Decoding error-correcting codes with Gröbner bases

Stanislav Bulygin
Technical University of Kaiserslautern
Department of Mathematics
P.O. Box 3049, 67653 Kaiserslautern
Germany
bulygin@mathematik.uni-kl.de

Ruud Pellikaan
Eindhoven University of Technology
Department of Mathematics
P.O. Box 513, NL-5600 MB, Eindhoven In
The Netherlands
g.r.pellikaan@tue.nl

Proceedings of 28th Symposium on Information Theory in the Benelux,
Enschede, May 24-25, (R. Veldhuis, H. Cronie, H. Hoeksema eds.) pp. 3-10, 2007.

Abstract

The decoding of arbitrary linear block codes is accomplished by solving a system of quadratic equations by means of Buchberger's algorithm for finding a Gröbner basis. This generalizes the algorithm of Berlekamp-Massey for decoding Reed-Solomon, Goppa and cyclic codes up to half the true minimum distance by introducing the unknown syndromes as variables. The complexity of this algorithm is exponential and the complexity coefficient is measured under the assumption that the over-determined system of quadratic equations is semi-regular using the results of Bardet et al. [5]. The complexity is compared to existing bounded distance decoding algorithms. Our method can be extended to complete and generic decoding, and to finding the minimum distance and the complete weight distribution.

1 Introduction

In this paper we consider bounded distance decoding of arbitrary linear codes with the use of Gröbner bases. The decoding of cyclic codes up to half the BCH distance is well-known by Peterson, Arimoto and Gorenstein-Zierler, by means of the syndromes s_i of a received word and the error-locator polynomial with coefficients σ_i. They satisfy generalized Newton identities. These equations form a system of t linear equations in the unknowns $\sigma_1, \ldots, \sigma_t$ with the known syndromes $s_1, \ldots, s_{2t}$ as coefficients, if the defining set of the cyclic code contains $2t$ consecutive elements. Gaussian elimination solves this system of equations with complexity $\mathcal{O}(n^3)$. This complexity was improved by the algorithm of Berlekamp-Massey and a variant of the Euclidean algorithm due to Sugiyama et al. Both these algorithms are more efficient than solving the system of linear equations, and are basically equivalent but they decode up to the BCH error-correcting capacity, which is often strictly smaller than the true capacity. All these methods do not correct up to the true error-correcting capacity.

The Gröbner bases techniques were addressed to remedy this problem. These methods can be divided into the following categories:

- Unknown syndromes by Berlekamp [7] and Tzeng-Hartmann-Chien [22, 23, 25],
- Power sums by Cooper [14, 15, 16] and Chen-Reed-Helleseth-Truong [10, 11, 12],
- Newton identities by Augot-Charpin-Sendrier [1, 2, 3].

Our method is a generalization of the first one. Recent work on the second method is by Mora-Sala [24] for cyclic codes. The second method was generalized to arbitrary linear codes by Lax-Fitzgerald [18, 19].

The theory of Gröbner basis is about solving systems of polynomial equations in several variables and can be viewed as a common generalization of linear algebra that deals with linear systems of equations in several variables and the Euclidean Algorithm that is about polynomial equations of arbitrary degree in one variable. The polynomial equations are linearized by treating the monomials as new variables. In this way the number of variables grows exponentially in the degree of the polynomials. The complexity of computing a Gröbner basis is doubly exponential in general, and exponential in our case of a finite set of solutions. The complexity of our algorithm is exponential and the complexity coefficient is measured under the assumption that the over-determined system of quadratic equations is semi-regular using the results of Bardet et al. [5] applied to algorithm F5 of Faugère [17]. The complexity is compared to existing bounded distance decoding algorithms such as exhaustive search, syndrome decoding and covering set decoding. Our method can be extended to complete and generic decoding, and to finding the minimum distance and the complete weight distribution.

2 Unknown syndromes and an MDS basis

Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{F}_q^n$. Now B is the $n \times n$ matrix with $\mathbf{b}_1, \ldots, \mathbf{b}_n$ as rows.

