Decoding error-correcting codes with Gröbner bases

Ruud Pellikaan
joint work with
Stanislav Bulygin

EMS Joint Math Weekend, March 1, 2008

Outline

- Introduction, motivation
- Cyclic codes
- Gröbner bases
- Unknown syndromes and MDS bases
- Decoding up to half the minimum distance
- Simulations and experimental results
- Conclusion

Motivation

- Nearest neighbor decoding is NP-hard
  (Berlekamp-McEliece-Van Tilborg)
- Decoding up to half the designed minimum distance has polynomial complexity for
  BCH, Goppa, Reed-Solomon, Algebraic geometry codes.
- Question: Is decoding up to half the minimum distance of polynomial complexity?
- McEliece-Niderreiter crypto system assumes the answer is no.
- Application of Gröbner bases theory to Coding theory.

$\mathbb{F}_q$ is the finite field with with $q = p^e$ elements, p a prime.

A subspace of $\mathbb{F}_q^n$ of dimension k is a
linear code over $\mathbb{F}_q$ of length n and dimension k.

The weight of $\mathbf{y} \in \mathbb{F}_q^n$ is

$$\mathsf{wt}(\mathbf{y}) = |\{i : y_i \neq 0\}|.$$

The minimum distance d of a linear code C is

$$d = \min\{\mathbf{wt}(\mathbf{c}) : 0 \neq \mathbf{c} \in C\}.$$

Parameters of C are denoted by $[n, k, d]$
length n, dimension k and minimum distance d.

Redundancy is $r = n - k$.
Error-correcting capacity is $\lfloor (d-1)/2 \rfloor$.

The code C can be constructed via a generator matrix G, which is any $k \times n$ matrix with as rows a basis of C.

Alternatively, one can see C as a null-space of an $(n-k) \times n$ parity-check matrix H, so

$$\mathbf{c} \in C \Leftrightarrow H\mathbf{c}^T = 0.$$

The code C is cyclic, if $(c_{n-1}, c_0, \ldots, c_{n-2})$ is in C for every codeword $\mathbf{c} = (c_0, \ldots, c_{n-1})$ in C.

$(c_0, \ldots, c_{n-1})$ is represented by the polynomial

$$c(x) = \sum_{i=0}^{n-1} c_i x^i \text{ with } x^n = 1.$$

So $c(x)$ is an element of the factor ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.

Cyclic codes over $\mathbb{F}_q$ of length n correspond one-to-one to ideals in this factor ring.

Assume $(q, n) = 1$. Let $\mathbb{F} = \mathbb{F}_{q^m}$ be the splitting field of $X^n - 1$ over $\mathbb{F}_q$. Then $\mathbb{F}$ has a primitive n-th root of unity, denoted by a.

Let I be a subset of $\mathbb{Z}_n$. The cyclic code with defining set I is given by

$$c(x) \in C \text{ if } c(a^i) = 0 \text{ for all } i \in I.$$

The complete defining set of C is the set of all $i \in \mathbb{Z}_n$ such that $c(a^i) = 0$ for all $c(x) \in C$.

If $c(a^i) = 0$, then $c(a^{qi}) = (c(a^i))^q = 0$.

If i is in a defining set of C, then

$$(1, a^i, \ldots, a^{(n-1)i})\mathbf{c}^T = c_0 + c_1 a^i + \cdots + c_{n-1} a^{(n-1)i} = c(a^i) = 0.$$

Hence $(1, a^i, \ldots, a^{(n-1)i})$ is a parity check of C.

Let $\{i_1, \ldots, i_r\}$ be a defining set of C. Then

$$H = \begin{pmatrix} 1 & a^{i_1} & a^{2i_1} & \ldots & a^{(n-1)i_1} \\ 1 & a^{i_2} & a^{2i_2} & \ldots & a^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a^{i_r} & a^{2i_r} & \ldots & a^{(n-1)i_r} \end{pmatrix}.$$

is a parity check matrix of C.

Let

$$y(x) = c(x) + e(x)$$

$c(x)$ the transmitted codeword,
$y(x)$ the received word,
$e(x)$ the error vector.

Then $\mathbf{s}$ is the syndrome vector

$$\mathbf{s}^T := H\mathbf{y}^T = H(\mathbf{c}^T + \mathbf{e}^T) = H\mathbf{c}^T + H\mathbf{e}^T = H\mathbf{e}^T,$$

since $H\mathbf{c}^T = 0$.

