont engendrés par $X^t \cdot f$ avec $f \in (\mathbb{F}_q)^\theta[X^{|\theta|}]$ avec $|\theta| =$ ordre de θ dans $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$.

$$\begin{array}{rcl} (\mathbb{F}_q)^n & \leftrightsquigarrow & \mathbb{F}_q[X,\theta]/(f) \\ a = (a_0, a_1, \ldots, a_{n-1}) & \leftrightsquigarrow & a(X) = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1} \\ C & \leftrightsquigarrow & \mathcal{C} = (g)/(f) \text{ avec } f = h \cdot g \end{array}$$

non unicité de la factorisation $\Rightarrow$ beaucoup de codes

$$f = X^n - 1 = h \cdot g \Rightarrow \; h^\perp = \theta^k(h_0)X^k + \theta^{k-1}(h_1)X^{k-1} + \ldots + 1$$

Polynômes tordus sur des anneaux de Galois

$$\varphi : \sum_{i=0}^{n} a_i y^i \in \mathbb{Z}_4[y] \mapsto \sum_{i=0}^{n} (a_i \bmod 2) y^i \in \mathbb{F}_2[y]$$

Définition : $GR(4^m) = \mathbb{Z}_4[y]/(h)$ avec $h \in \mathbb{Z}_4[y]$ tel que

1. $\varphi(h) \in \mathbb{F}_2[y]$ est unitaire irréductible de degré m
2. $\xi = \tilde{y} \in \mathbb{F}_2[y]/(\varphi(h))$ engendre le groupe multiplicatif de $\mathbb{F}_{2^m}$

Représentation des éléments :

1. $\alpha_0 + \alpha_1 \xi + \ldots + \alpha_{m-1} \xi^{m-1}$ avec $\alpha_i \in \mathbb{Z}_4$
2. $a + 2b \in GR(4^m)$ avec a et b dans $\{0, 1, \xi, \ldots, \xi^{2^m-2}\}$

$\theta : a + 2b \mapsto a^2 + 2b^2$ est automorphisme de $GR(4^m)$ d'ordre m.
NB : $\theta(\xi) = \xi^2$.

$\Rightarrow$ $GR(4^m)[X, \theta]$ **est anneau de polynômes tordus**

Polynômes tordus sur des anneaux de Galois

$$\varphi : \sum_{i=0}^{n} a_i y^i \in \mathbb{Z}_4[y] \mapsto \sum_{i=0}^{n} (a_i \bmod 2) y^i \in \mathbb{F}_2[y]$$

Définition : $GR(4^m) = \mathbb{Z}_4[y]/(h)$ avec $h \in \mathbb{Z}_4[y]$ tel que

1. $\varphi(h) \in \mathbb{F}_2[y]$ est unitaire irréductible de degré m
2. $\xi = \tilde{y} \in \mathbb{F}_2[y]/(\varphi(h))$ engendre le groupe multiplicatif de $\mathbb{F}_{2^m}$

Représentation des éléments :

1. $\alpha_0 + \alpha_1 \xi + \ldots + \alpha_{m-1} \xi^{m-1}$ avec $\alpha_i \in \mathbb{Z}_4$
2. $a + 2b \in GR(4^m)$ avec a et b dans $\{0, 1, \xi, \ldots, \xi^{2^m-2}\}$

$\theta : a + 2b \mapsto a^2 + 2b^2$ est automorphisme de $GR(4^m)$ d'ordre m.
NB : $\theta(\xi) = \xi^2$.

$\Rightarrow$ $GR(4^m)[X, \theta]$ **est anneau de polynômes tordus**

Polynômes tordus sur des anneaux de Galois

$$\varphi : \sum_{i=0}^{n} a_i y^i \in \mathbb{Z}_4[y] \mapsto \sum_{i=0}^{n} (a_i \bmod 2) y^i \in \mathbb{F}_2[y]$$

Définition : $GR(4^m) = \mathbb{Z}_4[y]/(h)$ avec $h \in \mathbb{Z}_4[y]$ tel que

1. $\varphi(h) \in \mathbb{F}_2[y]$ est unitaire irréductible de degré m
2. $\xi = \tilde{y} \in \mathbb{F}_2[y]/(\varphi(h))$ engendre le groupe multiplicatif de $\mathbb{F}_{2^m}$

Représentation des éléments :

1. $\alpha_0 + \alpha_1 \xi + \ldots + \alpha_{m-1} \xi^{m-1}$ avec $\alpha_i \in \mathbb{Z}_4$
2. $a + 2b \in GR(4^m)$ avec a et b dans $\{0, 1, \xi, \ldots, \xi^{2^m-2}\}$

$\theta : a + 2b \mapsto a^2 + 2b^2$ est automorphisme de $GR(4^m)$ d'ordre m.
NB : $\theta(\xi) = \xi^2$.