The *(unknown) syndrome* $\mathbf{u}(B, \mathbf{e})$ of a word $\mathbf{e}$ with respect to B is the column vector $\mathbf{u}(B, \mathbf{e}) = B\mathbf{e}^T$. It has entries $u_i(B, \mathbf{e}) = \mathbf{b}_i \cdot \mathbf{e}$ for $i = 1, \ldots, n$.

The matrix B is invertible. So the syndrome $\mathbf{u}(B, \mathbf{e})$ determines the error vector $\mathbf{e}$ uniquely, since

$$B^{-1}\mathbf{u}(B, \mathbf{e}) = B^{-1}B\mathbf{e}^T = \mathbf{e}^T.$$

From now on the following abbreviations $\mathbf{u}(\mathbf{e})$ and $u_i(\mathbf{e})$ are used for $\mathbf{u}(B, \mathbf{e})$ and $u_i(B, \mathbf{e})$, respectively.

Define the coordinatewise star product of two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ by
$\mathbf{x} * \mathbf{y} = (x_1y_1, \ldots, x_ny_n)$. Then $\mathbf{b}_i * \mathbf{b}_j$ is a linear combination of the basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, that is there are constants $\mu_{ijl} \in \mathbb{F}_q$ such that

$$\mathbf{b}_i * \mathbf{b}_j = \sum_{l=1}^{n} \mu_{ijl}\mathbf{b}_l.$$

The elements $\mu_{ijl} \in \mathbb{F}_q$ are called the *structure constants* of the basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$.

Define the $n \times n$ matrix of *(unknown) syndromes* $\mathcal{U}(\mathbf{e})$ of a word $\mathbf{e}$ by $u_{ij}(\mathbf{e}) = (\mathbf{b}_i * \mathbf{b}_j) \cdot \mathbf{e}$.

The relation between the entries of the matrix $\mathcal{U}(\mathbf{e})$ and the vector $\mathbf{u}(\mathbf{e})$ of unknown syndromes is given by

$$u_{ij}(\mathbf{e}) = \sum_{l=1}^{n} \mu_{ijl}u_l(\mathbf{e}).$$

Lemma 2.1 *The rank of* $\mathcal{U}(\mathbf{e})$ *is equal to the weight of* $\mathbf{e}$.

For the proof we refer to [9].

Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{F}_q^n$. Let B_r be the $r \times n$ matrix with $\mathbf{b}_1, \ldots, \mathbf{b}_r$ as rows. Let $B = B_n$. We say that $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is an *ordered MDS basis* and B an *MDS matrix* if all the $t \times t$ submatrices of B_t have rank t for all $t = 1, \ldots, n$. Let C_t be the code with B_t as parity check matrix. If B is an MDS matrix, then C_t is an MDS code for all t.

Let $\mathcal{U}$ be the $n \times n$ matrix with entries U_{ij}. Let $\mathcal{U}_{u,v}$ be the $u \times v$ matrix with entries U_{ij} with $1 \leq i \leq u$ and $1 \leq j \leq v$.

Proposition 2.2 *Suppose that B is an MDS matrix. Let $w = wt(\mathbf{e})$. If $u \geq w$, then*

$$rank(\mathcal{U}_{uv}(\mathbf{e})) = \min\{v, w\}.$$

For the proof we refer to [9].

Hence $\mathcal{U}_{nv}(\mathbf{e})$ has rank v if $v \leq \mathrm{wt}(\mathbf{e})$, and its rank is $\mathrm{wt}(\mathbf{e})$ if $v > \mathrm{wt}(\mathbf{e})$.

In case $n \leq q$ MDS bases are known to exist. Let $\mathbf{x} = (x_1, \ldots, x_n)$ be an n-tuple of mutually distinct elements in $\mathbb{F}_q$. Define

$$\mathbf{b}_i = (x_1^{i-1}, \ldots, x_n^{i-1}).$$

Then $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is an MDS basis and is called a *Vandermonde basis* and the corresponding matrix is denoted by $B(\mathbf{x})$ and is called a *Vandermonde matrix*. In particular, if $\alpha \in \mathbb{F}_q^*$ is an element of order n and $x_j = \alpha^{j-1}$ for all j, then $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is called a *Reed-Solomon (RS) basis* and the corresponding matrix is called a *RS matrix* and denoted by $B(\alpha)$. If $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is an RS basis of $\mathbb{F}_q^n$, then $b_i * b_j = b_{i+j-1}$ and $u_{ij}(\mathbf{e}) = u_{i+j-1}(\mathbf{e})$.