Define

$$s_i = y(a^i) \text{ for all } i = 1, \ldots, n.$$

The vector $\mathbf{s} = \mathbf{y}H^T$ has entries $(s_{i_1}, \ldots, s_{i_r})$.

Then $s_i = e(a^i)$ for all i in the complete defining set.
These s_i are called the known syndromes.

The remaining s_i are called the unknown syndromes.

If the error vector is of weight t, then

$$\mathbf{e} = (0, \ldots, 0, e_{j_1}, 0, \ldots, 0, e_{j_l}, 0, \ldots, 0, e_{j_t}, 0, \ldots, 0),$$

where $1 \leq j_1 < \cdots < j_t \leq n$ and

$$e_j \neq 0 \text{ if and only if } j \in \{j_1, \ldots, j_t\}.$$

The error locations are

$$z_1 = a^{j_1}, \ldots, z_t = a^{j_t}$$

The error-locator polynomial

$$\sigma(Z) = \prod_{l=1}^{t}(Z - z_l).$$

Expanded

$$\sigma(Z) = Z^t + \sigma_1 Z^{t-1} + \cdots + \sigma_{t-1} Z + \sigma_t,$$

The coefficients σ_i are the elementary symmetric functions in the error locations $z_1, \ldots, z_t$.

$$\sigma_i = (-1)^i \sum_{1 \le j_1 < j_2 < \cdots < j_i \le t} z_{j_1} z_{j_2} \ldots z_{j_i},\ 1 \le i \le t,$$

The generalized Newton identities

$$s_i + \sigma_1 s_{i-1} + \cdots + \sigma_t s_{i-t} = 0$$

hold for all i.

Suppose that the defining set of the cyclic code contains the $2t$ consecutive elements $1, 2, \ldots, 2t$.

Algorithm by Peterson, Arimoto and Gorenstein-Zierler

$$s_i + \sigma_1 s_{i-1} + \cdots + \sigma_t s_{i-t} = 0, \quad i = t+1, \ldots, 2t.$$

are t linear equations in the variables $\sigma_1, \ldots, \sigma_t$
with the known syndromes $s_1, \ldots, s_{2t}$ as coefficients.

Generalized Newton identities in matrix form:

$$\begin{pmatrix} s_1 & s_2 & \dots & s_t \\ s_2 & s_3 & \dots & s_{t+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_t & s_{t+1} & \dots & s_{2t-1} \end{pmatrix} \begin{pmatrix} \sigma_t \\ \sigma_{t-1} \\ \vdots \\ \sigma_1 \end{pmatrix} + \begin{pmatrix} s_{t+1} \\ s_{t+2} \\ \vdots \\ s_{2t} \end{pmatrix} = 0$$

$s_1, s_2, \dots, s_{2t}$ are known.
$\sigma_1, \sigma_2, \dots, \sigma_t$ are variables.

Gaussian elimination solves this system of linear 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
and are basically equivalent,
but they decode up to the BCH error-correcting capacity,
which is often strictly smaller than the true capacity.

They do not correct up to the true error-correcting capacity.

Gröbner bases techniques were addressed to remedy this problem.

These methods can be divided into the following categories:

- Unknown syndromes by Berlekamp, Tzeng-Hartmann-Chien and Augot-Charpin-Sendrier
- Power sums by Cooper and Chen-Reed-Helleseth-Truong, Orsini-Sala

Our method is a generalization of the first one.

Generalized Newton identities with unknown syndromes

$$s_i + \sigma_1 s_{i-1} + \cdots + \sigma_t s_{i-t} = 0, \quad i = 1, \ldots, n.$$

$\sigma_1, \sigma_2, \ldots, \sigma_t$ are variables,
s_i are known for i in the complete defining set,
and the remaining s_i are unknown,
these are treated as variables.

It is a set of n quadratic equations in $k + t$ variables.

The theory of Gröbner basis is about
solving systems of polynomial equations in several variables
with coefficients in a field.

It is as a common generalization of

- Linear Algebra,
  linear systems of equations in several variables,
- Euclidean Algorithm,
  polynomial equations of arbitrary degree in one variable.

The polynomial equations are linearized by treating the monomials as new variables. 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.
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. applied to algorithm F5 of Faugère.