$\Rightarrow$ $GR(4^m)[X, \theta]$ **est anneau de polynômes tordus**

Polynômes tordus sur des anneaux de Galois

$$\varphi : \sum_{i=0}^{n} a_i y^i \in \mathbb{Z}_4[y] \mapsto \sum_{i=0}^{n} (a_i \bmod 2) y^i \in \mathbb{F}_2[y]$$

Définition : $GR(4^m) = \mathbb{Z}_4[y]/(h)$ avec $h \in \mathbb{Z}_4[y]$ tel que

1. $\varphi(h) \in \mathbb{F}_2[y]$ est unitaire irréductible de degré m
2. $\xi = \tilde{y} \in \mathbb{F}_2[y]/(\varphi(h))$ engendre le groupe multiplicatif de $\mathbb{F}_{2^m}$

Représentation des éléments :

1. $\alpha_0 + \alpha_1 \xi + \ldots + \alpha_{m-1} \xi^{m-1}$ avec $\alpha_i \in \mathbb{Z}_4$
2. $a + 2b \in GR(4^m)$ avec a et b dans $\{0, 1, \xi, \ldots, \xi^{2^m-2}\}$

$\theta : a + 2b \mapsto a^2 + 2b^2$ est automorphisme de $GR(4^m)$ d'ordre m.
NB : $\theta(\xi) = \xi^2$.

$\Rightarrow$ $GR(4^m)[X, \theta]$ **est anneau de polynômes tordus**

Polynômes tordus sur des anneaux de Galois

$$\varphi : \sum_{i=0}^{n} a_i y^i \in \mathbb{Z}_4[y] \mapsto \sum_{i=0}^{n} (a_i \bmod 2) y^i \in \mathbb{F}_2[y]$$

Définition : $GR(4^m) = \mathbb{Z}_4[y]/(h)$ avec $h \in \mathbb{Z}_4[y]$ tel que

1. $\varphi(h) \in \mathbb{F}_2[y]$ est unitaire irréductible de degré m
2. $\xi = \tilde{y} \in \mathbb{F}_2[y]/(\varphi(h))$ engendre le groupe multiplicatif de $\mathbb{F}_{2^m}$

Représentation des éléments :

1. $\alpha_0 + \alpha_1 \xi + \ldots + \alpha_{m-1} \xi^{m-1}$ avec $\alpha_i \in \mathbb{Z}_4$
2. $a + 2b \in GR(4^m)$ avec a et b dans $\{0, 1, \xi, \ldots, \xi^{2^m-2}\}$

$\theta : a + 2b \mapsto a^2 + 2b^2$ est automorphisme de $GR(4^m)$ d'ordre m.
NB : $\theta(\xi) = \xi^2$.

$\Rightarrow$ $GR(4^m)[X, \theta]$ **est anneau de polynômes tordus**

Polynômes tordus sur des anneaux de Galois

$$\varphi : \sum_{i=0}^{n} a_i y^i \in \mathbb{Z}_4[y] \mapsto \sum_{i=0}^{n} (a_i \bmod 2) y^i \in \mathbb{F}_2[y]$$

Définition : $GR(4^m) = \mathbb{Z}_4[y]/(h)$ avec $h \in \mathbb{Z}_4[y]$ tel que

1. $\varphi(h) \in \mathbb{F}_2[y]$ est unitaire irréductible de degré m
2. $\xi = \tilde{y} \in \mathbb{F}_2[y]/(\varphi(h))$ engendre le groupe multiplicatif de $\mathbb{F}_{2^m}$

Représentation des éléments :

1. $\alpha_0 + \alpha_1 \xi + \ldots + \alpha_{m-1} \xi^{m-1}$ avec $\alpha_i \in \mathbb{Z}_4$
2. $a + 2b \in GR(4^m)$ avec a et b dans $\{0, 1, \xi, \ldots, \xi^{2^m-2}\}$

$\theta : a + 2b \mapsto a^2 + 2b^2$ est automorphisme de $GR(4^m)$ d'ordre m.
NB : $\theta(\xi) = \xi^2$.

