Decoding and finding the minimum distance with Gröbner bases

Stanislav Bulygin

S3CM: Soria Summer School on Computational Mathematics
"Algebraic Coding Theory"

July 4, 2008

Outline

Outline of the lecture

- Intoruction
- Cooper's philosophy and its development.
- Newton identities based method.
- Decoding affine variety codes.
- Open problems.

Introduction

Notation

Let C be a linear $[n, k, d]$ code over the finite field $\mathbb{F}_q$ with q elements. Here n is length, k is dimension, and d is minimum distance of the code C.

Decoding problem

- *Complete decoding*: Given $\mathbf{y} \in \mathbb{F}_q^n$ and a code $C \subseteq \mathbb{F}_q^n$, so that $\mathbf{y}$ is at distance $d(\mathbf{y}, C)$ from the code, find $\mathbf{c} \in C : d(\mathbf{y}, \mathbf{c}) = d(\mathbf{y}, C)$.
- *Bounded up to half the minimum distance*: Additional assumption $d(\mathbf{y}, C) \leq (d(C) - 1)/2$. Then a codeword with the above property is unique.

Introduction

Notation

Let C be a linear $[n, k, d]$ code over the finite field $\mathbb{F}_q$ with q elements. Here n is length, k is dimension, and d is minimum distance of the code C.

Decoding problem

- *Complete decoding*: Given $\mathbf{y} \in \mathbb{F}_q^n$ and a code $C \subseteq \mathbb{F}_q^n$, so that $\mathbf{y}$ is at distance $d(\mathbf{y}, C)$ from the code, find $\mathbf{c} \in C : d(\mathbf{y}, \mathbf{c}) = d(\mathbf{y}, C)$.
- *Bounded up to half the minimum distance*: Additional assumption $d(\mathbf{y}, C) \leq (d(C) - 1)/2$. Then a codeword with the above property is unique.

Introduction

Decoding via systems solving

One distinguishes between two concepts:

- *Generic decoding*: Solve some system $S(C)$ and obtain some "closed" formulas F. Evaluating these formulas at data specific to a received word $\mathbf{y}$ should yield a solution to the decoding problem. For example for $f \in F : f(syndrome(\mathbf{y}), x) = poly(x)$. The roots of $poly(x) = 0$ yield error positions – general error-locator polynomial f.
- *Online decoding*: Solve some system $S(C, \mathbf{y})$. The solutions should solve the decoding problem.

Computational effort

- Generic decoding. Preprocessing: very hard. Decoding: relatively simple (if the formulas are sparse!).
- Online decoding. Preprocessing: – . Decoding: hard.

Introduction

Decoding via systems solving

One distinguishes between two concepts:

- *Generic decoding*: Solve some system $S(C)$ and obtain some "closed" formulas F. Evaluating these formulas at data specific to a received word $\mathbf{y}$ should yield a solution to the decoding problem. For example for $f \in F : f(syndrome(\mathbf{y}), x) = poly(x)$. The roots of $poly(x) = 0$ yield error positions – general error-locator polynomial f.
- *Online decoding*: Solve some system $S(C, \mathbf{y})$. The solutions should solve the decoding problem.

Computational effort

- Generic decoding. Preprocessing: very hard. Decoding: relatively simple (if the formulas are sparse!).
- Online decoding. Preprocessing: – . Decoding: hard.

Cooper's philosophy and its development

Computing syndromes in cyclic code case

Let C be an $[n, k]$ cyclic code over $\mathbb{F}_q$; $\mathbb{F}$ is a splitting field with a being a primitive n-th root of unity. Let $S_C = \{i_1, \ldots, i_{n-k}\}$ be the complete defining set of C. Let $\mathbf{r} = \mathbf{c} + \mathbf{e}$ be a received word with $\mathbf{c} \in C$ and $\mathbf{e}$ an error vector. Denote the corresponding polynomials in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ by $r(x)$, $c(x)$ and $e(x)$, resp. Compute syndromes

$$s_{i_m} = r(a^{i_m}) = e(a^{i_m}) = \sum_{l=1}^{t} e_{j_l}(a^{i_m})^{j_l}, \quad 1 \leq m \leq n-k,$$

where t is the number of errors, $\{j_1, \ldots, j_t\}$ are the *error-positions* and $e_{j_1}, \ldots, e_{j_t}$ are the *error values*

