Tesi di Laurea

LA TRASFORMATA DI WINOGRAD
NELLA TEORIA DEI CODICI CORRETTORI

Sebastiano Ferraris

Università degli studi di Torino
Facoltà di Scienze Matematiche Fisiche Naturali
Corso di laurea Magistrale in Matematica

$$
\begin{tikzcd}
\mathbb{F}[x] \big/ (x^r - 1) \arrow[rrr, "\psi_4"] \arrow[d, "\psi_2"] & & & \mathbb{F}C_r \arrow[d, "\psi_3"] \\
\mathcal{V}_{r,\mathbb{F}}^{c} \arrow[rrr, "\psi_1"] & & & \mathcal{M}_{r,\mathbb{F}}^{c}
\end{tikzcd}
$$

- Per ogni $\varphi \in Gal(\mathbb{F}(\xi), \mathbb{F})$, ξ e $\varphi(\xi)$ hanno lo stesso polinomio minimo.

$$E^{(r)} = \{\xi^j\}_{j=0}^{r-1} \cong \mathbb{Z}_r \qquad G \trianglelefteq \mathbb{Z}_r^\star \qquad G \cong Gal(\mathbb{F}(\xi), \mathbb{F})$$

$$\begin{aligned} Gal(\mathbb{F}(\xi), \mathbb{F}) \times E^{(r)} &\longrightarrow E^{(r)} \\ (\varphi_k, \xi^l) &\longmapsto \varphi_k(\xi^l) = \xi^{lk} \end{aligned}$$

$$\begin{aligned} G \times \mathbb{Z}_r &\longrightarrow \mathbb{Z}_r \\ (g, l) &\longmapsto gl \end{aligned}$$

Due elementi l_1 ed l_2 di $\mathbb{Z}_r$ sono nella stessa orbita della azione

$$\begin{aligned} G \times \mathbb{Z}_r &\longrightarrow \mathbb{Z}_r \\ (g, l) &\longmapsto gl \end{aligned}$$

se e solo se ξ^{l_1} e ξ^{l_2} hanno lo stesso polinomio minimo su $\mathbb{F}$.
La **classe ciclotomica** o $(r, \mathbb{F})$**-orbita** di t è definita come l'insieme

$$O_{r,\mathbb{F}}(t) = O(t) = \{gt \mod r \mid g \in G\} \subseteq \mathbb{Z}_r$$

Diciamo **etichetta** il più piccolo elemento di ogni orbita, e indichiamo l'**insieme delle etichette** con

$$\mathscr{L}_{r,\mathbb{F}} = \mathscr{L}$$

La cardinalità dell'orbita di t

$$m_{r,\mathbb{F}}(t) = m(t) = |O(t)|$$

coincide con il grado del polinomio minimo di ξ^t

La cardinalità dell'insieme delle etichette

$$l_{r,\mathbb{F}} = l = |\mathscr{L}|$$

coincide con il numero di fattori irriducibili di $x^r - 1$

Teorema

Sia r intero positivo ed $\mathbb{F}$ campo perfetto.

1. *Ad ogni orbita $O(v)$ corrisponde un polinomio irriducibile in $\mathbb{F}[x]$ definito da*

$$M^{(v)}(x) = \prod_{t \in O(v)} (x - \xi^t)$$

2. *La decomposizione in $\mathbb{F}$ di $x^r - 1$ in fattori irriducibili è data da*

$$x^r - 1 = \prod_{v \in \mathscr{L}} M^{(v)}(x)$$

Teorema

$\mathbb{F}$ *campo perfetto,* r *intero positivo ed*

$$x^r - 1 = \prod_{v \in \mathscr{L}} M^{(v)}(x)$$

Allora γ*,* **trasformata di Winograd***, è un isomorfismo di algebre*

$$\gamma : {}^{\mathbb{F}[x]}\Big/_{x^r - 1} \longrightarrow \prod_{v \in \mathscr{L}} {}^{\mathbb{F}[x]}\Big/_{M^{(v)}(x)}$$

$$a(x) \longmapsto (a(x) \mod M^{(v)}(x))_{v \in \mathscr{L}}$$

Dimostrazione.

$$
\begin{tikzcd}
\mathbb{F}[x] \big/ (x^r - 1) \arrow[rr, "\pi"] \arrow[dr, "\gamma"] & & \mathbb{F}[x] \big/ (x^r - 1) \big/ \prod_{v \in \mathscr{L}} M^{(v)}(x) \arrow[dl, "\sim"] \\
& \prod_{v \in \mathscr{L}} \mathbb{F}[x] \big/ M^{(v)}(x) &
\end{tikzcd}
$$

