Decoding cyclic codes: the Cooper philosophy

Teo Mora (theomora@disi.unige.it)
Department of Mathematics, University of Genoa, Italy.

Emmanuela Orsini (orsini@posso.dm.unipi.it)
Department of Mathematics, University of Milan, Italy.

In 1990, Cooper [6, 7] suggested to use Gröbner basis computation in order to deduce error locator polynomials of cyclic codes.

Following his idea, Chen et al. [3, 4, 5] suggested a general algorithm to pursue Cooper's approach. The aim of the talk is to follow, on an illuminating example, the arguments which, through a series of papers [8, 2, 9], led to the following result:

Theorem 1. *For each $[n, k, d]$ binary cyclic code C with n odd, denoting $\mathbb{F}$ the splitting field of $x^n - 1$ over $\mathbb{Z}_2$, a proper Gröbner basis computation allows to produce a polynomial $\mathcal{L} \in \mathbb{Z}_2[X, z]$, where $X = (x_1, \dots, x_{n-k})$ which satisfies the following properties:*

1. $\mathcal{L}(X, z) = z^t + a_{t-1}(X)z^{t-1} + \cdots + a_0(X)$*, with* $a_j \in \mathbb{Z}_2[X]$*,* $0 \leq j \leq t - 1$*;*
2. *given a syndrome vector* $\mathbf{s} = (s_1, \dots, s_{n-k}) \in (\mathbb{F})^{n-k}$ *corresponding to an error with weight* $\mu \leq t$*, if we evaluate the* X *variables in* $\mathbf{s}$*, then the* t *roots of* $\mathcal{L}(\mathbf{s}, z)$ *are the* μ *error locations plus zero counted with multiplicity* $t - \mu$*.*

We illustrate the efficiency of this approach on the recent results discussed in [10] and we also discuss an alternative approach to the solution of the Cooper problem proposed in [4, 1].

References

[1] D. Augot, M. Bardet, J.-C. Faugere, Efficient decoding of (binary) cyclic codes above the correction capacity of the code using Gröbner bases, *Proc. IEEE Int. Symp. Information Theory 2003*, (2003) .

[2] M. Caboara, The Chen-Reed-Helleseth-Truong Decoding Algorithm and the Gianni-Kalkbrenner Gröbner Shape Theorem ,*J AAECC*, **13** (2002)

[3] X. Chen, I. S. Reed, T. Helleseth, K. Truong, Use of Gröbner Bases to Decode Binary Cyclic Codes up to the True Minimum Distance, *IEEE Trans. on Inf. Th.*, **40** (1994) , 1654–1661.

[4] X. Chen, I. S. Reed, T. Helleseth, K. Truong, General Principles for the Algebraic Decoding of Cyclic Codes, *IEEE Trans. on Inf. Th.*, **40** (1994) , 1661–1663.

[5] X. Chen, I. S. Reed, T. Helleseth, K. Truong, Algebraic decoding of cyclic codes: A polynomial Ideal Point of View, *Contemporary Mathematics*, **168** (1994), 15–22

[6] A.B. III Cooper, Direct solution of BCH decoding equations, In E. Arikan (Ed.) *Communication, Control and Singal Processing*, 281–286, Elsevier (1990)

[7] A.B. III Cooper, Finding BCH error locator polynomials in one step *Electronic Letters*, **27** (1991) 2090–2091

[8] P. Loustaunau, E.V. York, On the decoding of cyclic codes using Gröbner bases,*J AAECC*, **8** (1997) 469–483.

[9] E. Orsini, M. Sala, Correcting errors and erasures via the syndrome variety, *J. Pure Appl. Algebra*, **200** (2005), 191–226.

[10] E. Orsini, M. Sala, General error locator polynomials for binary cyclic codes with $t \leq 2$ and $n < 63$, *BCRI preprint*, 2005, available at `http://www.bcri.ucc.ie`.