Rewrite

Define $z_l = a^{j_l}$ and $y_l = e_{j_l}$. Then $z_1, \ldots, z_t$ are the error locations and $y_1, \ldots, y_t$ are the error values and the syndromes above become *generalized power sum functions* $s_{i_m} = \sum_{l=1}^{t} y_l z_l^{i_m}, \quad 1 \leq m \leq n-k.$

Cooper's philosophy and its development

Computing syndromes in cyclic code case

Let C be an $[n, k]$ cyclic code over $\mathbb{F}_q$; $\mathbb{F}$ is a splitting field with a being a primitive n-th root of unity. Let $S_C = \{i_1, \ldots, i_{n-k}\}$ be the complete defining set of C. Let $\mathbf{r} = \mathbf{c} + \mathbf{e}$ be a received word with $\mathbf{c} \in C$ and $\mathbf{e}$ an error vector. Denote the corresponding polynomials in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ by $r(x)$, $c(x)$ and $e(x)$, resp. Compute syndromes

$$s_{i_m} = r(a^{i_m}) = e(a^{i_m}) = \sum_{l=1}^{t} e_{j_l}(a^{i_m})^{j_l}, \quad 1 \leq m \leq n-k,$$

where t is the number of errors, $\{j_1, \ldots, j_t\}$ are the *error-positions* and $e_{j_1}, \ldots, e_{j_t}$ are the *error values*

Rewrite

Define $z_l = a^{j_l}$ and $y_l = e_{j_l}$. Then $z_1, \ldots, z_t$ are the error locations and $y_1, \ldots, y_t$ are the error values and the syndromes above become *generalized power sum functions* $s_{i_m} = \sum_{l=1}^{t} y_l z_l^{i_m}, \quad 1 \leq m \leq n-k$.

Cooper's philosophy and its development

Composing the syndrome ideal

Replace the values on the previous slide by variables and add some natural restrictions. Introduce

- $f_u := \sum_{l=1}^{e} Y_l Z_l^{i_u} - X_u = 0, 1 \leq u \leq n-k$;
- $\epsilon_j := X_j^{q^m} - X_j = 0, 1 \leq j \leq n-k$, since $s_j \in \mathbb{F}$;
- $\eta_i := Z_i^{n+1} - Z_i = 0, 1 \leq i \leq e$, since a^{j_i} are either n-th roots of unity or zero;
- $\lambda_i := Y_i^{q-1} - 1 = 0, 1 \leq i \leq e$, since $y_l \in \mathbb{F}_q \setminus \{0\}$.

We obtain the following set of polynomials in the variables $X = (X_1, \ldots, X_{n-k})$, $Z = (Z_1, \ldots, Z_e)$ and $Y = (Y_1, \ldots, Y_e)$:

$$F_C = \{f_j, \epsilon_j, \eta_i, \lambda_i : 1 \leq j \leq n-k, 1 \leq i \leq e\} \subset \mathbb{F}_q[X, Z, Y].$$

The zero-dimensional ideal I_C generated by F_C is the *CRHT-syndrome ideal* associated to the code C, and the variety $V(F_C)$ defined by F_C is the *CRHT-syndrome variety*, after Chen, Reed, Helleseth and Truong.

Cooper's philosophy and its development

General error-locator polynomial

Adding some more polynomials to F_C, thus obtaining some F'_C, it is possible to prove the following: Every cyclic code C possesses a *general error-locator polynomial* L_C from $\mathbb{F}_q[X_1, \ldots, X_{n-k}, Z]$ that satisfies the following two properties:

- $L_C = Z^e + a_{t-1}Z^{e-1} + \cdots + a_0$ with $a_j \in \mathbb{F}_q[X_1, \ldots, X_{n-k}]$, $0 \leq j \leq e-1$, where e is the error-correcting capacity;
- given a syndrome $\mathbf{s} = (s_1, \ldots, s_{n-k}) \in \mathbb{F}^{n-k}$ corresponding to an error of weight $t \leq e$ and error locations $\{k_1, \ldots, k_t\}$, if we evaluate the $X_i = s_i$ for all $1 \leq i \leq n-k$, then the roots of $L_C(\mathbf{s}, Z)$ are exactly $a^{k_1}, \ldots, a^{k_t}$ and 0 of multiplicity $e-t$, in other words $L_C(\mathbf{s}, Z) = Z^{e-t}\prod_{i=1}^{t}(Z - a^{k_i})$.

