Codes correcteurs d'erreurs avec les polynômes tordus

Delphine Boucher, Willi Geiselmann, Felix Ulmer

IRMAR, UMR 6625, Université de Rennes 1

Nice, novembre 2007

Codes linéaires

- Un code linéaire $\mathcal{C}$ de longueur n sur $\mathbb{F}_q$ est un sous-espace de $(\mathbb{F}_q)^n$ de dimension k
- $a = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C} \in (\mathbb{F}_q)^n$ est un mot du code
- $\mathcal{C}$ est un code cyclique si

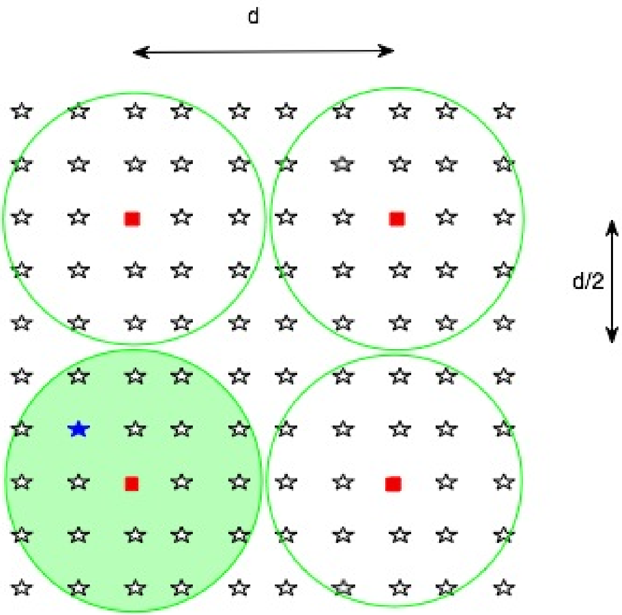
$$(a_0, a_1, a_2 \ldots, a_{n-1}) \in \mathcal{C} \Rightarrow (a_{n-1}, a_0, a_2 \ldots, a_{n-2}) \in \mathcal{C}$$

- Distance de Hamming

$$d(a, b) = card(\{i : a_i \neq b_i\}) \quad \text{avec } a, b \in (\mathbb{F}_q)^n$$

- Si $d = min_{a \in \mathcal{C}^*}\{d(a, 0)\}$, alors $\mathcal{C}$ est un code $[n, k, d]$.
- $\Rightarrow$ on peut reconnaître $d - 1$ erreurs

  $\Rightarrow$ on peut corriger $\lfloor \frac{d-1}{2} \rfloor$ erreurs


d
d/2

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

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

$$a^\pi(x) \;=\; x \cdot a(x) - a_{n-1} \cdot (x^n - 1)$$

$$a(x) \in \mathcal{C} \quad \Rightarrow \quad x \cdot a(x) \in \mathcal{C}$$

$$\boxed{\mathcal{C} \textbf{ est cyclique} \quad \Leftrightarrow \quad \mathcal{C}(x) \subset \mathbb{F}_q[x]/(x^n - 1) \textbf{ est un idéal}}$$

$\mathbb{F}_q[x]/(x^n-1)$ anneau principal

$$\Rightarrow \quad \mathcal{C}(x) = (g) \text{ avec } g \mid (x^n-1)$$

Exemple : $\mathbb{F}_4 = \mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1) = \{0, 1, \alpha, \alpha^2 = \alpha+1\}$,

$\mathcal{C} = (x^2-1) \subset \mathbb{F}_4[X]/(x^4-1)$

$$\mathcal{C}(x) = \{(b_1x+b_0)\cdot(x^2-1) \mid b_i \in \mathbb{F}_4\}$$

$$\begin{array}{rcccc} (x+\alpha)\cdot(x^2+1) & = & x^3+\alpha x^2+x+\alpha & \leftrightsquigarrow & (1,\alpha,1,\alpha) \\ 1\cdot(x^2+1) & = & x^3+1 & \leftrightsquigarrow & (0,1,0,1) \end{array}$$

