Decoding linear codes via solving systems of polynomial equations

Stanislav Bulygin and Ruud Pellikaan

IMA Annual Program Year Workshop "Complexity, Coding, and Communications"

bulygin@mathematik.uni-kl.de, g.r.pellikaan@tue.nl

DASMOD Dependable Adaptive Systems and Mathematical Modeling

Technische Universität Kaiserslautern

TU/e technische universiteit eindhoven

Introduction

We consider the problem of decoding for linear codes. Let C be an $[n,k,d]$ linear code over $\mathbb{F}_q$. Suppose we transmit a codeword c and after transmition obtain $y = c + e$, e an error vector.

Complete decoding: Given $y \in \mathbb{F}_q^n$ find $c \in C : y = c + e$ and $wt(e)$ is minimal, where wt is the weight of a vector. *Bounded decoding*: The same as above, but additional constraint $wt(e) \leq (d-1)/2$ is given.

We concentrate more on the latter.

Different methods of decoding

- Exhaustive search.
- Syndrome decoding.
- Advanced linear algebra (bit swapping etc.)
- Decoding based on optimization techniques in the Euclidian space.
- Decoding via solving systems of polynomial equations.

Our work belongs to the last part. This method was initially proposed for cyclic codes by Cooper (1990-1), the works of Chen, Reed, Helleseth, Truong (1994) and later works of Sala, Mora, Augot, Bardet, Faugere followed. Some generalizations to linear codes by Lax, Fitzgerald and O'Keeffe, Fitzpatrick were proposed.

MDS basis

Let $b_1, \ldots, b_n$ be a basis of $\mathbb{F}_q^n$ and let B be a matrix with $b_1, \ldots, b_n$ as rows. The *unknown syndrome* $u(B,e)$ of a vector e w.r.t B is the column vector $u(B,e) = Be^T$; it has entries $u_i(B,e) = b_i \cdot e$ for $i = 1, \ldots, n$. We abbreviate $u(B,e)$ by $u(e)$.

For two vectors x and y, $x * y := (x_1 y_1, \ldots, x_n y_n)$.

Then we have $b_i * b_j = \sum_{l=1}^{n} c_{ijl} b_l$ for some c_{ijl}, which are called structure constants.

Let B_t be a submatrix of B composed of the first t rows. We say that the basis $b_1, \ldots, b_n$ is an *MDS basis* and matrix B is in the *MDS form* iff all submatricies of B_t have full rank for all $t = 1, \ldots, n$.

The system

We may assume that after a finite extension of the field $\mathbb{F}_q$ we have $n \leq q$, so that we can construct an MDS basis.

Let H be a parity check matrix of the code C. We can express: $h_i = \sum_{j=1}^{n} a_{ij} b_j$, where h_i are the rows of H, $i = 1, \ldots, n-k$. For all codewords $h_i \cdot c = 0$, so $s_i(y) := h_i \cdot y = h_i \cdot e =: s_i(e)$, where $s(y)$ is a usual *known syndrome*. We have $s(y) = \sum_{j=1}^{n} a_{ij} u_j(e)$. Define the following ideals in the ring $\mathbb{F}_q[U_1, \ldots, U_n, V_1, \ldots, V_t]$

- $J(y) = \langle \sum_{j=1}^{n} a_{ij} U_j - s_i(y) \rangle_{i=1,\ldots,n-k}$
- $I(t,U,V) = \langle \sum_{j=1}^{t} U_{ij} V_j - U_{i,t+1} \rangle_{i=1,\ldots,n}$, where $U_{ij} = \sum_{l=1}^{n} c_{ijl} U_l$.
- $I(t,y) = J(y) + I(t,U,V)$.

Main results

Suppose that $wt(e) \leq (d-1)/2$, $wt(e) \neq 0$. Let t be the smallest positive integer, such that the system $I(t,y)$ has a solution (u,v) over an algebraic closure $\bar{\mathbb{F}}$. Then:

- $t = wt(e)$.
- the solution (u,v) is unique over the algebraic closure and satisfies $u_i = u_i(e)$ for all $i = 1, \ldots, n$.
- multiplicity of the solution (u,v) is 1, so the reduced Gröbner basis of $I(t,y)$ w.r.t any well ordering is of the form

$$U_i - u_i, i = 1, \ldots, n, V_j - v_j, j = 1, \ldots, t.$$

- after solving the system $I(t,y)$ decoding is simple:

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

Other problems that can be solved

- Finding minimum distance.
- Finding weight distribution.
- Complete decoding.
- Generic decoding.

for the latter three one needs to add the field equations.

Complexity estimates with semi-regular sequences

We want to estimate the complexity of finding the reduced Gröbner basis of the system $I(t,y)$. Estimates of complexity due to Bardet, Salvy, Faugere, Yang (2005) are available for the so-called *semi-regular sequences* and F5 algorithm by Faugere.

