Winograd Transform in Error Correcting Code theory

Sebastiano Ferraris

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

The main goal of the thesis was exploring possible applications of the Winograd transform in Error Correcting Code theory. The Winograd transform consists of a generalisation of the Discrete Fourier Transform, defined as the transformation matrix from the ubiquitous polynomial algebra ${}^{\mathbb{F}[x]}\big/_{(x^r - 1)}$ and the product of fields defined by its isomorphic factorisation $x^r - 1$ [3].
This transformation factorizes the algebra into a product of fields in analogy to how whole numbers split into product of prime numbers. Algebraic fields can be then seen as elementary particles composing a more complex compound, and the Winograd transform as the mass spectrometer providing its composition.
The thesis can be broadly subdivided into three parts. In the first one we introduce the algebraic structures at the core of Error Correcting Code theory, with particular emphasis on the ideals and idempotents and on their transformations. The Winograd transform is here introduced and its behaviour over ideals and idempotents analysed. The second part introduces the theory of error correcting codes; here the definitions and results introduced from an algebraic perspective are set to work in the definition of linear codes, cyclic codes and BCH codes [2,4].
In the third part, the first two parts are combined to prove that the blocks of the Winograd transform can be used as *control matrices* or *generating matrices* in the cyclic codes and that the same blocks can be used to diminish the amount of information to be embedded in a message, via the identification of *null-information subvectors*.

The first part can be quickly summarized with a diagram:

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

where $\mathcal{V}^c_{r,\mathbb{F}}$ e $\mathcal{M}^c_{r,\mathbb{F}}$ are the circulant vectors and circulant matrices algebras and the of dimension r over the field $\mathbb{F}$. $\prod_v \mathbb{F}(\xi^v)$ e $\prod_v {}^{\mathbb{F}[x]}\big/_{(M^{(v)}(x))}$ are product of the splitting fields, and all the arrows are isomorphisms.

Idempotents and ideals of $\mathbb{F}[x]\big/(x^r-1)$, that plays a fundamental role in the theory and that are in general not simple to be found, becomes easily accessible in the splitting field, thanks to the Winograd transform γ.

The diagram also shows the strong relationship between circulant matrices and the Winograd transform, which led to the definition of a new structure, here called *interlinked circulant vectors.*
This definition allows to define the vectors of the residual polynomials over every factor of the decomposition x^r-1 in a vector of vectors of various dimensions, that are still keeping the same properties they had in the original structure. Which means:

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

Where $\prod$ is the usual product of fields, $\coprod$ is the interlinked product defined in the thesis, $\mathscr{L}$ is the set of the degreed of the divisors of x^r-1.

Afterwards we explore the new diagram, where γ can be identified with ρ through the interlinked circulant vectors:

$$\begin{tikzcd}
 & \prod_v \mathbb{F}[x]\big/(M^{(v)}(x)) \arrow[drr, "\psi_5"] & & \\
\prod_v \mathbb{F}(\xi^v) \arrow[ur, "\mu"] \arrow[drr, "\psi_6"'] & \mathbb{F}[x]\big/(x^r-1) \arrow[u, "\gamma"] \arrow[l, "\eta"] \arrow[r, "\psi_2"] & \mathcal{V}^c_{r,q} \arrow[r, "\rho"] \arrow[d, "\delta"] & \coprod_{v\in\mathscr{L}} \mathcal{V}^c_{m(v),q} \arrow[dl, "Id_r"] \\
 & & \coprod_{v\in\mathscr{L}} \mathcal{V}^c_{m(v),q} &
\end{tikzcd}$$

Having in mind a thesis oriented towards application, and in the attempt of exploiting the understanding of the relationships between algebraic structures, in the thesis the reader can find numerous examples:
Considering $r=7$ over the field $\mathbb{Z}_2$, it follows:

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

Where the second equality of each line shows the polynomial in the corresponding interlinked circular vector. The matrix Γ, defining the Winograd transform, in this case results to be the block circulant matrix:

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

Every subset of prime polynomials in the decomposition of $x^r - 1$ defines a set of blocks in the matrix Γ, which can be recomposed to create cyclic code's generating matrices, or duals' control matrices. The inverse of Γ, indicated with Δ in the literature, can be used to decode an encoded message: Δ can be a turn into a device to quickly find the *null-information subvectors* in the interlinked circular vectors, and so to recover the original message in a quicker way if compared to the classical syndrome-based method.
There are 31 titles in the thesis bibliography, though the main source is the pre-print written by the supervisor [1], that we combined with the three strongholds in error correcting code theory [2,3,4].

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.