Decoding

The general error-locator polynomial actually is an element of the reduced Gröbner basis of $\langle F'_C \rangle$. Having this polynomial, decoding of the cyclic code C reduces to univariate factorization.

Cooper's philosophy and its development

General error-locator polynomial

Adding some more polynomials to F_C, thus obtaining some F'_C, it is possible to prove the following: Every cyclic code C possesses a *general error-locator polynomial* L_C from $\mathbb{F}_q[X_1, \ldots, X_{n-k}, Z]$ that satisfies the following two properties:

- $L_C = Z^e + a_{t-1}Z^{e-1} + \cdots + a_0$ with $a_j \in \mathbb{F}_q[X_1, \ldots, X_{n-k}]$, $0 \leq j \leq e-1$, where e is the error-correcting capacity;
- given a syndrome $\mathbf{s} = (s_1, \ldots, s_{n-k}) \in \mathbb{F}^{n-k}$ corresponding to an error of weight $t \leq e$ and error locations $\{k_1, \ldots, k_t\}$, if we evaluate the $X_i = s_i$ for all $1 \leq i \leq n-k$, then the roots of $L_C(\mathbf{s}, Z)$ are exactly $a^{k_1}, \ldots, a^{k_t}$ and 0 of multiplicity $e-t$, in other words $L_C(\mathbf{s}, Z) = Z^{e-t}\prod_{i=1}^{t}(Z - a^{k_i})$.

Decoding

The general error-locator polynomial actually is an element of the reduced Gröbner basis of $\langle F'_C \rangle$. Having this polynomial, decoding of the cyclic code C reduces to univariate factorization.

Cooper's philosophy and its development

Finding minimum distance

The method described can be adapted to find minimum distance of a code. Namely, the following holds: Let C be a binary $[n, k, d]$ cyclic code with a defining set $S_C = \{i_1, \ldots, i_v\}$. Let $1 \leq w \leq n$ and let $J_C(w)$ denote the system:

$$\begin{cases} Z_1^{i_1} + \cdots + Z_w^{i_1} = 0, \\ \vdots \\ Z_1^{i_v} + \cdots + Z_w^{i_v} = 0, \\ Z_1^n - 1 = 0, \\ \vdots \\ Z_w^n - 1 = 0 \\ p(n, Z_i, Z_j) = 0, 1 \leq i < j \leq w \end{cases}$$

Then the number of solutions of $J_C(w)$ is equal to $w!$ times the number of codewords of weight w. And for $1 \leq w \leq d$: either $J_C(w)$ has no solutions, which is equivalent to $w < d$, or $J_C(w)$ has some solutions, which is equivalent to $w = d$.

Newton identities based method

Error-locator polynomial

The *error-locator polynomial* is defined by

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

If this product is expanded

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

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

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

Newton identities based method

Generalized Newton identities

The syndromes $s_i = r(a^i) = e(a^i)$ and the coefficients σ_i satisfy the following *generalized Newton identities*:

$$s_i + \sum_{j=1}^{t} \sigma_j s_{i-j} = 0, \quad \text{for all} \quad i \in \mathbb{Z}_n.$$

Decoding up to BCH bound

Suppose that S_C contains the $2t$ consecutive elements $b, \ldots, b+2t-1$ for some b. Then $d \geq 2t+1$ by the *BCH bound*. Furthermore the set of equations above for $i = b+t, \ldots, b+2t-1$ is a system of t linear equations in the unknowns $\sigma_1, \ldots, \sigma_t$ with the known syndromes $s_b, \ldots, s_{b+2t-1}$ as coefficients. Gaussian elimination solves the system of equations with complexity $\mathcal{O}(t^3)$. In this way we have obtained the *APGZ decoding* algorithm, after Arimoto, Peterson, Gorenstein and Zierler.