$\square$

Ad esempio:

- $r = 7, \quad \mathbb{F} = \mathbb{Q}, \quad G = \mathbb{Z}_7^\star$

$$\begin{aligned} O(0) &= \{0\} \\ O(1) &= \{1,2,3,4,5,6\} \end{aligned}$$

$$\begin{aligned} x^7 - 1 &= M^{(0)}(x) M^{(1)}(x) = \Phi_1(x)\Phi_7(x) \\ &= (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) \end{aligned}$$

- $r = 7, \quad \mathbb{F} = GF(2) \quad G = \{1,2,4\} \lhd \mathbb{Z}_7^\star$

$$\begin{aligned} O(0) &= \{0\} \\ O(1) &= \{1,2,4\} \\ O(3) &= \{3,5,6\} \end{aligned}$$

$$\begin{aligned} x^7 - 1 &= M^{(0)}(x) M^{(1)}(x) M^{(3)}(x) \\ &= (x-1)(x^3 + x + 1)(x^3 + x^2 + 1) \end{aligned}$$

$x^7 - 1$ si scompone in $\mathbb{Q}$ in due fattori irriducibili

$$\mathbb{Q}[x] \Big/ (x^7 - 1) \cong \mathbb{Q}[x] \Big/ \Phi_1(x) \times \mathbb{Q}[x] \Big/ \Phi_7(x)$$

$x^7 - 1$ si scompone in $\mathbb{Z}_2$ in tre fattori irriducibili

$$\mathbb{Z}_2[x] \Big/ (x^7 - 1) \cong \mathbb{Z}_2[x] \Big/ M^{(0)}(x) \times \mathbb{Z}_2[x] \Big/ M^{(1)}(x) \times \mathbb{Z}_2[x] \Big/ M^{(3)}(x)$$

Lemma

$$\forall v \in \mathscr{L} \qquad \mathbb{F}(\xi^v) \cong {}^{\mathbb{F}[x]}\Big/_{M^{(v)}(x)}$$

Corollario

$$^{\mathbb{F}[x]}\Big/_{(x^r - 1)} \cong \prod_{v \in \mathscr{L}} {}^{\mathbb{F}[x]}\Big/_{M^{(v)}(x)} \cong \prod_{v \in \mathscr{L}} \mathbb{F}(\xi^v)$$

$$\begin{tikzcd} \mathbb{F}[x] \big/ (x^r - 1) \arrow[r, "\psi_4"] \arrow[d, "\psi_2"] & \mathbb{F}C_r \arrow[d, "\psi_3"] \\ \mathcal{V}^c_{r,\mathbb{F}} \arrow[r, "\psi_1"] & \mathcal{M}^c_{r,\mathbb{F}} \end{tikzcd}$$

$$
\begin{tikzcd}
 & \prod_{v\in\mathscr{L}} {\mathbb{F}[x]}\big/{M^{(v)}(x)} & \\
\prod_{v\in\mathscr{L}} \mathbb{F}(\xi^v) \arrow[ur, "\mu"] & {\mathbb{F}[x]}\big/{(x^r-1)} \arrow[l, "\eta"'] \arrow[u, "\gamma"'] \arrow[r, "\psi_4"] \arrow[d, "\psi_2"] & \mathbb{F}C_r \arrow[d, "\psi_3"] \\
 & \mathcal{V}^c_{r,\mathbb{F}} \arrow[r, "\psi_1"] & \mathcal{M}^c_{r,\mathbb{F}}
\end{tikzcd}
$$

Ideali

Teorema

$$\mathfrak{a} \trianglelefteq \left. \mathbb{F}[x] \middle/ (x^r - 1) \right.$$

se e solo se

$$\exists! \;\; a(x), \quad a(x) \mid x^r - 1 \quad monico, \quad \mathfrak{a} = (a(x))$$

Teorema

$$
\begin{tikzcd}
 & \{\cup_{t\in A} O(t) \mid A \subseteq \mathscr{L}\} \arrow[d] \\
\{A \mid A \subseteq \mathscr{L}\} \arrow[ur] \arrow[r] & \{\mathfrak{a} \mid \mathfrak{a} \trianglelefteq {}^{\mathbb{F}[x]}\big/_{(x^r - 1)}\}
\end{tikzcd}
$$

sono biiezioni.