3 Decoding up to half the minimum distance

Without loss of generality we may assume that after a finite extension of the finite field $\mathbb{F}_q$ we have $n \leq q$. Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{F}_q^n$. From now on we assume that the corresponding matrix B is an MDS matrix.

Let C be an $\mathbb{F}_q$-linear code with parameters $[n, k, d]$. Choose a parity check matrix H of C. The redundancy is $r = n - k$. Let $\mathbf{h}_1, \ldots, \mathbf{h}_r$ be the rows of H. The row $\mathbf{h}_i$ is a linear combination of the basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$. So there are constants $a_{ij} \in \mathbb{F}_q$ such that

$$\mathbf{h}_i = \sum_{j=1}^{n} a_{ij} \mathbf{b}_j.$$

In other words $H = AB$ where A is the $r \times n$ matrix with entries a_{ij}.

Let $\mathbf{y} = \mathbf{c} + \mathbf{e}$ be a received word with $\mathbf{c} \in C$ a codeword and $\mathbf{e}$ an error vector. The syndromes of $\mathbf{y}$ and $\mathbf{e}$ with respect to H are equal and known:

$$s_i(\mathbf{y}) := \mathbf{h}_i \cdot \mathbf{y} = \mathbf{h}_i \cdot \mathbf{e} = s_i(\mathbf{e})$$

and they can be expressed in the unknown syndromes of $\mathbf{e}$ with respect to B:

$$s_i(\mathbf{y}) = \sum_{j=1}^{n} a_{ij} u_j(\mathbf{e}),$$

since $\mathbf{h}_i = \sum_{j=1}^{n} a_{ij}\mathbf{b}_j$ and $\mathbf{b}_j \cdot \mathbf{e} = u_j(\mathbf{e})$.

The system $E(\mathbf{y})$ of equations in the variables $U_1, \ldots, U_n$ is given by:

$$\sum_{l=1}^{n} a_{jl}U_l \quad = \quad s_j(\mathbf{y}) \quad \text{for} \quad j = 1, \ldots, r.$$

The system $E(t)$ of equations in the variables $U_1, \ldots, U_n, V_1, \ldots, V_t$ is given by

$$\sum_{j=1}^{t} \sum_{l=1}^{n} \mu_{ijl}U_l V_j \quad = \quad \sum_{l=1}^{n} \mu_{it+1l}U_l \quad \text{for} \quad i = 1, \ldots, n.$$

The system $E(t, \mathbf{y})$ of equations is the union of $E(t)$ and $E(\mathbf{y})$. It consists of $n - k$ linear equations in n variables and n quadratic equations in $n + t$ variables. The linear equations are independent and can be used to eliminate $n - k$ variables. Thus we get a system of n quadratic equations in $k + t$ variables.

Theorem 3.1 *Let B be an MDS matrix with structure constants μ_{ijl}. Let H be a parity check matrix of the code C such that $H = AB$. Let $\mathbf{y} = \mathbf{c} + \mathbf{e}$ be a received word with $\mathbf{c}$ in C the codeword sent and $\mathbf{e}$ the error vector. Suppose that the weight of $\mathbf{e}$ is not zero and at most $(d(C) - 1)/2$. Let t be the smallest positive integer such that $E(t, \mathbf{y})$ has a solution $(\mathbf{u}, \mathbf{v})$ over some extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. Then $wt(\mathbf{e}) = t$ and the solution is unique satisfying $\mathbf{u} = \mathbf{u}(\mathbf{e})$.*

For the proof we refer to [9].

4 Simulations and experimental results

All computations in this section were undertaken on an AMD Athlon 64 Processor 2800+ (1.8MHz), 512MB RAM under Linux. The computations of Gröbner bases were realized in SINGULAR 3-0-1 [20, 21]. The command `std` was chosen as more effective than `slimgb`. The file Err.lib containing the algorithms used can be found at [8].