1. $a \in \mathcal{C}$ se teste via division
2. Structure d'idéal : BCH (distance prescrite), décodage

Anneaux polynômes todus (avec Automorphisme)

Soit $\theta \in \mathrm{Aut}(\mathbb{F}_q)$:

$$\mathbb{F}_q[X,\theta] = \{a_0 + a_1 X + \ldots + a_n X^n \mid a_i \in \mathbb{F}_q \text{ et } n \in \mathbb{N}\}.$$

1. addition : comme dans $\mathbb{F}_q[X]$
2. multiplication : pour $a \in \mathbb{F}_q$ on a $X \cdot a = \theta(a) \cdot X$

Exemple : $\mathbb{F}_4[X,\theta]$, $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\alpha^2 = \alpha + 1$, $\alpha^3 = 1$, $\theta(\alpha) = \alpha^2$

$$\begin{aligned} X + \alpha &= \alpha^2 (\alpha X + 1) + 1 \\ &= (\alpha X + 1)\,\alpha + 0 \quad = \quad \alpha(\alpha^2 X) + \alpha \end{aligned}$$

$\mathbb{F}_q[X,\theta]$ **est un anneau euclidien à droite et à gauche**

Codes θ-cycliques

$$\boxed{|\theta| \text{ divise } n \quad \Leftrightarrow \quad (X^n - 1) \text{ est un } \textbf{idéal} \text{ de } \mathbb{F}_q[X, \theta]}$$

1. $\mathcal{C}$ iest un idéal à gauche de $\mathbb{F}_q[X, \theta]/(X^n - 1)$
2. $\mathcal{C} = (g)/(X^n - 1)$, avec g un diviseur à droite de $(X^n - 1)$.
3. $\mathcal{C}$ est un code θ-cyclique

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

$$X \left(a_0 + a_1 X + \ldots + a_{n-1} X^{n-1}\right)$$

$$= \theta(a_0)X + \theta(a_1)X^2 + \ldots + \theta(a_{n-2})X^{n-1} + \theta(a_{n-1})X^n$$

$$= \left(\theta(a_{n-1}) + \theta(a_0)X + \ldots + \theta(a_{n-2})X^{n-2}\right) + \theta(a_{n-1})(X^n - 1)$$

Codes θ-cycliques dans $\mathbb{F}_4[X, \theta]/(X^4 - 1)$

k	d	générateur	cyclique ?
3	2	$X + 1$	oui
3	2	$X + \alpha$	
3	2	$X + \alpha^2$	
2	2	$X^2 + 1$	oui
2	3	$X^2 + \alpha X + \alpha$	
2	3	$X^2 + \alpha X + \alpha^2$	
2	3	$X^2 + \alpha^2 X + \alpha$	
2	3	$X^2 + \alpha^2 X + \alpha^2$	
2	3	$X^2 + X + \alpha$	
2	3	$X^2 + X + \alpha^2$	
1	4	$X^3 + X^2 + X + 1$	oui
1	4	$X^3 + \alpha X^2 + X + \alpha$	
1	4	$X^3 + \alpha^2 X^2 + X + \alpha^2$	

Codes sur $\mathbb{F}_4$:

(n, k, d_{min})	No	g
$(42, 17, 16)$	3	$x^{25}+x^{23}+\alpha\,x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+\alpha^2\,x^{17}+\alpha^2\,x^{16}+\alpha\,x^{15}+\alpha\,x^{14}+x^{13}+x^{11}+x^{10}+x^8+\alpha^2\,x^4+\alpha^2\,x^3+x^2+\alpha\,x+1$
$(42, 23, 11)$	92	$x^{19}+x^{17}+\alpha^2\,x^{16}+\alpha\,x^{15}+\alpha^2\,x^{14}+\alpha\,x^{13}+\alpha\,x^{11}+\alpha^2\,x^{10}+\alpha\,x^9+x^7+\alpha\,x^6+\alpha^2\,x^5+\alpha\,x^4+\alpha\,x+\alpha^2$
$(40, 16, 15)$	6	$x^{24}+\alpha\,x^{23}+x^{22}+x^{21}+\alpha^2\,x^{20}+\alpha\,x^{19}+\alpha\,x^{18}+\alpha\,x^{17}+x^{15}+x^{14}+x^{13}+\alpha\,x^{11}+\alpha^2\,x^{10}+x^9+x^8+x^7+\alpha^2\,x^6+\alpha\,x^5+\alpha^2\,x^4+\alpha\,x^2+\alpha^2$
$(36, 20, 10)$	13	$x^{16}+\alpha^2\,x^{15}+x^{13}+\alpha^2\,x^{12}+x^{11}+\alpha\,x^{10}+x^9+\alpha^2\,x^8+\alpha\,x^7+\alpha\,x^6+\alpha\,x^4+\alpha^2\,x^3+\alpha^2\,x^2+1$
$(30, 16, 9)$	422	$x^{14}+x^{13}+\alpha\,x^{11}+x^{10}+x^9+x^8+\alpha\,x^7+x^6+\alpha\,x^5+\alpha^2\,x^4+\alpha^2\,x^2+\alpha\,x+\alpha^2$

Codes sur $\mathbb{F}_9$:

(n, k, d_{min})	No	g
$(44, 20, 17)$	5	$x^{24} + x^{21} + x^{20} + \alpha^7 x^{19} + \alpha^3 x^{18} + 2x^{17} + \alpha^3 x^{16} + \alpha^5 x^{14} + \alpha^5 x^{13} + 2x^{12} + \alpha^2 x^{10} + \alpha^7 x^9 + 2x^6 + \alpha^5 x^5 + \alpha^7 x^4 + \alpha^3 x^3 + \alpha^7 x^2 + \alpha^2 x + 2$

$$g = 1 \cdot X^r + g_{r-1}X^{r-1} + \ldots + g_1 X + g_0 \text{ divise } X^n - 1 \in \mathbb{F}_q[X,\theta]$$

$$G = \begin{bmatrix} g_0 & \ldots & g_{r-1} & 1 & 0 & \ldots & 0 \\ 0 & \theta(g_0) & \ldots & \theta(g_{r-1}) & 1 & \ldots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \ldots & 0 & \theta^{n-r-1}(g_0) & \ldots & \theta^{n-r-1}(g_{r-1}) & 1 \end{bmatrix}$$

La ligne i correspond à

$$X^i g(X) = \sum_{j=0}^{r} \theta^i(g_j) X^j$$

$$\left(\sum_{i=0}^{n-r-1} m_i X^i \right) \cdot g(X) \leftrightsquigarrow (m_0, m_1, \ldots, m_{n-r-1}) \cdot G$$

Codes θ-cycliques auto-duaux

Produit scalaire dans $(\mathbb{F}_q)^n$: $\quad < a, b >= \sum a_i b_i$

Le code dual au code $\mathcal{C}$ est :

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

$\mathcal{C}$ est auto-dual si $\mathcal{C} = \mathcal{C}^{\perp}$

1. $x^n - 1 = h \cdot g \in \mathbb{F}_q[x]$ avec $h = h_0 + h_1 x + \ldots + x^{n-r}$

   $\Rightarrow (g)^{\perp}$ est engendré par $h_0 x^{n-r} + h_1 x^{n-r-1} + \ldots + 1$

2. Pour un code θ-cyclique : $X^n - 1 = h \cdot g \in \mathbb{F}_q[X, \theta]$

   $\Rightarrow (g)^{\perp}$ est engendré par

   $$h^{\perp} = \theta^{n-r}(h_0) X^{n-r} + \theta^{n-r-1}(h_1) X^{n-r-1} + \ldots + 1$$