Ad esempio $r = 9$, $q = 2$: $G = \mathbb{Z}_9^\star$, $\mathscr{L} = \{0, 1, 3\}$:

$$M^{(0)}(x) = x + 1$$
$$M^{(1)}(x) = x^6 + x^3 + 1$$
$$M^{(3)}(x) = x^2 + x + 1$$

$$\mathfrak{a}_{\{0\}} = (M^{(0)}(x)) = (x - 1)$$
$$\mathfrak{a}_{\{1\}} = (M^{(1)}(x)) = (x^6 + x^3 + 1)$$
$$\mathfrak{a}_{\{3\}} = (M^{(3)}(x)) = (x^2 + x + 1)$$
$$\mathfrak{a}_{\{0,1\}} = (M^{(0)}(x)M^{(1)}(x)) = (x^3 - 1)$$
$$\mathfrak{a}_{\{0,3\}} = (M^{(0)}(x)M^{(3)}(x)) = (x^7 + x^6 + x^4 + x^3 + x + 1)$$
$$\mathfrak{a}_{\{1,3\}} = (M^{(1)}(x)M^{(3)}(x)) = (x^8 + x^7 + \cdots + x + 1)$$
$$\mathfrak{a}_{\{0,1,3\}} = (M^{(0)}(x)M^{(1)}(x)M^{(3)}(x)) = (x^9 - 1) = (0)$$
$$\mathfrak{a}_{\emptyset} = (1)$$

Idempotenti

Definizione

$$a(x) \in \mathbb{F}[x] \big/ (x^r - 1) \qquad a(x)^2 = a(x)$$

Idempotenti

Definizione

$$a(x) \in {}^{\mathbb{F}[x]}\big/_{(x^r - 1)} \qquad\qquad a(x)^2 = a(x)$$

Proprietà

In $\prod_{v \in \mathscr{L}} {}^{\mathbb{F}[x]}\big/_{M^{(v)}(x)}$ sono tutti e soli i vettori l-dimensionali di polinomi costituiti da 1 e da 0.

Idempotente minimale: $\mathrm{e}_j = (0, \ldots, 0, 1, 0, \ldots, 0)$
Idempotente massimale: $\hat{\mathrm{e}}_j = (1, \ldots, 1, 0, 1, \ldots, 1)$

Teorema

1. *L'intero l, cardinalità dei fattori di $x^r - 1$ in $\mathbb{F}_q$ coincide con il numero degli idempotenti minimali e con il numero degli idempotenti massimali.*
2. *Gli idempotenti sono ortogonali:* $\mathrm{e}_i \mathrm{e}_j = 0$ *per* $i \neq j$.
3. *Gli idempotenti decompongono l'unità:* $\sum_{i \in \mathscr{L}} \mathrm{e}_i = 1$.
4. *Le combinazioni di idempotenti generano tutti gli ideali.*
5. *Ogni elemento di* $\prod_{v \in \mathscr{L}} \mathbb{F}(\xi^v)$ *si decompone come combinazione lineare a coefficienti in* $\mathbb{F}_q$ *degli idempotenti minimali.*
6. (e_j) *è un ideale minimale,* $(\hat{\mathrm{e}}_j)$ *un ideale massimale.*

Le immagini tramite γ degli elementi della base di $\mathbb{F}_2[x] \big/ _{(x^7-1)}$ sono

$$\begin{aligned}
\gamma(x^0) &= (1,1,1)\\
\gamma(x^1) &= (1,x,x)\\
\gamma(x^2) &= (1,x^2,x^2)\\
\gamma(x^3) &= (1,1+x^2,1+x+x^2)\\
\gamma(x^4) &= (1,1+x,x+x^2)\\
\gamma(x^5) &= (1,1+x+x^2,1+x^2)\\
\gamma(x^6) &= (1,x+x^2,1+x)
\end{aligned}$$

per

$$\begin{aligned}
x^7+1 &= M^{(0)}(x)M^{(1)}(x)M^{(3)}(x)\\
&= (x+1)(x^3+x+1)(x^3+x^2+1)
\end{aligned}$$