Here we present some results on decoding with the use of Theorem 3.1 for binary random codes. First we determine the minimum distance of a random code with a similar procedure and than perform decoding of some given number of received words. The number of errors that occur in these received words equals the error capacity of the code. The results are given in the following table, with in the columns: the parameters of the code, the error-correcting capacity, time to compute the minimum distance, total time to decode with Gröbner bases, the number of received words, and the average time to decode with Gröbner bases, respectively. The time is provided in seconds.

Code	err. cap.	mindist.	GB dec.	no. of rec.	average
[25,11,4]	1	2.99	1.10	300	0.0037
[25,11,5]	2	21.58	2.89	300	0.0096
[25,8,5]	2	0.99	1.84	300	0.0061
[25,8,6]	2	3.38	1.79	300	0.0060
[25,8,7]	3	12.26	6.94	300	0.0231
[31,15]	2	-	10.76	300	0.0359
[31,15]	3	-	11.19	10	1.119

We only cite the time needed for GB computations in the decoding. They are responsible for approximately 90% of the overall decoding time. The rest is spent on auxiliary operations and manipulations. The bar "-" means that a computation took more than 1000 sec. and we were not able to compute the minimum distance in a short time, so we assumed the error capacity.

We are able to correct even more errors in larger codes. Next table shows timings for binary $[120, 10], [120, 20], [120, 30]$ and $[150, 10]$ codes, where 1 means one second or less. As the behavior of decoding seems to be more or less the same for all error-vectors of a given weight, we have used only one received word in the table below.

no. of err.	[120,40]	[120,30]	[120,20]	[120,10]	[150,10]
2	1	1	1	1	1
3	13	1	1	1	1
4	313	9	1	1	1
5	-	62	1	1	1
6	-	200	5	1	3
7	-	933	14	1	4
8	-	-	32	1	4
9	-	-	74	1	4
10	-	-	183	2	6
11	-	-	633	3	6
12	-	-	-	4	6
13	-	-	-	5	8
14	-	-	-	6	8
15	-	-	-	14	10
16	-	-	-	20	11
17	-	-	-	29	16
18	-	-	-	71	16
19	-	-	-	139	34
20	-	-	-	327	53
21	-	-	-	483	84
22	-	-	-	-	133
23	-	-	-	-	241
24	-	-	-	-	513

5 Complexity of the algorithm

In general it is very hard to estimate the complexity of the algorithms, which compute Gröbner bases. Only the worst-case complexities are known. In practice, however, these algorithms can perform much better. As parameters for the complexity we take the number of variables l, the number of equations m and the maximum degree of the polynomials which occur in the system considered.

Bardet et al. [5] consider a generalization of regular sequences to the over-determined

case, namely semi-regular sequences. In particular, they study the index of regularity i_{reg} of quadratic semi-regular systems which gives an upper bound for the complexity of algorithm F5 of Faugère [17]. The idea is that polynomial equations in several variables are linearized by treating monomials as new variables. In this way we get an infinite number of variables. The index of regularity estimates the maximum number of variables needed in the computation of a Gröbner basis. Let $\alpha > 1$ be fixed. In [5] it is shown that the index of regularity is $i_{reg} = A \cdot l + o(l)$, for a semi-regular system of $m = [\alpha l]$ homogeneous quadratic equations in l variables, where

$$A = \alpha - \frac{1}{2} - \sqrt{\alpha(\alpha - 1)}.$$

The F5 algorithm performs Gaussian elimination on a matrix of size

$$\binom{l + i_{reg}}{l}.$$

The complexity of solving a $N \times N$ linear system of equations is $O(N^\omega)$, where $\omega < 2.39$ is the exponent in the advanced Gaussian elimination algorithms. The total number of arithmetic operations in $\mathbb{F}_q$ performed by the matrix version of F5 is bounded by

$$O\Big(m \cdot i_{reg} \binom{l + i_{reg} - 1}{i_{reg}}^\omega\Big).$$

Bardet et al. [5] write "... over a finite field of positive characteristic we conjecture that the proportion of semi-regular sequences tends to 1 as the number of variables tends to infinity". Thus we think that it is reasonable to conjecture that our systems also possess this property asymptotically.