A homogeneous sequence of polynomials $(f_1, \ldots, f_m)$ from $\mathbb{F}[x_1, \ldots, x_l]$ is *semi-regular* if for all $i = 1, \ldots, m$ and g such that

$$g f_i \in \langle f_1, \ldots, f_{i-1} \rangle, \ \deg(g f_i) < i_{reg}$$

holds that $g \in \langle f_1, \ldots, f_{i-1} \rangle$. The *index of regularity* of a homogeneous zero-dimensional ideal $I = \langle f_1, \ldots, f_m \rangle$ is defined by

$$i_{reg}(I) = \min \left\{ d \geq 0 \mid \dim_{\mathbb{F}}(I(d)) = \binom{l'+d}{d} \right\},$$

where $I(d) := \{ f \in I, \deg(f) = d \}$ is the vector subspace of polynomials in I of degree d; $l' = l - 1$.

The complexity estimate that we need is: For a homogeneous semi-regular system the total number of arithmetic operations in $\mathbb{F}$ performed by F5 (matrix version) is bounded by

$$O\left(m \cdot i_{reg} \binom{l + i_{reg} - 1}{i_{reg}}^{\omega} \right),$$

where $\omega < 2.39$ is the exponent in the advanced Gaussian elimination algorithms. Bardet et al. conjecture that as the number of variables tends to infinity, the proportion of semi-regular sequences tends to 1, so it is reasonable to conjecture that also $I(t,y)$ is semi-regular asymptotically. We measure the complexity via *complexity coefficient*: 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

$$\frac{1}{n} \log_q(Compl(C)),$$

so that

$$Compl(C) = q^{nCC(R)}.$$

Complexity estimates with semi-regular sequences (cont.)

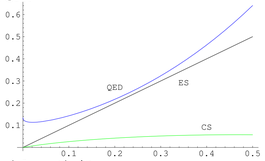
Using the results of Bardet et al. we obtain the complexity coefficient for our algorithm in the case of decoding random linear codes:

$$CC_{QED}(R) = \omega \log_q 2 \cdot \frac{A+1}{\alpha} \cdot H_2\left(\frac{1}{A+1}\right),$$

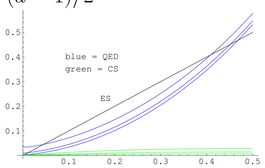
where $A = (\alpha - \frac{1}{2} - \sqrt{\alpha(\alpha-1)}), \alpha = \frac{1}{R+\delta/2}, \delta = H_q^{-1}(1-R)$, and $H_q(x) = -x \log_q x - (1-x) \log_q (1-x) + x \log_q (q-1)$ is the q-ary entropy function

Comparing with other algorithms

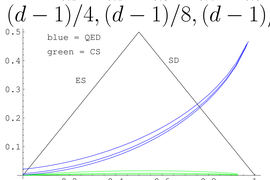
We compare the complexity coefficients of the following: QED = our method of quadratic equations decoding, ES = exhaustive search, SD = syndrome decoding, CS = covering set decoding, CP = covering polynomial decoding, SCS = systematic coset search.



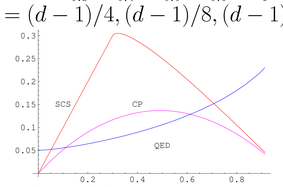
$q = 2, e = (d-1)/2$



$q = 2, e = (d-1)/4, (d-1)/8, (d-1)/16$



$q = 49, e = (d-1)/4, (d-1)/8, (d-1)/16$



$q = 2^{10}, e = (d-1)/2$

Experimental results

Below are the results obtained for computing the reduced Gröbner basis of $I(t,y)$ with SINGULAR computer algebra system. All computations were made on AMD Athlon 64 Processor 2800+ (1.8MHz), 512MB RAM under Linux Gentoo. We consider here only binary codes. The time is in seconds; "1" means 1 second or less. We write n, k as column headers.

e	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

For the "true" decoding when we do not know the number of errors that occurred, so we have to solve the systems $I(i,y)$ for $i = 1, \ldots, e$, where e is the actual number of errors. In the table below cumulative time needed to solve the first $e-1$ systems is shown, then time needed for solving the system $I(e,y)$ and the ratio between the two. The codes are: [120,40], $e = 4$; [120,30], $e = 7$; [120,20],$e = 11$; [120,10],$e = 21$; [150,10],$e = 24$.

14	273	312	628	651
313	933	633	483	513
0.04	0.29	0.49	1.3	1.27

Acknowledgements: The first author would like to thank "DASMOD: Cluster of Excellence in Rhineland-Palatinate" for funding his research. 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.