Le immagini tramite γ degli elementi della base di $\mathbb{F}_2[x] \Big/ _{(x^7-1)}$ sono

$$\gamma(1,0,0,0,0,0,0) = \gamma(x^0) = (1,1,1) = (1|1,0,0|1,0,0)$$
$$\gamma(0,1,0,0,0,0,0) = \gamma(x^1) = (1,x,x) = (1|0,1,0|0,1,0)$$
$$\gamma(0,0,1,0,0,0,0) = \gamma(x^2) = (1,x^2,x^2) = (1|0,0,1|0,0,1)$$
$$\gamma(0,0,0,1,0,0,0) = \gamma(x^3) = (1,1+x^2,1+x+x^2) = (1|1,0,1|1,1,1)$$
$$\gamma(0,0,0,0,1,0,0) = \gamma(x^4) = (1,1+x,x+x^2) = (1|1,1,0|0,1,1)$$
$$\gamma(0,0,0,0,0,1,0) = \gamma(x^5) = (1,1+x+x^2,1+x^2) = (1|1,1,1|1,0,1)$$
$$\gamma(0,0,0,0,0,0,1) = \gamma(x^6) = (1,x+x^2,1+x) = (1|0,1,1|1,1,0)$$

per

$$\begin{aligned} x^7+1 &= M^{(0)}(x)M^{(1)}(x)M^{(3)}(x) \\ &= (x+1)(x^3+x+1)(x^3+x^2+1) \end{aligned}$$

Definizione

La matrice della trasformazione γ fra le algebre

$$\mathbb{F}[x] \Big/ (x^r - 1) \quad e \quad \prod_{v \in \mathscr{L}} \mathbb{F}[x] \Big/ M^{(v)}(x)$$

nelle rispettive rappresentazioni vettoriali

$$\mathcal{V}_{r,q}^{c} \quad e \quad \mathcal{V}_{r,q}^{\mathscr{L}}$$

è detta **trasformata di Winograd**
È indicata con Γ, e la sua inversa è indicata con Δ.

$$\Gamma = \begin{pmatrix} \Gamma^{(0)} \\ \\ \Gamma^{(1)} \\ \\ \Gamma^{(3)} \end{pmatrix} = \left(\begin{array}{ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right)$$

$$\Delta = \left(\ \Delta^{(0)} \ \middle| \ \Delta^{(1)} \ \middle| \ \Delta^{(3)} \ \right) = \left(\begin{array}{c|ccc|ccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

Lemma

$c(x) \in (M^{(v)}(x))$ *se e solo se* $\Gamma^{(v)}\mathbf{c}^t = 0$.

Dimostrazione.

Dato che

1. $\eta^{(v)}(x^j) = \xi^{vj} = \sum_{i=0}^{m(v)-1} \Gamma_{i,j}^{(v)} \xi^{iv}$ per $j \in \mathbb{Z}_r$.
2. Per $H^{(v)}$ matrice dell'epimorfismo $\eta^{(v)}$ si ha $\eta^{(v)} m(x) = H^{(v)}\mathbf{m}^t$.
3. $H = \Gamma$ per H e Γ matrici di trasformazione di η e γ.

allora vale la catena di biimplicazioni:
$m(x) \in (M^{(v)}(x)) \iff M^{(v)}(x)$ divide $m(x) \iff m(\xi^v) = 0$
$\iff \eta^{(v)}(m(x)) = H^{(v)}\mathbf{m}^t = 0 \iff \Gamma^{(v)}\mathbf{m}^t = 0$. $\square$

Proprietà

1. *La prima colonna di ogni blocco $\Delta^{(v)}$ di Δ è l'idempotente miminale e_v che genera l'ideale minimale*

$$(\hat{M}^{(v)}(x)) = \left(\frac{1 - x^r}{M^{(v)}(x)}\right)$$

2. *L'insieme $\{\Delta^{(v)}_{\sim,0}\}_{v \in \mathscr{L}}$ delle prime colonne di tutti i blocchi di Δ costituisce l'insieme di tutti gli idempotenti minimali che generano tutti gli ideali minimali.*
3. $v \in \mathscr{L}$, $j \in \{0, 1 \ldots, m(v) - 1\}$:

$$\left(\Delta^{(v)}_{\sim,j}\right)^t \in \mathcal{V}^c_{m(v),q} \qquad \left(\Delta^{(v)}_{\sim,j}\right)^t = (0, 1, 0, \ldots, 0)^j \star \left(\Delta^{(v)}_{\sim,0}\right)^t$$

Applicazioni della trasformata di Winograd
nella
teoria dei codici correttori

Coici Ciclici

Definizione

Un codice lineare C di lunghezza r (cioè sottospazio vettoriale di $\mathbb{F}^r$) si dice **ciclico** *se è chiuso rispetto alla permutazione ciclica dei suoi elementi verso destra:*

$$\mathbf{c} = (c_0, c_1, \ldots, c_{r-1}) \in C \Longrightarrow (c_{r-1}, c_0, \ldots, c_{r-2}) \in C$$

Teorema

Un codice lineare C di lunghezza r sull'alfabeto $\mathbb{F}_q$ è ciclico se e solo se è un ideale di $\mathbb{F}[x] \big/ (x^r - 1)$.