$\Rightarrow$ $GR(4^m)[X, \theta]$ **est anneau de polynômes tordus**

Idéaux de $GR(4^m)[X,\theta]$ et codes tordus sur $GR(4^m)$

Situation identique à $\mathbb{Z}[x]$:

1. Les idéaux ne sont plus tous principaux.
2. On peut diviser par des polynômes unitaires .

Les $f \in \mathbb{Z}_4[X^m]$ unitaires de degré n engendrent des idéaux bilatères. Si $n = deg(f)$ alors

$$\begin{aligned} (GR(4^m))^n &\leftrightsquigarrow GR(4^m)[X,\theta]/(f) \\ a = (a_0, a_1, \ldots, a_{n-1}) &\leftrightsquigarrow a(X) = a_0 + a_1 X + \ldots + a_{n-1}X^{n-1} \\ \mathcal{C} &\leftrightsquigarrow \mathcal{C}(X) = (g)/(f) \text{ avec } f = h \cdot g \end{aligned}$$

avec g polynôme unitaire.

Idéaux de $GR(4^m)[X,\theta]$ et codes tordus sur $GR(4^m)$

Situation identique à $\mathbb{Z}[x]$:

1. Les idéaux ne sont plus tous principaux.
2. On peut diviser par des polynômes unitaires .

Les $f \in \mathbb{Z}_4[X^m]$ unitaires de degré n engendrent des idéaux bilatères. Si $n = deg(f)$ alors

$$\begin{aligned} (GR(4^m))^n &\leftrightsquigarrow GR(4^m)[X,\theta]/(f) \\ a = (a_0, a_1, \ldots, a_{n-1}) &\leftrightsquigarrow a(X) = a_0 + a_1 X + \ldots + a_{n-1}X^{n-1} \\ \mathcal{C} &\leftrightsquigarrow \mathcal{C}(X) = (g)/(f) \text{ avec } f = h \cdot g \end{aligned}$$

avec g polynôme unitaire.

$X^4 + 1 = h \cdot (X^2 + \xi X + \xi + 1)$ dans $GR(4^2)[X, \theta]$.

$$G = \begin{pmatrix} \xi+1 & \xi & 1 & 0 \\ 0 & 3\xi & 3\xi+3 & 1 \end{pmatrix}$$

à chaque ligne on ajoute une ligne multiplié par ξ

$$\begin{pmatrix} \xi+1 & \xi & 1 & 0 \\ 3 & 3\xi+3 & \xi & 0 \\ 0 & 3\xi & 3\xi+3 & 1 \\ 0 & \xi+1 & 1 & \xi \end{pmatrix}$$

l'entrée $a + \xi b$ est remplacée par les deux entrées $3a$ et $a + b$.

$$\begin{pmatrix} 3 & 2 & 0 & 1 & 3 & 1 & 0 & 0 \\ 1 & 3 & 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 & 2 & 3 & 1 \\ 0 & 0 & 3 & 2 & 3 & 1 & 0 & 1 \end{pmatrix}$$

Codes constacycliques autoduaux sur $GR(4^m)$

Si $X^n \pm 1 = h\,g$ avec $h = X^k + \sum_{i=0}^{r-1} h_i X^i$, alors

$$g^{\perp} \;=\; h_k + \theta(h_{k-1})X + \ldots + \theta^k(h_0)X^k.$$

Donc pour un code autodual euclidien :

$$h = X^k + \sum_{i=1}^{k-1} \left(\theta^{k-i}(g_0^{-1})\,\theta^{k-i}(g_{k-i})X^i \right) + \theta^r(g_0^{-1})$$

On pose

$$\left(X^k + \sum_{i=0}^{k-1} g_i X^i \right) \left(\theta^k(g_0^2) + \sum_{i=1}^{k} \theta^{k-i}(g_0^2\, g_{r-i})X^i \right) = X^{2k} \pm 1$$

pour un code autodual Hermitien :

$$g^H = \sum_{i=0}^{k} \theta^{m-1+i}(h_{k-i})\, X^i$$

Codes constacycliques autoduaux sur $GR(4^m)$

Si $X^n \pm 1 = h\,g$ avec $h = X^k + \sum_{i=0}^{r-1} h_i X^i$, alors

$$g^{\perp} \;=\; h_k + \theta(h_{k-1})X + \ldots + \theta^k(h_0)X^k.$$

Donc pour un code autodual euclidien :

$$h = X^k + \sum_{i=1}^{k-1} \left(\theta^{k-i}(g_0^{-1})\,\theta^{k-i}(g_{k-i})X^i \right) + \theta^r(g_0^{-1})$$