$a \in \mathcal{C} \Leftrightarrow a(X) \cdot h \equiv 0 \pmod{h \cdot g}$, car $X^n - 1 = h \cdot g = g \cdot h$

$$\begin{pmatrix} 1 & \dots & \theta^{n-r-1}(h_1) & \theta^{n-r}(h_0) & 0 & \dots & 0 \\ 0 & 1 & \dots & \dots & \theta^{n-r+1}(h_0) & \dots & 0 \\ 0 & \ddots & \ddots & & & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \dots & \ddots & 0 \\ 0 & \dots & 0 & 1 & \dots & \theta^{n-2}(h_1) & \theta^{n-1}(h_0) \end{pmatrix}$$

$$\boxed{\mathcal{C} \text{ est auto-dual} \Leftrightarrow \quad (g) = (h^{\perp})}$$

Calcul de $g(x)$ de degré $k = \frac{n}{2}$ avec une base de Gröbner

$$\left(\sum_{i=0}^{k-1} \theta^{(m-1)(k-i)}(g_0^{q-2}\, g_{k-i})\, x^i + x^k\right)\left(\sum_{i=0}^{k-1} g_i x^i + x^k\right) = x^{2k} - 1$$

Codes θ-cycliques auto-duaux sur $\mathbb{F}_4$

n	notre d	meilleur d connu	nb de g	non équivalents
4-6	3	3	2	1
8-10	4	4	2-4	1
12-14	6	6	4-2	1
16	$\boxed{4}$	$\boxed{6}$	2	1
18	6	6	12	2
20-22	8	8	8-10	1
24	$\boxed{7}$	$\boxed{8}$	16	2
26	8	8	36	3
28	9	9	32	4
30	10	10	8	1
32	$\boxed{4}$	$\boxed{10}$	2	1
34	10	10	96	6
36	$\boxed{11}$	$\boxed{10}$	36	3
38	11	11	36	2

Dual d'un code θ-cyclique est θ-cyclique

$$\begin{pmatrix} 1 & \dots & \theta^{k-1}(h_1) & \theta^k(h_0) & 0 & \dots & 0 \\ 0 & 1 & \dots & \dots & \theta^{k+1}(h_0) & \dots & 0 \\ 0 & \ddots & \ddots & & & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \dots & \ddots & 0 \\ 0 & \dots & 0 & 1 & \dots & \theta^{n-2}(h_1) & \theta^{n-1}(h_0) \end{pmatrix}$$

Il faut montrer que $\theta^{n-r}(h_0)X^{n-r} + \ldots + \theta(h_{n-r-1})X + h_{n-r}$ est aussi un diviseur à droite de $X^n - 1$.

$$X \cdot a = \theta(a) \cdot X \;\Rightarrow\; aX^{-1} = X^{-1}\theta(a) \text{ dans } \mathbb{F}_q(X,\theta)$$

$$\begin{array}{rcl} \varphi\colon \mathbb{F}_q[X,\theta] & \rightarrow & \left\{ \sum_{i=0}^{n} X^{-i} a_i \mid a_1 \in \mathbb{F}_q \right\} \subset \mathbb{F}_q(X,\theta) \\ \sum_{i=0}^{n} a_i X^i & \mapsto & \sum_{i=0}^{n} X^{-i} a_i \end{array}$$

est un anti-isomorphisme. Si $X^n - 1 = h \cdot g$, alors $\varphi(X^n - 1) =$

$$X^{-n} - 1 \;=\; \varphi(h \cdot g) \;=\; \varphi(g \cdot h) \;=\; \left(\sum_{j=0}^{n-r} X^{-j} h_j \right) \left(\sum_{i=0}^{r} X^{-i} g_j \right)$$

$$X^{n-r} \left(X^{-n} - 1\right) X^r \;=\; -(X^n - 1)$$

$$= \left(h_{n-r} + \theta(h_{n-r-1})X + \ldots + \theta^{n-r}(h_0)X^{n-r}\right) \cdot \tilde{g}$$

