Efficient decoding of (binary) cyclic codes above the correction capacity of the code using Gröbner bases

Daniel Augot
INRIA-Rocquencourt, Bat. 10
Domaine de Voluceau, B.P. 105
F-78153 Le Chesnay Cedex
e-mail: Daniel.Augot@inria.fr

Magali Bardet
Projet SPACES LIP6/LORIA
CNRS/UPMC/INRIA
8, rue du capitaine Scott F-75015 Paris
e-mail: bardet@calfor.lip6.fr

Jean-Charles Faugère
Projet SPACES LIP6/LORIA
CNRS/UPMC/INRIA
8, rue du capitaine Scott F-75015 Paris
e-mail: jcf@calfor.lip6.fr

Abstract — **This paper revisits the topic of decoding cyclic codes with Gröbner bases. We introduce new algebraic systems, for which the Gröbner basis computation is easier. We show that *formal* decoding formulas are too huge to be useful, and that the most efficient technique seems to be to recompute a Gröbner basis for each word (*online* decoding). We use new Gröbner basis algorithms and "*trace preprocessing*" to gain in efficiency.**

I. Introduction

Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_2$, with defining set $Q \subset \{1,\dots,n\}$ and correction capacity t, and let $\alpha \in \mathbb{F}_{2^m}$ be a primitive n-th root of unity. For any error e of weight v, if Z_j^* denote the locators of e, we can compute its *syndroms* $S_i^* = e(\alpha^i) = \sum_{j=1}^{v} Z_j^{*i}\ \forall i \in Q$. As long as $v \le t$, the system $\textsc{Syn}_v = \left\{\ S_i - \sum_{j=1}^{v} Z_j^i,\ \ i \in Q\ \right\}$ specialized for $S_i = S_i^*$ has a unique solution (cf. [4]). To use the symmetry of the problem, we introduce the symmetric functions of the locators: $\textsc{Sym}_v = \left\{\ \sigma_j - \sum_{l_1<\dots<l_j} Z_{l_1}\cdots Z_{l_j},\ j \in [1,v]\ \right\}$. The S_i^*'s and the σ_j^*'s associated to the Z_j^*'s are also solutions of the following system (cf. [1])

$$\textsc{Newton}_v = \left\{ \begin{array}{l} S_i + \sum_{j=1}^{i-1}\sigma_j S_{i-j} + i\sigma_i,\ i \in [1,v] \\ S_i + \sum_{j=1}^{v}\sigma_j S_{i-j},\ i \in [v, v+n-1] \end{array} \right. \quad (1)$$

A Gröbner basis describes the set $V_{\overline{\mathbb{K}}}(I) = \{x \in \overline{\mathbb{K}}^s : \forall f \in I,\ f(x) = 0\}$ of solutions of an ideal $I \subset \mathbb{K}[x_1,\dots,x_s]$ where $\overline{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$. To compute $V_{\mathbb{K}}(I) = V_{\overline{\mathbb{K}}}(I) \cap \mathbb{K}^s$, we have to add the field equations. We add a $^+$ to an ideal to denote the ideal together with the field equations ($Z_j^{n+1} - Z_j, S_i^{2^m} - S_i$ or $\sigma_j^{2^m} - \sigma_j$).

It has been shown that the problem of decoding cyclic codes up to their true minimum distance can be solved by the use of Gröbner bases [3], with the algebraic system $\textsc{Syn}_v^+$.

II. New Systems and their properties

Starting from the system (1), we eliminate the unknowns syndroms S_i, $i \notin Q$ to obtain the new system $\textsc{Bin} = \{S_i - f_i(\sigma_1,\dots,\sigma_v)\ \ i \in Q\}$, where the f_i's are the Waring functions. We show that this new system and the systems $\textsc{Sym}_v$ and $\textsc{Newton}_v$ used in [3, 4] are closely related, and that for these systems the field equations are not necessary:

Proposition 1. *The ideals and their variety are related by:*

$$\begin{array}{rcl} \langle \textsc{Bin}_v^+ \rangle = \langle \textsc{Syn},\textsc{Sym}_v^+ \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}] & = & \langle \textsc{Newton}_v^+ \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}] \\ \langle \textsc{Bin} \rangle = \langle \textsc{Syn},\textsc{Sym}_v \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}] & = & \langle \textsc{Newton}_v \rangle \cap \mathbb{F}_2[\underline{\sigma}_v, \underline{S}] \\ V_{\overline{\mathbb{F}_2}}(\textsc{Syn},\textsc{Sym}_v^+) & = & V_{\overline{\mathbb{F}_2}}(\textsc{Syn},\textsc{Sym}_v) \\ V_{\overline{\mathbb{F}_2}}(\textsc{Newton}_v^+) & = & V_{\overline{\mathbb{F}_2}}(\textsc{Newton}_v) \end{array}$$

n	d	$\mathbb{F}_{2^m}$	v	number of multiplications in $\mathbb{F}_{2^m}$
73	13	2^9	$3,4,5,6,7$	$2^{5.4}, 2^{7.2}, 2^{10.5}, 2^{13.6}, 2^{17.4}$
89	17	2^{11}	$3,4,5,6,7,8$	$2^{5.1}, 2^{8.9}, 2^{11.6}, 2^{15.5}, 2^{20.3}, 2^{25.0}$
113	15	2^{28}	$3,4,5,6,7,8$	$2^{6.3}, 2^{8.9}, 2^{12.0}, 2^{15.6}, 2^{18.8}, 2^{23.9}$

Table 1: Decoding QR Codes

Proposition 2 (Uniqueness). *Let $\underline{S}^* \subset \mathbb{F}_{2^m}$ be the syndrom of an error e of weight $v \le t$, then the specialized system $\textsc{Bin}(\underline{S}^*)$ has a unique solution $(\sigma_1^*,\dots,\sigma_v^*)$ and $L_e(Z) = \sum_{j=0}^{v}\sigma_j^* Z^{v-j}$ is the locator polynomial of e. In practice, the Gröbner basis of $\textsc{Bin}(\underline{S}^*)$ is always $\{\sigma_1 + \sigma_1^*,\dots,\sigma_v + \sigma_v^*\}$.*

Proposition 3 (List Decoding). *If $v > t$ then the Gröbner basis of $\textsc{Bin}(\underline{S}^*)$ gives all the possible errors of weight at most v that have $\underline{S}^*$ as syndroms.*

With these new systems, we are able to do *formal* decoding as well as *online* decoding. But the size of the formal formulas are so huge that the computation of the Gröbner basis is intractable, and even if we could obtain these formulas, the cost of their evaluation would be much too large.

III. Practical decoding

In practice we do *online* decoding with a subset of the system $\textsc{Bin}$ (we take the minimal number of equations to have a single solution, and choose the equations of minimal degree to speed the computation). This is a very general method, we only need the length and the defining set of the cyclic code.

If the field is big enough (e.g. 2^{20}), we use a general method for solving systems with parameters: the behavior of the Gröbner basis computation is almost the same for all the possible values of the syndroms corresponding to an error of a given weight. Hence as a *preprocessing*, we can compute a Gröbner basis for $\textsc{Bin}(S_{e_0}^*)$ for a random error e_0 of weight v, and record the *trace* of the computation (we do it as a C program). Then for any error e, the C program executed on $\textsc{Bin}(S_e^*)$ gives the values of the σ_j's. This reduce drastically the complexity of the online computation (by a factor 1000).

This method is implemented in Maple, and call the C software FGb from the third author to compute a Gröbner basis. FGb is an implementation of the algorithm F4 [2].

References

[1] D. Augot. Description of minimum weight codewords of cyclic codes by algebraic systems. *Finite Fields Appl.*, vol. 2, pp. 138–152, 1996.

[2] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra*, 139(1-3):61–88, 1999.

[3] P. Loustaunau and E. Von York. On the decoding of cyclic codes using Gröbner bases. *Appl. Algebra Eng. Commun. Comput.*, 8(6):469–483, 1997.

[4] I.S. Reed, T.K. Truong, X. Chen, and X. Yin. The algebraic decoding of the (41, 21, 9) quadratic residue code. *IEEE Trans. Inform. Theory*, 38(3):974–986, 1992.