On pose

$$\left(X^k + \sum_{i=0}^{k-1} g_i X^i \right) \left(\theta^k(g_0^2) + \sum_{i=1}^{k} \theta^{k-i}(g_0^2\, g_{r-i})X^i \right) = X^{2k} \pm 1$$

pour un code autodual Hermitien :

$$g^H = \sum_{i=0}^{k} \theta^{m-1+i}(h_{k-i})\, X^i$$

Codes constacycliques autoduaux sur $GR(4^m)$

Si $X^n \pm 1 = h\,g$ avec $h = X^k + \sum_{i=0}^{r-1} h_i X^i$, alors

$$g^{\perp} \;=\; h_k + \theta(h_{k-1})X + \ldots + \theta^k(h_0)X^k.$$

Donc pour un code autodual euclidien :

$$h = X^k + \sum_{i=1}^{k-1} \left(\theta^{k-i}(g_0^{-1})\,\theta^{k-i}(g_{k-i})X^i \right) + \theta^r(g_0^{-1})$$

On pose

$$\left(X^k + \sum_{i=0}^{k-1} g_i X^i \right) \left(\theta^k(g_0^2) + \sum_{i=1}^{k} \theta^{k-i}(g_0^2\, g_{r-i})X^i \right) = X^{2k} \pm 1$$

pour un code autodual Hermitien :

$$g^H = \sum_{i=0}^{k} \theta^{m-1+i}(h_{k-i})\, X^i$$

Three applications of $GR(4,2)$

The Galois ring $GR(4,2)$ of order 16 and characteristic 4 shares, as a coding alphabet, properties of both the ring $\mathbb{Z}_4$ and the field $\mathbb{F}_4$. Consider three applications of self dual codes of length n over $GR(4,2)$

- self-dual $\mathbb{Z}_4$-codes of length $2n$ by projection on a Trace Orthogonal Basis
- Quasi-Cyclic self-dual $\mathbb{Z}_4$-codes of length $3n$ by the cubic construction
- Modular Lattices of dimension $2n$ by Construction A

Self dual codes over $GR(4, 2)$

A code over $GR(4, 2)$ is Euclidean self-dual iff it is equal to its dual for the Euclidean scalar product

$$\sum_i x_i y_i$$

A code over $GR(4, 2)$ is Hermitian self-dual iff it is equal to its dual for the Hermitian scalar product

$$\sum_i x_i \theta(y_i)$$

A Trace Orthogonal Basis of $GR(4,2)$ over $\mathbb{Z}_4$

Write $GR(4,2) = \mathbb{Z}_4[\alpha]$, with $\alpha^2 + \alpha + 1 = 0$.
Let $\gamma = \alpha$ and $\delta = \alpha^2 + 2\alpha = \alpha + 3$. Then (γ, δ) is a TOB
Note that $Tr(\alpha\delta) = 0$ and $Tr(\alpha^2) = Tr(\delta^2) = 1$
(Observe that reduction modulo 2 yields a TOB of $\mathbb{F}_4$ over $\mathbb{F}_2$.)
Define a projection map ν say which maps $c\gamma + d\delta \in R$ onto $(c,d) \in \mathbb{Z}_4^2$.
A result special to TOB's is
If $C \subseteq R^n$ is a euclidean self-dual code then $\nu(C)$ is a self-dual $\mathbb{Z}_4$ code.

Self dual $\mathbb{Z}_4$-codes

A linear code of length n over $\mathbb{Z}_4$ is a submodule of $\mathbb{Z}_4^n$.
A code is self-dual if it is equal to its dual.
A self-dual code is Type II if all vectors in the code have Euclidean weights which are 0 (mod 8) and Type I otherwise. The minimum Euclidean (resp. Lee) weight of the code is denoted by d_E (resp.d_L).

A_4 construction of a lattice from a $\mathbb{Z}_4$-code

Define the reduction modulo 4, by $\rho : \mathbb{Z}^n \to \mathbb{Z}_4^n$, by

$$\rho(x_1, \ldots, x_n) = (x_1 \pmod 4, \ldots, x_n \pmod 4).$$

Given a code C over $\mathbb{Z}_4$ we construct a lattice by

$$\Lambda(C) = \frac{1}{2}\{x \in \mathbb{Z}^n \mid \rho(x) \in C\}. \tag{1}$$

If C is a Type I code then $\Lambda(C)$ is a Type I unimodular lattice, and that if C is a Type II code then $\Lambda(C)$ is a Type II unimodular lattice the minimum norm of the lattice is $\min\{4, \frac{d_E}{4}\}$.

Type I Lattices in dimension 24

The 156 Type I lattices in dimension 24 are classified (Borcherds) by their roots systems formed by their norm 2 vectors .
These are among $A_1^{24}, A_2^8, A_3^8, D_4^6$. So 8 distinct *swe*'s only yield 4 distinct lattices.
It is an open and challenging open problem to recover all 156 Type I lattices by Construction A_4 as it has been done for the 24 Niemeier lattices by Bonnecaze et al in 1999.

