Winograd Transform in Error Correcting Code theory

Translation and re-adaptation of the Master Thesis
La Trasformata di Winograd nella Teoria dei Codici Correttori
Sebastiano Ferraris
Supervisor: Umberto Cerruti
Presented: 17/07/2013

Version 0.0.0 (in progress)
April 24, 2020

Introduction

> "Exact computations to start to know all the existing things and all the obscure and mysterious secrets."
>
> - Ahmes, 1600 a.C.

The starting point of this thesis are some *Laboratorio di applicazioni dell'algebra* laboratory held at the University of Turin in 2011 and a pre-print by prof. Umberto Cerruti [8] that I had used to learn several topics regarding Error Correcting Code theory that arose my interest and curiosity.
The main ones reported in this thesis are:

Chapter 1 Decomposition of the algebra $\mathcal{R}_{r,\mathbb{F}} = {}^{\mathbb{F}[x]}\big/_{(x^r - 1)}$ in a product of fields. Through the study of the factorisation of $x^r - 1$ through a group isomorphic to the Galois group $Gal(\mathbb{F}(\xi), \mathbb{F}))$ acting on the group generated by x over $\mathcal{R}_{r,\mathbb{F}}$ we build a new algebra over the irriducible factors of $x^r - 1$. For $M^{(v)}(x)$ irriducible factor of $x^r - 1$, then every quotient

$$ {}^{\mathbb{F}[x]}\big/_{M^{(v)}(x)} $$

is a field, and we can build a new algebra as the product of these fields. This is still isomorphic to $\mathcal{R}_{r,\mathbb{F}}$ and the isomorphism between them is called **Winograd transform**.
Still in Chapter 1 we prove a formula based on the Burnside theorem to determine the cardiality of the set of irriducible factors $M^{(v)}(x)$.

Chapter 2 Study of $\mathcal{R}_{r,q}$ ideals and idempotents: from this chapter onwards we account only for the finite fields, as this is where the applications considered in the subsequent chapters are. After defining some of the operators over $\mathcal{R}_{r,q}$, we present a study over the ideals and idempotents, playing a fundamental role in the Error Correcting Code theory. Given the field's ideals and idempotents simplicity when represented in the new algebra defined in the previous chapter, the analysis is not carried forward over $\mathcal{R}_{r,q}$.

Chpater 3 Winograd transform as linear transform between $\mathcal{R}_{r,q}$ and its splitting product: we dive into the definition of Winograd transform, obtaining its transformation matrix and its inverse. We also present some of its more relevant properties. To define the transformation matrix in the most direct way, we start from the definition of **interlinked circulant vectors**. This is still isomorphic to the ones already provided, and it keeps the structure of product of fields, though with a simple structure to allow to talk about transformation matrix. In this chapter too there can be found several numerical examples.

Chapter 4 and 5 Error correcting code theory introduction: in this interlude we present the error correcting code theory from its basics, to define linear codes, cyclic codes and BCH codes. In this chapter we will be using most of the results provided in chapters 1 and 2 and we prepare the terrain for presenting the applications of Winograd transform in error correcting code theory, aim of the thesis.

capitolo 6 Applications of the study of $\mathcal{R}_{r,q}$ and the Winograd transform in the error correcting code theory: the first applicatoin we see that a choice of Winograd transform blocks defines a matrix, that can work as control matrix as well as generating matrix. The second application is a system to encode a message diminishing the quantity of information, detecting in each word subvectors whose information contained can be neglected.

Originally, Winograd transform was discovered as a tool to decrease the computational complexity of convolution product, and as alternative to the Discrete Fourier Transform (DFT).
It had been introduced in the Shmuel Winograd's paper *On Computing the Discrete Fourier Transform* [31].
In this research I omitted the connection between the Winograd transform and DFT, we omitted any reference to the spectral code theory, and the application of the Winograd transofrm to error correcting codes discovered by Miller Truong and reed is nowhere to be found (*Efficient Program for decoding the* $(255, 223)$ *Reed-Solomon Code over* $GF(2^8)$ [22]).
I had instead considered the Winograd transform as a linear transform between two spaces, and the consequent direct applications. Main sources for this research, other than the already cited Cerruti's pre-print are *Theory and Practice of Error Control Codes*, di Richard E. Blahut [4] and *Algebra e teoria dei codici correttori* di Luigia Berardi [2].