Now the complexity of our method is estimated by assuming that they are semi-regular asymptotically. We concentrate on the system for decoding up to half the minimum distance, the so-called bounded hard decoding. We compare our estimates with estimates for the known algorithms for such decoding as given in [6]. The relative minimum distance of an $[n, k, d]$ linear code is $\delta = d/n$ and the information rate R is defined by $R = k/n$. We use the fact [13] that virtually all linear codes lie on the Gilbert-Varshamov bound. Now our method gives a quadratic system of $m = n$ equations in $l = k + t$ variables, where $t = \lfloor (d-1)/2 \rfloor$. Hence $\alpha = 1/(R + \delta/2)$.

The following notion is our measuring instrument. Given a decoding algorithm for a code C of rate R over $\mathbb{F}_q$ of complexity $Compl(C)$, the complexity coefficient $CC(R)$ is defined as $CC(R) = \frac{1}{n} \log_q(Compl(C))$. The complexity coefficient for our method under the asymptotic semi-regularity assumption is computed as follows:

$$\omega \cdot \log_q 2 \cdot \frac{A+1}{\alpha} \cdot H_2\Big(\frac{1}{A+1}\Big),$$

where $A = \alpha - \frac{1}{2} - \sqrt{\alpha(\alpha-1)}$ and $\alpha = 1/(R + \delta/2)$ and $\delta = H_q^{-1}(1-R)$, with H_q the q-ary entropy function.

It turns out that in the binary case the complexity of our method is worse than exhaustive search. But with increasing alphabet our method is better. Figure 1 depicts the complexity coefficients for $q = 2^{10}$ of exhaustive search (ES), syndrome decoding (SD), systematic coset search (SCS), covering polynomials (CP) and covering sets (CD), see [6, 13], and our method using quadratic equations (QED).

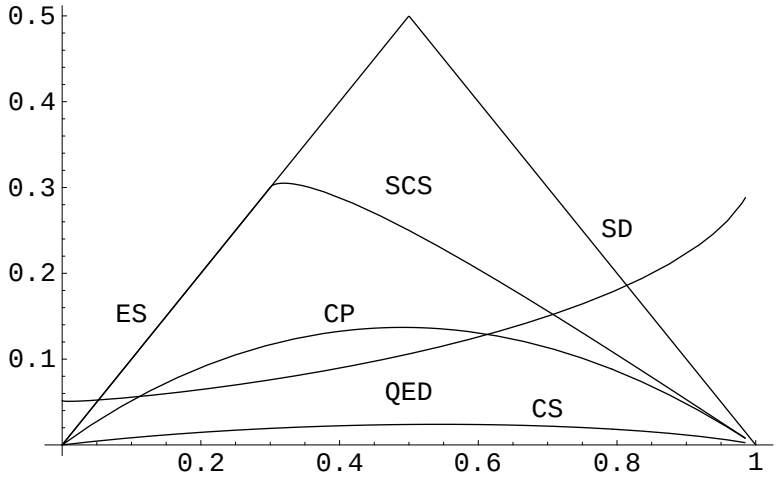

Figure 1: Comparison of complexities for $q = 2^{10}$

Acknowledgment

The first author would like to thank "DASMOD: Cluster of Excellence in Rhineland-Palatinate" for funding his research, and also personally his Ph.D. supervisor Prof.Dr. Gert-Martin Greuel and his second supervisor Prof.Dr. Gerhard Pfister for continuous support. This work has been continuously inspired by the Special Semester on Groebner Bases, February 1 - July 31, 2006, organized by RICAM, Austrian Academy of Sciences, and RISC, Johannes Kepler University, Linz, Austria.

References

[1] D. Augot, P. Charpin, N. Sendrier, "The minimum distance of some binary codes via the Newton's Identities," *Eurocodes'90, LNCS 514,* p 65-73, 1990.

[2] D. Augot, P. Charpin and N. Sendrier, "Studying the locator polynomial of minimum weight codewords of BCH codes," *IEEE Trans. Inform. Theory*, vol. IT-38, pp. 960-973, May 1992.

[3] D. Augot, M. Bardet, J.-C. Faugère "Efficient Decoding of (binary) Cyclic Codes beyond the correction capacity of the code using Gröbner bases," *INRIA Report,* no. 4652, Nov. 2002.