Newton identities based method

Generalized Newton identities

The syndromes $s_i = r(a^i) = e(a^i)$ and the coefficients σ_i satisfy the following *generalized Newton identities*:

$$s_i + \sum_{j=1}^{t} \sigma_j s_{i-j} = 0, \quad \text{for all} \quad i \in \mathbb{Z}_n.$$

Decoding up to BCH bound

Suppose that S_C contains the $2t$ consecutive elements $b, \ldots, b+2t-1$ for some b. Then $d \geq 2t+1$ by the *BCH bound*. Furthermore the set of equations above for $i = b+t, \ldots, b+2t-1$ is a system of t linear equations in the unknowns $\sigma_1, \ldots, \sigma_t$ with the known syndromes $s_b, \ldots, s_{b+2t-1}$ as coefficients. Gaussian elimination solves the system of equations with complexity $\mathcal{O}(t^3)$. In this way we have obtained the *APGZ decoding* algorithm, after Arimoto, Peterson, Gorenstein and Zierler.

Newton identities based method

Decoding up to error-correcting capacity

We have $s_{i+n} = s_i$, for all $i \in \mathbb{Z}_n$, since $s_{i+n} = r(a^{i+n}) = r(a^i)$. Furthermore $s_i^q = (e(a^i))^q = e(a^{iq}) = s_{qi}$, for all $i \in \mathbb{Z}_n$, and $\sigma_i^{q^m} = \sigma_i$, for all $1 \leq i \leq t$. Replace the syndromes by variables and obtain following set of polynomials $Newton_t$ in the variables $S_1, \ldots, S_n$ and $\sigma_1, \ldots, \sigma_t$:

$$Newton_t \begin{cases} \sigma_i^{q^m} - \sigma_i, & \text{for all } 1 \leq i \leq t, \\ S_{i+n} - S_i, & \text{for all } i \in \mathbb{Z}_n, \\ S_i^q - S_{qi}, & \text{for all } i \in \mathbb{Z}_n, \\ S_i + \sum_{j=1}^{t} \sigma_j S_{i-j}, & \text{for all } i \in \mathbb{Z}_n, \\ S_i - s_i(\mathbf{r}) & \text{for all } i \in S_C. \end{cases}$$

Decoding affine variety codes

Affine codes

Let $I = \langle g_1, \ldots, g_m \rangle \subseteq \mathbb{F}_q[X_1, \ldots, X_s]$ be an ideal. Define $I_q := I + \langle X_1^q - X_1, \ldots, X_s^q - X_s \rangle$. So I_q is a 0-dimensional ideal. Define also $V(I_q) =: \{P_1, \ldots, P_n\}$. Every q-ary linear code C with parameters $[n, k]$ can be seen as an *affine variety code* $C(I, L)$, that is the image of a vector space L of the *evaluation map*

$$\begin{cases} \phi : R \to \mathbb{F}_q^n \\ \bar{f} \mapsto (f(P_1), \ldots, f(P_n)), \end{cases}$$

where $R := \mathbb{F}_q[U_1, \ldots, U_s]/I_q$, L is a vector subspace of R and $\bar{f}$ the coset of f in $\mathbb{F}_q[U_1, \ldots, U_s]$ modulo I_q.

Decoding affine variety codes

Every linear code is an affine one

Given a q-ary $[n, k]$ code C with a generator matrix $G = (g_{ij})$:

1. choose s, such that $q^s \geq n$, and construct s distinct points $P_1, \ldots, P_s$ in $\mathbb{F}_q^s$.
2. Construct a Gröbner basis $\{g_1, \ldots, g_m\}$ for an ideal I of polynomials from $\mathbb{F}_q[X_1, \ldots, X_s]$ that vanish at the points $P_1, \ldots, P_s$. Denote by $\xi_i \in \mathbb{F}_q[X_1, \ldots, X_s]$ such $\xi_i(P_i) = 1, \xi_i(P_j) = 0, i \neq j$.
3. Then $f_i = \sum_{i=1}^{n} g_{ij}\xi_j$ span the space L, so that $g_{ij} = f_i(P_j)$.

In this way we obtain that the code C is an image of the evaluation above, so $C = C(I, L)$. In the same way by considering a parity check matrix instead of a generator matrix we have that the dual code is also an affine variety code.

Decoding affine variety codes

Setup

The method of decoding is a generalization of CRHT. One needs to add polynomials $(g_l(X_{k1}, \ldots, X_{ks}))_{l=1,\ldots,m;k=1,\ldots,t}$ for every error position. We also assume that field equations on X_{ij}'s are included among the polynomials above. Let C be a q-ary $[n, k]$ linear code such that its dual is written as an affine variety code of the form $C^{\perp} = C(I, L)$. Let $\mathbf{r} = \mathbf{c} + \mathbf{e}$ as usual and $t \leq e$. Then the syndromes are computed by $s_i = \sum_{j=1}^{n} r_j f_i(P_j) = \sum_{j=1}^{n} e_j f_i(P_j)$ for $i = 1, \ldots, n-k$.