θ-Codes

Les idéaux bilatères sont engendrés par :

$$(b_0 + b_1 X^m + b_2 X^{2m} + \ldots + b_s X^{s \cdot m}) X^t$$

avec $m = |<\theta>|$ et $b_i \in (\mathbb{F}_q)^\theta$

Exemple : $\mathbb{F}_4[X, \theta]$ avec $\mathbb{F}_2(\alpha)$, $\alpha^2 = \alpha + 1$, $\alpha^3 = 1$, $\theta(\alpha) = \alpha^2$

$$\begin{aligned}
X^4 + X^2 + 1 &= (X^2 + X + 1)(X^2 + X + 1) \\
&= (X^2 + \alpha^2)(X^2 + \alpha) \\
&= (X^2 + \alpha)(X^2 + \alpha^2) \\
&= (X^2 + \alpha^2 X + 1)(X^2 + \alpha^2 X + 1) \\
&= (X^2 + \alpha X + 1)(X^2 + \alpha X + 1)
\end{aligned}$$

$n \setminus r$	2	3	4	5	6	7	8	9	10
4	C_{3a}^{θ}	C_4							
6	C_2	C_4	C_4^{θ}	C_6					
8	C_2	C_3^{θ}	C_{4a}^{θ}	C_5^{θ}	C_6^{θ}	C_8			
10	C_2	θ_3	C_4^{θ}	C_5^{θ}	C_6^{θ}	θ_6	θ_8	C_{10}	
12	C_2	θ_3	θ_4	C_4	C_{6a}^{θ}	C_6^{θ}	C_7^{θ}	C_8^{θ}	C_9^{θ}
14	C_2	C_3^{θ}	C_4^{θ}	C_4	C_5^{θ}	C_{6a}^{θ}	C_7^{θ}	-1	-1
16	C_2	-1	-1	C_4^{θ}	-1	-1	-1	-1	C_8^{θ}
18	C_2	-1	θ_3	θ_4	-1	-1	C_6^{θ}	-1	C_8^{θ}
20	C_2	-1	θ_3	θ_4	-1	-1	θ_6	C_7^{θ}	C_8^{θ}
22	θ_2	θ_2	θ_3	θ_4	θ_4	θ_5	-1	C_6^{θ}	C_7^{θ}
24	C_2^{θ}	C_2^{θ}	θ_3	C_4^{θ}	C_4^{θ}	-1	-1	C_6^{θ}	C_7^{θ}
26	θ_2	θ_2	θ_3	θ_4	θ_4	-1	-1	C_6^{θ}	-1
28	C_2^{θ}	C_2^{θ}	θ_3	C_4^{θ}	C_4^{θ}	-1	θ_5	C_6^{θ}	C_6^{θ}
30	C_2^{θ}	C_2^{θ}	C_3^{θ}	C_4^{θ}	C_4^{θ}	-1	C_5^{θ}	C_6^{θ}	C_6^{θ}
32	C_2^{θ}	C_2^{θ}	-1	-1	θ_4	-1	θ_5	C_6^{θ}	θ_6
34	θ_2	θ_2	-1	-1	θ_4	-1	C_5^{θ}	C_6^{θ}	C_6^{θ}

Borne d'un idéal

$P \in \mathbb{F}_q[X,\theta]$ engendre un θ-code de longueur n s'il existe $Q \in \mathbb{F}_q[X,\theta]$de degré n , avec (Q) idéal bilatère et $(Q) \subset (P)$.

N. Jacobson : La borne d'un idéal à gauche $(P) \subset \mathbb{F}_q[X,\theta]$ est un $Q \in \mathbb{F}_q[X,\theta]$ tel que $(Q) \subset (P)$ soit un idéal bilatère. La borne P^* de P est la borne unitaire de plus petit degré.