Type II Lattices in dimension 24

There is a unique Type II lattice of norm 4 in dimension 24 : the Leech lattice (Conway).
There are exactly 23 unimodular Type II lattices of norm 2 in dimension 24. They were classified by Niemeier and later by Venkov , and are uniquely characterized by the roots systems spanned by their norm 2 vectors.
We compute the systems of roots of the lattices obtained by the Type II codes by Construction A and find A_1^{24}, A_3^8, D_4^6, D_6^4, D_{12}^2 and E_8^3 (12 classes).

The Odd Leech lattice

The codes of length 24 over $\mathbb{Z}_4$ and Euclidean distance $d_E = 12$ are of Type I
give by Construction A the so-called Odd Leech lattice, the unique unimodular lattice of norm 3 in dimension 24 .
They are distinct from the four codes of Gulliver Harada (1997) as their *swe*'s are different (inspection of the monomial terms in $a^{12}c^{12}$ and $a^{15}b^8c$).

The Leech lattice

The Type II codes of length 24 and Euclidean distance $d_E = 16$ give rise to the Leech lattice by Construction A.
Since their Lee weight is only 8 (and not 12) they are not one of the thirteen Lee-optimal codes classified by Eric Rains in 1999.

Cubic Construction of $\mathbb{Z}_4$ codes

A code C over $\mathbb{Z}_4$ of length 3ℓ is ℓ-quasi-cyclic if it is invariant under the power ℓ of the shift.
By results of Ling-S., every such code can be written as

$$C = \{(x + Tr(y)|x + Tr(\alpha^2 y)|x + Tr(\alpha y))|\ \mathbf{x} \in C_1,\ y \in C_2\}$$

where C_1 is a code over $\mathbb{Z}_4$ of length ℓ
and C_2 is a code of length ℓ over $GR(4, 2)$.
Furthermore, if both C_1 and C_2 are self-dual so is C. In that case C is Type II iff C_1 is.

Eisenstein lattices

Let A_2 denote the hexagonal lattice scaled to have norm 2.
Let ρ be a complex third root of unity $\rho = \exp(2\pi\sqrt{-1}/3)$
In other words $A_2 = \sqrt{2}E$ where $E := \mathbb{Z}[\rho]$ stands for the ring of Eisenstein integers . To every $GR(4,2)-$code we attach an E-lattice
Define construction A_3 as

$$A_3(C) = \frac{1}{\sqrt{2}}(C + 4A_2^n).$$

In particular such lattices are $3-$modular : isometric (as quadratic forms) to three times their dual.
If C is an hermitian self-dual $R-$code of length n then the real image of $A_3(C)$ is a $3-$modular $\mathbb{Z}-$lattice of dimension $2n$ and of norm

$$\min(8, w_3(C)/2).$$

Eisenstein lattices : Examples

Length $2k$	Generator polynomial g	Norm	BKN
4	$X^2+2\xi+1$	2	2
6	$X^3+2X^2+2X+2\xi+1$	4	4
8	$X^4+2X^3+2X+2\xi+1$	4	4
10	$X^5+2X^3+2X^2+2\xi+1$	4	4
12	$X^6+2X^4+2X^2+2\xi+1$	4	6
14	$X^7+(3\xi+1)X^6+(\xi+2)X^5+(\xi+1)X^4+$ $(3\xi+2)X^3+(3\xi+3)X^2+\xi X+2\xi+1$	6	6
16	$X^8+2X^5+2X^3+2\xi+1$	4	6
18	$X^9+\cdots+1$	6	8
20	$X^{10}+\cdots+2\xi+1$	6	8

TAB.: Hermitian Self-dual θ-Constacyclic Codes $(g)/(X^{2k}-c)$ with $c=(-1)^{k \bmod 2}$

Eisenstein lattices : Remark

We notice that the 36 lattices of norm 6 we obtain in length $n = 14$ are all isometric to one of the two known extremal lattices of dimension 28, $Beis_{14}$ in the notation of Nebe-Sloane.
This lattice was constructed by Bachoc combining Construction A modulo 2 over the Eisenstein integers with Kneser neighboring.
By using $GR(4, 2)$ instead of $\mathbb{F}_4$, (Construction A modulo 4) we avoid neighboring.
Thus, just like $\mathbb{Z}_4$ provides the simplest construction(s) of the Leech lattice, $GR(4, 2)$ the simplest constructions of the Bachoc Eisenstein lattice in dimension 14.