La Trasformata di Winograd nella Teoria dei Codici Correttori

Sebastiano Ferraris

Supervisore: Umberto Cerruti.
Unvesrsità: Università degli studi di Torino, Facoltà di Scienze Matematiche Fisiche Naturali, Corso di Laurea in Matematica.
Date: 17/07/2013

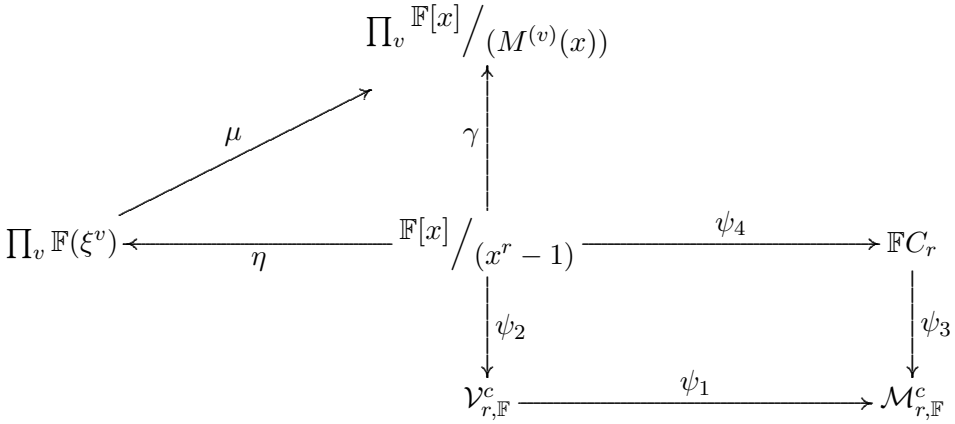
Breve Presentazione

Sebastiano Ferraris ha conseguito la laurea magistrale in Matematica all'università degli studi di Torino, sotto la supervisione del professor Umberto Cerruti.
Durante il periodo degli studi, l'autore ha lavorato come sviluppatore di algoritmi presso l'azienda tc-web di Torino e di modelli di simulazione di sistemi industriali presso la simtec di Almese. Nel periodo successivo alla laurea ha deciso di cogliere l'opportunità di una borsa di studio quadriennale presso la University College London nel Regno Unito, dove sta attualmente terminando l'ultimo anno di dottorato in Medical Imaging and Bioengineering.
Il punto di partenza che ha portato allo sviluppo della tesi presentata in queste pagine sono stati il contenuto di alcune lezioni di *Laboratorio di Applicazioni dell'Algebra* tenuto nel 2011 dal professor Umberto Cerruti ed un suo pre-print [1] sulle relazioni fra la trasformata di Winograd sui campi finiti e la teoria dei codici correttori.

Descrizione della tesi

Lo scopo principale della tesi è stato l'esplorazione delle possibilità di applicazione della trasformata di Winograd alla teoria dei codici correttori. La trasformata di Winograd consiste in una generalizzazione della trasformata di Fourier Discreta, definita come la matrice di trasformazione fra l'onnipresente algebra polinomiale $\mathbb{F}[x]\Big/(x^r-1)$ ed il prodotto di campi definito dalla fattorizzazione di x^r-1 a cui è isomorfo [3].
Questa trasformazione permette di fattorizzare l'algebra in campi, in modo analogo in cui i numeri interi si fattorizzano in numeri primi. I campi possono essere visti come particelle elementari che compongono un materiale più complesso: come esistono gli spettrometri di massa per passare dal materiale complesso alle particelle elementari, esiste una trasformazione lineare per passare dall'algebra al prodotto di campi, chiamata trasformata di Winograd.
La tesi può essere divisa in tre parti. Nella prima parte vengono introdotte le strutture algebriche a fondamento della teoria dei codici correttori, con particolare enfasi sui loro ideali e idempotenti e sulle loro trasformazioni, fra le quali compare la trasformata di Winograd.
La seconda parte introduce la teoria dei codici correttori; qui le definizioni ed i risultati della prima parte vengono giustificati definendo i codici lineari, i codici ciclici ed i codici BCH [2,4] come loro applicazione.
Nella terza parte si combinano le prime due, per dimostrare che i blocchi della trasformata di Winograd possono essere usati come matrici di controllo o matrici generatrici dei codici ciclici e che gli stessi blocchi possono essere utilizzati come sistema per diminuire la quantità di informazione dei messaggi, individuando in ogni parola alcuni sottovettori privi di informazioni.