Soit $m = |<\theta>|$ et $t = [\mathbb{F}_q : (\mathbb{F}_q)^\theta]$:

$$\boxed{\textbf{degré}(P) = r \Rightarrow \textbf{degré}(P^*) \leq m \cdot t \cdot r}$$

Soit $m = | < \theta > |$ et $t = [\mathbb{F}_q : (\mathbb{F}_q)^\theta]$

Les polynômes de degré $< r$ dans $\mathbb{F}_q[X, \theta]$ forment un $\mathbb{F}_q$-espace vectoriel de dimension r, et un $(\mathbb{F}_q)^\theta$-espace vectoriel de dimension $t \cdot r$.

$$X^{m \cdot i} \; = \; Q_i \cdot P \; + \; R_i, \qquad i = 0, 1 \ldots, t \cdot r$$

$$\text{degré}(R_i) < r \; \Rightarrow \; \exists \delta_i \in (\mathbb{F}_q)^\theta) \text{ avec } \sum_{i=0}^{t \cdot r} \delta_i R_i = 0$$

$$\sum_{i=0}^{t \cdot r} \delta_i X^{m \cdot i} \; = \left(\sum_{i=0}^{t \cdot r} \delta_i Q_i \right) \cdot P.$$

Exemple :

$\mathbb{F}_4 = \mathbb{F}_2(\alpha),\ \alpha^2 = \alpha + 1,\ \alpha^3 = 1,\ \theta(\alpha) = \alpha^2.$

$X^{12} + X^{11} + \alpha X^{10} + X^9 + \alpha^2 X^8 + X^6 + X^5 + \alpha^2 X^4 + X^2 + X + \alpha^2$

est un facteur à droite de $f = X^{14} + X^{12} + X^{10} + 1 \in \mathbb{F}_4[X, \theta]$.

$\Rightarrow (g)/(f) \subset \mathbb{F}_4[X, \theta]/(f)$ est un θ-code de type $[14, 2, 11]$

$$g \ = \ 1 \cdot X^r + g_{r-1}X^{r-1} + \ldots + g_1 X + g_0 \text{ diviseur de } g^* \in \mathbb{F}_q[X,\theta]$$

$$\begin{bmatrix} g_0 & \ldots & g_{r-1} & 1 & 0 & \ldots & 0 \\ 0 & \theta(g_0) & \ldots & \theta(g_{r-1}) & 1 & \ldots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \ldots & 0 & \theta^{n-r-1}(g_0) & \ldots & \theta^{n-r-1}(g_{r-1}) & 1 \end{bmatrix}$$

La ligne i correspond à

$$X^i g(X) = \sum_{j=0}^{r} \theta^i(g_j) X^j$$

$n \setminus r$	2	3	4	5	6	7	8	9	10
4	C^θ_{3a}	C_4							
6	C_2	C_4	C^θ_4	C_6					
8	C_2	C^θ_3	C^θ_{4a}	C^θ_5	C^θ_6	C_8			
10	C_2	θ_3	C^θ_4	C^θ_5	C^θ_6	θ_6	θ_8	C_{10}	
12	C_2	θ_3	θ_4	C_4	C^θ_{6a}	C^θ_6	C^θ_7	C^θ_8	C^θ_9
14	C_2	C^θ_3	C^θ_4	C_4	C^θ_5	C^θ_{6a}	C^θ_7	-1	-1
16	C_2	-1	-1	C^θ_4	-1	-1	-1	-1	C^θ_8
18	C_2	-1	θ_3	θ_4	-1	-1	C^θ_6	-1	C^θ_8
20	C_2	-1	θ_3	θ_4	-1	-1	θ_6	C^θ_7	C^θ_8
22	θ_2	θ_2	θ_3	θ_4	θ_4	θ_5	-1	C^θ_6	C^θ_7
24	C^θ_2	C^θ_2	θ_3	C^θ_4	C^θ_4	-1	-1	C^θ_6	C^θ_7
26	θ_2	θ_2	θ_3	θ_4	θ_4	-1	-1	C^θ_6	-1
28	C^θ_2	C^θ_2	θ_3	C^θ_4	C^θ_4	-1	θ_5	C^θ_6	C^θ_6
30	C^θ_2	C^θ_2	C^θ_3	C^θ_4	C^θ_4	-1	C^θ_5	C^θ_6	C^θ_6
32	C^θ_2	C^θ_2	-1	-1	θ_4	-1	θ_5	C^θ_6	θ_6
34	θ_2	θ_2	-1	-1	θ_4	-1	C^θ_5	C^θ_6	C^θ_6