La matrice di trasformazione fra lo spazio $\mathbb{F}^r$ ed il codice ciclico $(a(x))$ è chiamata **matrice generatrice** ed è indicata con G. La matrice di trasformazione fra lo spazio $\mathbb{F}^r$ ed il codice duale $(a(x))^\perp = (\hat{a}(x)^\perp)$ è chiamata **matrice di controllo** ed è indicata con H.

Teorema

Sia $\mathfrak{a}$ codice ciclico

$$c(x) \in \mathfrak{a} \iff H\mathbf{c}^t = \mathbf{0}^t$$
$$c(x) \in \mathfrak{a}^\perp \iff G\mathbf{c}^t = \mathbf{0}^t$$

Consideriamo i risultati:

$$\begin{aligned} c(x) \in \mathfrak{a} &\iff H\mathbf{c}^t = \mathbf{0}^t \\ c(x) \in \mathfrak{a}^\perp &\iff G\mathbf{c}^t = \mathbf{0}^t \\ c(x) \in (M^{(v)}(x)) &\iff \Gamma^{(v)}\mathbf{c}^t = \mathbf{0}^t \end{aligned}$$

Teorema

Sia $v \in \mathscr{L}$, allora il codice ciclico massimale $\mathfrak{a} = (M^{(v)}(x))$ ha come matrice di controllo $\Gamma^{(v)}$, v-esimo blocco della trasformata di Winograd.

Teorema

Sia $v \in \mathscr{L}$, allora il codice ciclico minimale $(M^{(-v)}(x))^\perp$ ha come matrice generatrice $\Gamma^{(v)}$ v-esimo blocco della trasformata di Winograd.

Generalizzazione: sia $a(x) = M^{(v_1)}(x) \cdots M^{(v_k)}(x)$.

Corollario

$A = (v_1, \ldots, v_k) \subseteq \mathscr{L}$, *allora*

$$\Gamma^{(A)} = \begin{pmatrix} \Gamma^{(v_1)} \\ \\ \vdots \\ \\ \Gamma^{(v_k)} \end{pmatrix}$$

è matrice di controllo del codice $\mathfrak{a} = (M^{(v_1)}(x) \cdots M^{(v_k)}(x))$ *ed è matrice generatrice del codice* $(M^{(-v_1)}(x) \cdots M^{(-v_k)}(x))^{\perp}$.

$A = (v_1, \ldots, v_k) \subseteq \mathscr{L}$, $\mathfrak{a} = (M^{(v_1)}(x) \cdots M^{(v_k)}(x))$. L'immagine della parola $c(x)$ di $\mathfrak{a}$ tramite γ è costituita da sottovettori circolanti nulli nei posti $v_1, \ldots, v_k$. Definiamo questi sottovettori **privi di informazione**.

$$\mathbf{c} \in \mathcal{V}_{r,q}^{\mathscr{L}} \mapsto \mathbf{c} \Big| \coprod_{v \in \mathscr{L} \setminus A} \mathcal{V}_{m(v),q}^{c}$$

Esempio

$c(x) = 1 + x + x^2 + x^5 = (1,1,1,0,0,1,0) \in (M^{(0)}(x)M^{(1)}(x))$.
Tramite γ *diventa:*

$$\gamma(c(x)) = (0,0,x^2) = (0|0,0,0|0,0,1)$$

Sarà sufficiente inviare il terzo blocco $(0,0,1)$ *invece della parola* $(1,1,1,0,0,1,0)$. *In fase di decodifica si aggiungeranno i sottovettori privi di informazione e si applicherà* Δ *per ottenere* $(1,1,1,0,0,1,0)$.

Fonti principali:

- U. Cerruti, F. Vaccarino *From Cyclotomic Extensions to Generalized Ramanuyan's Sum through the Winograd Transform*, pre-print.
- Luigia Berardi, *Algebra e teoria dei codici correttori*, Franco angeli Editore 1994.
- Richard E. Blahut, *Theory and Practice of Error Control Codes*, Addison Wesley publishing Company, 1984.
- Ian F. Blake, Ronald C. Mullin, *The Mathematical Theory of Coding*, Academic Press 1975.