[4] M. Bardet and J.-C. Faugère and B. Salvy, "Complexity of Gröbner basis computation for semi-regular overdetermined sequences over GF(2) with solutions in GF(2)," *INRIA Report,* no. 5049, 2003.

[5] M. Bardet and J.-C. Faugère and B. Salvy and B-Y. Yang "Asymptotic Behaviour of the Index of Regularity of Quadratic Semi-regular Polynomial Systems," in *MEGA 2005, Eighth International Symposium on Effective Methods in Algebraic Geometry*, Porto Conte, Alghero, Sardinia (Italy), May 27th - June 1st, 2005.

[6] A. Barg "Complexity issues in coding theory," in *Handbook on Coding Theory*, V.S Pless and W.C. Huffmann eds., pp.649-754, 1998

[7] E.R. Berlekamp, *Algebraic coding theory,* Mc Graw Hill, New York, 1968.

[8] S. Bulygin, Err.lib, http://www.mathematik.uni-kl.de/~bulygin/files/Err.lib, 2006.

[9] S. Bulygin and Pellikaan, "Bounded distance decoding of linear error-correcting codes with Gröbner bases," submitted to *Journal Symbolic Computations.*

[10] X. Chen, I.S. Reed, T. Helleseth and T.K. Truong, "Algebraic decoding of cyclic codes: a polynomial point of view," *Contemporary Math.* vol. 168, pp. 15-22, 1994.

[11] X. Chen, I.S. Reed, T. Helleseth and T.K. Truong, "Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance," *IEEE Trans. Inform. Theory,* vol. IT-40, pp. 1654-1661, Sept. 1994.

[12] X. Chen, I.S. Reed, T. Helleseth and T.K. Truong, "General principles for the algebraic decoding of cyclic codes," *IEEE Trans. Inform. Theory,* vol. IT-40, pp. 1661-1663, Sept. 1994.

[13] J.T. Coffey and R.M. Goodman and P.G. Farrell "New approaches to reduced-complexity decoding", *Discrete Applied Mathematics*, no.33, pp.43-60, 1991.

[14] A.B. Cooper III, "Direct solution of BCH decoding equations," *Communication, Control and Signal Processing,* Elsevier Sc. Publ., pp. 281-286, 1990.

[15] A.B. Cooper III, "Finding BCH error locator polynomials in one step," *Electronic Letters*, vol. 27 ,pp. 2090-2091, 1991.

[16] A.B. Cooper, "Toward a new method of decoding algebraic codes using Gröbner bases," *Trans. 10th Army Conf. Appl. Math. and Comp.,*, pp.1-11, 1993.

[17] J.-C. Faugère, "A new efficient algorithm for computing Groebner bases without reduction to zero F5," in *Proceedings of ISSAC*, T.Mora, ed., pp.75-83, 2002.

[18] J. Fitzgerald, "Applications of Gröbner bases to Linear Codes," *Ph.D. Thesis*, Louisiana State University, 1996.

[19] J. Fitzgerald and R.F. Lax, "Decoding affine variety codes using Gröbner bases," *Designs, Codes and Cryptography,* vol. 13, pp. 147–158, 1998.

[20] G.-M.Greuel and G.Pfister, "A SINGULAR Introduction to Commutative Algebra", *Springer-Verlag,* 2002.

[21] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3.0. A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern (2005). `http://www.singular.uni-kl.de`.

[22] C.R.P. Hartmann, "Decoding beyond the BCH bound," *IEEE Trans. Inform. Theory,* vol. IT-18, pp. 441-444, May 1972.

[23] C.R.P. Hartmann and K.K. Tzeng, "Decoding beyond the BCH bound using multiple sets of syndrome sequences," *IEEE Trans. Inform. Theory,* vol. IT-20, pp. 292-295, Mar. 1974.

[24] T. Mora and M.Sala, "On the Groebner bases for some symmetric systems and their application to Coding Theory," *J. Symb. Comp.*, vol. 35, no.2, p.177-194, 2003.

[25] K.K. Tzeng, C.R.P. Hartmann and R.T. Chien, "Some notes on iterative decoding," in *Proc. 9th Allerton Conf. Circuit and Systems Theory,* Oct. 1971.