Decoding affine codes

Consider the ring $\mathbb{F}_q[X_{11}, \ldots, X_{1s}, \ldots, X_{t1}, \ldots, X_{ts}, E_1, \ldots, E_t]$, where $(X_{i1}, \ldots, X_{is})$ correspond to the i-th error position and E_i to the i-th error value. Consider the ideal $\mathcal{I}_C$ generated by

$$\begin{cases} \sum_{j=1}^{t} E_j f_i(X_{j1}, \ldots, X_{js}) - s_i, 1 \leq i \leq n-k, \\ g_l(X_{j1}, \ldots, X_{js}), 1 \leq l \leq m, \\ E_k^{q-1} - 1. \end{cases}$$

Decoding affine variety codes

Setup

The method of decoding is a generalization of CRHT. One needs to add polynomials $(g_l(X_{k1}, \ldots, X_{ks}))_{l=1,\ldots,m;k=1,\ldots,t}$ for every error position. We also assume that field equations on X_{ij}'s are included among the polynomials above. Let C be a q-ary $[n, k]$ linear code such that its dual is written as an affine variety code of the form $C^{\perp} = C(I, L)$. Let $\mathbf{r} = \mathbf{c} + \mathbf{e}$ as usual and $t \leq e$. Then the syndromes are computed by $s_i = \sum_{j=1}^{n} r_j f_i(P_j) = \sum_{j=1}^{n} e_j f_i(P_j)$ for $i = 1, \ldots, n-k$.

Decoding affine codes

Consider the ring $\mathbb{F}_q[X_{11}, \ldots, X_{1s}, \ldots, X_{t1}, \ldots, X_{ts}, E_1, \ldots, E_t]$, where $(X_{i1}, \ldots, X_{is})$ correspond to the i-th error position and E_i to the i-th error value. Consider the ideal $\mathcal{I}_C$ generated by

$$\begin{cases} \sum_{j=1}^{t} E_j f_i(X_{j1}, \ldots, X_{js}) - s_i, 1 \leq i \leq n-k, \\ g_l(X_{j1}, \ldots, X_{js}), 1 \leq l \leq m, \\ E_k^{q-1} - 1. \end{cases}$$

Decoding affine variety codes

Elimination order

Let S be some subset of variables in X. A monomial order $>$ on $\mathbb{F}[X]$ is called an *elimination order* with respect to S if for all $f \in \mathbb{F}[X]$ from the fact that $\mathrm{lm}(f) \in \mathbb{F}[X \setminus S]$ follows that $f \in \mathbb{F}[X \setminus S]$. Lexicographic order is an elimination order w.r.t to any set of variables.

Theorem

Let G be the reduced Gröbner basis for $\mathcal{I}_C$ with respect to an elimination order w.r.t $X_{11}, \ldots, X_{1s}, E_1$, such that $X_{11} < \cdots < X_{1s} < E_1$. Then we may solve for the error locations and values by applying elimination theory to the polynomials in G.

Decoding affine variety codes

Elimination order

Let S be some subset of variables in X. A monomial order $>$ on $\mathbb{F}[X]$ is called an *elimination order* with respect to S if for all $f \in \mathbb{F}[X]$ from the fact that $\mathrm{lm}(f) \in \mathbb{F}[X \setminus S]$ follows that $f \in \mathbb{F}[X \setminus S]$. Lexicographic order is an elimination order w.r.t to any set of variables.

Theorem

Let G be the reduced Gröbner basis for $\mathcal{I}_C$ with respect to an elimination order w.r.t $X_{11}, \ldots, X_{1s}, E_1$, such that $X_{11} < \cdots < X_{1s} < E_1$. Then we may solve for the error locations and values by applying elimination theory to the polynomials in G.

Open questions

Open questions

- Existence of general error-locator polynomial for arbitrary linear codes.
- Complexity estimates of GB-based methods.
- The methods considered are quite "heavy weight", thus one needs to reduce complexity.
- Develop the method of generalized Newton identities for arbitrary linear codes.
- Alternative schemes?

The End

That's it! Questions? Remarks?