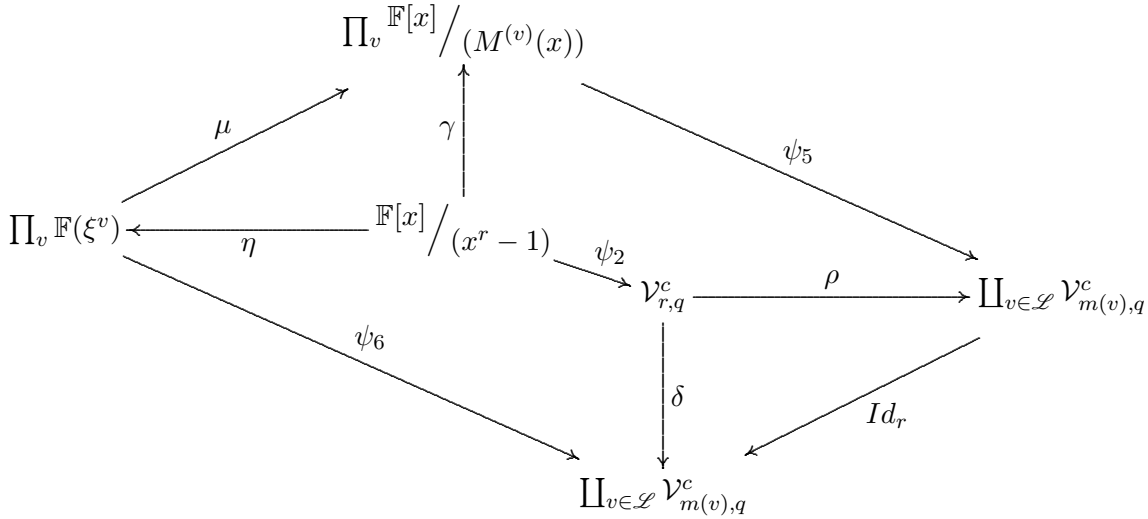
Per riassumere la prima parte può essere utile considerare un diagramma:



dove $\mathcal{V}^c_{r,\mathbb{F}}$ e $\mathcal{M}^c_{r,\mathbb{F}}$ sono l'algebra dei vettori circolanti e delle matrici circolanti di dimensione r sul campo $\mathbb{F}$. $\prod_v \mathbb{F}(\xi^v)$ e $\prod_v {\mathbb{F}[x]}/{(M^{(v)}(x))}$ sono prodotti dei campi di spezzamento e tutte le frecce sono isomorfismi.
Gli idempotenti e gli ideali di ${\mathbb{F}[x]}/{(x^r-1)}$, che giocano un ruolo fondamentale nella teoria dei codici correttori e che non sono in generale semplici da trovare, diventano facilmente accessibili con trasformata di Winograd, indicata con γ.
Il diagramma mette anche in luce la forte relazione fra le matrici ed i vettori circolanti e la trasformata di Winograd, cosa che porta alla definizione di una nuova struttura chiamata *vettori circolanti concatenati*.
Questa permette di definire i vettori dei residui dei polinomi su ogni fattore della decomposizione di x^r-1 in un vettore di vettori di dimensioni diverse, che però mantiene le setesse proprietà che aveva nella struttura originale prima della fattorizzazione. Cioè:

$$\psi_5 : \prod_{v\in\mathscr{L}} {\mathbb{F}_q[x]}/{M^{(v)}(x)} \longrightarrow \coprod_{v\in\mathscr{L}} \mathcal{V}^c_{m(v),q}$$
$$(a(x) \mod M^{(v)}(x))_{v\in\mathscr{L}} \longmapsto ((a_v)_0, (a_v)_1, \dots (a_v)_{m(v)-1})_{v\in\mathscr{L}} \ ,$$

dove $\prod$ è il prodotto tradizionale, $\coprod$ è il prodotto concatenato ed $\mathscr{L}$ è l'insieme dei gradi dei polinomi divisori di x^r-1. Successivamente, viene esplorato un nuovo diagramma, dove γ può essere identificata con ρ, tramite la rappresentazione dei vettori circolanti concatenati:



Avendo in mente una tesi orientata alle applicazioni, e soprattutto nel tentativo di capire le idee esplorate e le loro relazioni, nella tesi vengono proposti diversi esempi.

Se si considera $r = 7$ sul campo $\mathbb{Z}_2$, segue che:

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

dove la seconda uguaglianza di ogni riga porta alla rappresentazione del polinomio nel corrispondente vettore circolante concatenato. La matrice Γ che definisce la trasformata di Winograd in questo caso risulta essere la matrice circolante a blocchi:

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

Ogni scelta dei polinomi primi nella decomposizione di $x^r - 1$ definisce un insieme di blocchi della matrice Γ, i quali possono essere composti fra loro per creare le matrici generatrici dei codici ciclici, o le matrici di controllo per i loro duali. L'inversa di Γ, indicata con Δ in letteratura, può essere usata per la decodifica di un messaggio: Δ può essere usata per trovare i sotto-vettori privi di informazione nei vettori circolanti concatenati, e quindi per recuperare il messaggio originale in un modo più rapido rispetto alla classica decodifica con la sindrome.
Nella bibliografia della tesi ci sono 31 titoli. La fonte principale è il pre-print scritto dal relatore della tesi, assieme a tre capisaldi sulla teoria dei codici correttori e sulla trasformata di Winograd.

1. U. Cerruti, F. Vaccarino *From Cyclotomic Extensions to Generalized Ramanuyan's Sum through the Winograd Transform*, pre-print.

2. Luigia Berardi, *Algebra e teoria dei codici correttori*, Franco angeli Editore 1994.

3. Richard E. Blahut, *Theory and Practice of Error Control Codes*, Addison Wesley publishing Company, 1984.

4. Ian F. Blake, Ronald C. Mullin, *The Mathematical Theory of Coding*, Academic Press 1975.