Contents

In progress...
In progress...

Bibliography

[1] Michael Artin, *Algebra*, Prentice Hall of India, New Delhi 2007

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

[3] E.R. Berkelamp, *Factoring Polynomials over Finite Fileds*, The Bell System Technical Journal, October 1967, pag. 1853-1859.

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

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

[6] Giulia Maria Piacentini Cattaneo, *Algebra, un approccio algoritmico*, Zanichelli 2007, prima ed. 1996.

[7] D.G. Cantor, H. Zasenhaus, *A new Algorithm for Factoring Polynomials over Finite Fileds*, Mathematics of Computation, volume 36, numero 154, aprile 1981, pag. 587-592.

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

[9] K.M. CHerung, F. Pollara *Phobos Lander Coding System: Software and Analysis*, TDA progess report, April-June 1988, pag 274-286.

[10] Lindsday N. Childs, *A Concrete Introduction to Higher Algebra*, Springer-Verlag Gmbh, Third Edition 2009.

[11] Philip J. Davis, *Circulant Matrices*, John Wiley and Sons, 1979.

[12] Angela Di Febbraro, Alessandro Giua, *Sistemi ad eventi discreti*, McGraw Hill, ed 2011, prima ed 2002.

[13] I.N. Herstein, *Algebra*, editori riuniti, University Press 2010, prima ed. 1982.

[14] Nathan Jacobson, *Basic Algebra I*, W.H. Freeman and Company, prima ed. 1985.

[15] Thomas Koshy, *Elementary Number Theory with applications*, Accademic Press, Elzevier, 2007.

[16] A. Languasco, A. Zaccagnini, *Introduzione alla crittografia*, Ulrico Hoepli editore 2004.

[17] R. Lidl, H. Niederreiter *Introduction to Finite Fields and Applications*, Cambridge university press 1994, prima edizione 1986.

[18] J.H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, GTM 86 Third Edition 1999.

[19] J.S. Milne, *Fields and Galois Theory*, electronic version, Creative Commons license, 27 May 1998.

`http://www.jmilne.org/math/`

[20] Timothy Murphy, *Course 373, Finite Fields*, electronic version, Creative Commons license.

`pet.ece.iisc.ernet.in/sathish/FiniteFields.pdf`

[21] Andrea Montabone, *Matrici Circolanti ed Applicazioni*, Tesi di Laurea Magistrale, Università degli studi di Torino, Ottobre 2011. Relatore: Prof. U. Cerruti.

[22] R. L. Miller, T. K. Truong e I. S. Reed, *Efficient Program for decoding the* $(255, 223)$ *Reed-Solomon Code over* $GF(2^8)$, IEEE num. 127 1980 pag 136-142.

[23] Daniel Perrin, *Algebraic Geometry, an introduction*, Springer 2008.

[24] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland Publishing company 1977.

[25] Claude E. Shannon, *A Mathematica Theory of Comunication*, Bell System Technical Journal 27 379-423, July/October 1948.

[26] Victor Shoup, *A Computational Introduction to Number Theory and Algebra*, electronic version, Creative Commons license, 2008, version 2.

`http://shoup.net/ntb/`

[27] R. Sivaramakrishnan, *Classical Theory of Arithmetic Functions*, Taylor and Francis, 1989.

[28] M. Stoka, *Corso di Geometria*, CEDAM, 1995.

[29] Alun Wyn-jones, *Circulants*, no editor: electronic version, Creative Commons license, January 2008.

`http://www.circulants.org/circ/`

[30] S. Winograd, *Arithmetic Complexity of Computations*, SIAM 1980.

[31] S. Winograd, *On Computing the Discrete Fourier Transform*, Mathematics of Computation, Vol. 32, Num. 141, Gennaio 1978, pag. 175-199.