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

The (unknown) syndrome of a word $\mathbf{e}$ with respect to B
is the column vector $\mathbf{u}(\mathbf{e}) = \mathbf{u}(B, \mathbf{e}) = B\mathbf{e}^T$.
with entries $u_i(\mathbf{e}) = u_i(B, \mathbf{e}) = \mathbf{b}_i \cdot \mathbf{e}$ 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:

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

The coordinatewise star product of $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ by

$$\mathbf{x} * \mathbf{y} = (x_1 y_1, \ldots, x_n y_n).$$

Then $\mathbf{b}_i * \mathbf{b}_j$ is a linear combination of the basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$.
There are structure constants $\mu_{ijl} \in \mathbb{F}_q$ such that

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

$\mathcal{U}(\mathbf{e})$ is the $n \times n$ matrix of (unknown) syndromes of a word $\mathbf{e}$ with entries

$$u_{ij}(\mathbf{e}) = (\mathbf{b}_i * \mathbf{b}_j) \cdot \mathbf{e}.$$

The entries of $\mathcal{U}(\mathbf{e})$ and $\mathbf{u}(\mathbf{e})$ are related by

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

Lemma

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

Let B_r be the $r \times n$ sub matrix of B with $\mathbf{b}_1, \ldots, \mathbf{b}_r$ as rows.

$\mathbf{b}_1, \ldots, \mathbf{b}_n$ is called an MDS basis and B an MDS matrix
if all the $t \times t$ sub matrices 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.

Proposition
B is an MDS matrix if and only if C_t is an [n,n-t,t+1] code for all t.

MDS bases are known to exist if $n \leq q$.

Let $\mathbf{x} = (x_1, \ldots, x_n)$ be n mutually distinct elements in $\mathbb{F}_q$.
Define

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

Then $\mathbf{b}_1, \ldots, \mathbf{b}_n$ with matrix $B(\mathbf{x})$ are MDS and
are called a Vandermonde basis and matrix, resp.

If $\alpha \in \mathbb{F}_q^*$ is an element of order n and $x_j = \alpha^{j-1}$,
then we get a Reed-Solomon (RS) basis and matrix with

$$b_i * b_j = b_{i+j-1} \text{ and } u_{ij}(\mathbf{e}) = u_{i+j-1}(\mathbf{e}).$$

Proposition

Suppose that B is an MDS matrix.

Let $\mathcal{U}_{u,v}(\mathbf{e})$ be the $u \times v$ sub matrix of $\mathcal{U}(\mathbf{e})$ consisting of the first u rows and v columns.

Then

$$\text{rank}(\mathcal{U}_{nv}(\mathbf{e})) = \begin{cases} v & \text{if } v \leq \text{wt}(\mathbf{e}), \\ \text{wt}(\mathbf{e}) & \text{if } v > \text{wt}(\mathbf{e}). \end{cases}$$

Let C be an $\mathbb{F}_q$-linear code of
length n, dimension k, minimum distance d,
and redundancy $r = n - k$.

Choose a parity check matrix H of C.
Let $\mathbf{h}_1, \ldots, \mathbf{h}_r$ be the rows of H.
There are constants $a_{ij} \in \mathbb{F}_q$ such that

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

Let A be the $r \times n$ matrix with entries a_{ij}. Then $H = AB$.

Let $\mathbf{y} = \mathbf{c} + \mathbf{e}$ be a received word
with $\mathbf{c} \in C$ a code word and $\mathbf{e}$ an error vector.

The syndromes of $\mathbf{y}$ and $\mathbf{e}$ with respect to H are equal and known

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

Expressed in the unknown syndromes of $\mathbf{e}$ with respect to B:

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

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

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

It consists of $r = n - k$ independent linear equations in n variables.

Let

$$U_{ij} = \sum_{l=1}^{n} \mu_{ijl} U_l$$

The system $E(t)$ in the variables $U_1, \ldots, U_n$ and $V_1, \ldots, V_t$:

$$\sum_{j=1}^{t} U_{ij} V_j \;=\; U_{it+1} \;\text{ for }\; i = 1, \ldots, n.$$

It consists of n quadratic equations in $n + t$ variables.

The system of equations $E(t, \mathbf{y})$ 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
used to eliminate $n - k$ variables.

Thus we get a system of n quadratic equations in $k + t$ variables.

Linear equations

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

Quadratic equations in matrix form with B Reed-Solomon

$$\begin{pmatrix} U_1 & U_2 & \ldots & U_t \\ U_2 & U_3 & \ldots & U_{t+1} \\ \vdots & \vdots & \ddots & \vdots \\ U_t & U_{t+1} & \ldots & U_{2t-1} \\ U_{t+1} & U_{t+2} & \ldots & U_{2t} \\ \vdots & \vdots & \ddots & \vdots \\ U_n & U_1 & \ldots & U_t \end{pmatrix} \begin{pmatrix} V_1 \\ V_2 \\ \vdots \\ V_t \end{pmatrix} = \begin{pmatrix} U_{t+1} \\ U_{t+2} \\ \vdots \\ U_{2t} \\ U_{2t+1} \\ \vdots \\ U_{t-1} \end{pmatrix}$$

Special case of cyclic code with defining set $\{1, 2, \ldots, 2t\}$

$$U_j = s_j(\mathbf{y}) \text{ for } j = 1, \ldots, 2t.$$

Quadratic equations in matrix form with B Reed-Solomon

$$\begin{pmatrix} s_1 & s_2 & \ldots & s_t \\ s_2 & s_3 & \ldots & s_{t+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_t & s_{t+1} & \ldots & s_{2t-1} \\ s_{t+1} & s_{t+2} & \ldots & s_{2t} \\ s_{t+2} & s_{t+3} & \ldots & U_{2t+1} \\ \vdots & \vdots & \ddots & \vdots \\ U_n & s_1 & \ldots & s_t \end{pmatrix} \begin{pmatrix} V_1 \\ V_2 \\ \vdots \\ V_t \end{pmatrix} = \begin{pmatrix} s_{t+1} \\ s_{t+2} \\ \vdots \\ s_{2t} \\ U_{2t+1} \\ U_{2t+2} \\ \vdots \\ s_{t-1} \end{pmatrix}$$

Theorem

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 $(d-1)/2$.

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 $\mathrm{wt}(\mathbf{e}) = t$ and the solution is unique satisfying $\mathbf{u} = \mathbf{u}(\mathbf{e})$.

Let $J(t, \mathbf{y})$ be the ideal generated by $E(t, \mathbf{y})$.

Let $0 < \mathrm{wt}(\mathbf{e}) \leq (d-1)/2$ and
and let $(\mathbf{u}, \mathbf{v})$ be the unique solution of $E(t, \mathbf{y})$.

Then $J(t, \mathbf{y})$ has multiplicity one and

the Gröbner basis of $J(t, \mathbf{y})$ is

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

Experiments were done on an
AMD Opteron Processor 242 (1.6MHz), 8GB RAM under Linux.

The computations of Gröbner bases were realized in SINGULAR 3-0-1.

Download the SINGULAR library Err.lib to experiment.

Also MAGMA was used.

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

no. of err.	[120,40]		[120,30]		[120,20]		[120,10]		[150,10]	
2	1	1	1	1	1	1	1	1	1	1
3	22	7	1	1	1	1	1	1	1	1
4	172	64	5	14	1	1	1	1	1	1
5	804	228	31	36	1	1	1	1	1	1
6	-	-	98	63	3	9	1	1	2	1
7	-	-	471	144	7	15	1	1	2	1
8	-	-	-	-	17	25	1	1	2	1
9	-	-	-	-	43	38	1	1	2	1
10	-	-	-	-	109	51	1	1	2	1
11	-	-	-	-	392	84	1	1	3	1
12	-	-	-	-	-	630	2	8	3	1
13	-	-	-	-	-	-	2	9	4	1
14	-	-	-	-	-	-	3	11	4	1
15	-	-	-	-	-	-	7	13	5	20
16	-	-	-	-	-	-	10	16	5	22
17	-	-	-	-	-	-	22	19	8	26
18	-	-	-	-	-	-	38	23	8	30

Conclusion

- Our method is a generalization of the decoding of cyclic codes.
- Complexity of decoding with quadratic equations depends very much on how well the MDS matrix B matches the code C.
- Over-determined system of n quadratic equations in $k + t$ variables.
- The complexity is $O(n^3)$ for a random code and $n \geq (k + 1)(t + 1)$.
- Future research: semi-regular sequences and Faugère F5.
- Gröbner bases theory $\rightleftarrows$ Coding theory.