Algebraic Geometry Codes

Shelly Manber

December 2, 2011

References

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Main Source: Stichtenoth, Henning. *"Algebraic Function Fields and Codes".* Springer, 2009.

Other Sources:

- Høholdt, Lint and Pellikaan. *"Algebraic geometry codes."* Handbook of Coding Theory, vol 1, p 871-961, Amsterdam, 2011.
- Bartley and Walker. *"Algebraic Geometric Codes over Rings."* World Scientific Review, June 2008.
- Guruswami,Venkatesan. *"Notes 2: Gilbert-Varshamov bound."* Jan 2010.

Error Correcting Codes

Algebraic Geometry Codes

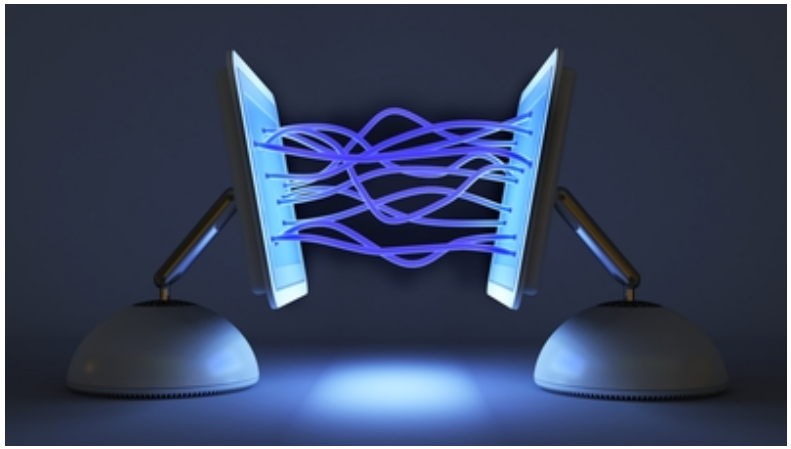
Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding



Error Correcting Codes

Algebraic Geometry Codes

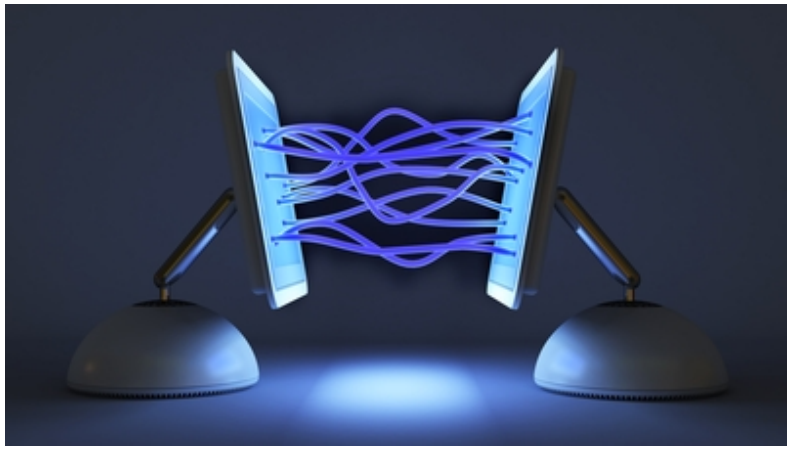
Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding



- Natural way of sending information is a stream of bits: 011100010100100011...

Error Correcting Codes

Algebraic Geometry Codes

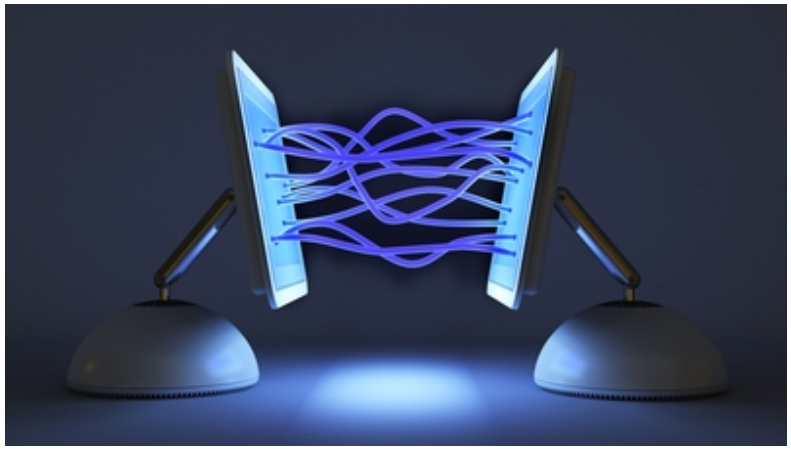
Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding



- Natural way of sending information is a stream of bits: 01110001010010011...
- If one bit is off, the entire message may be 100% different

Error Correcting Codes

Algebraic Geometry Codes

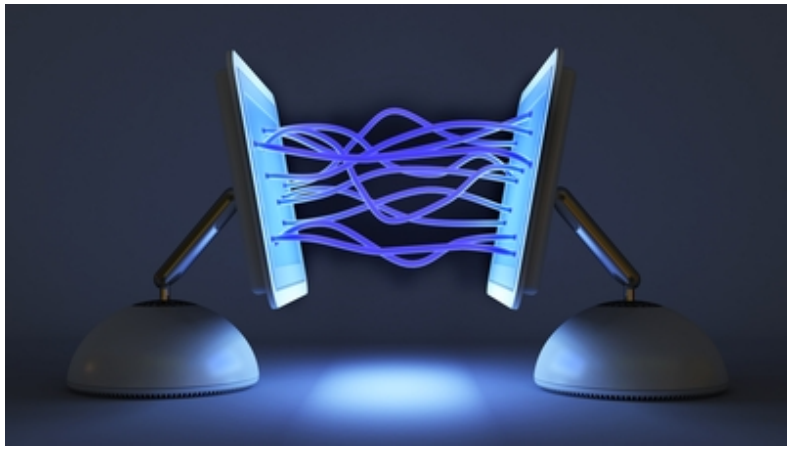
Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding



- Natural way of sending information is a stream of bits: 01110001010010011...
- If one bit is off, the entire message may be 100% different
- Error Correcting Codes: a way to send information along a noisy channel so that the original message can be recovered with high probability

Definitions

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Definition: A *linear code* C is a linear subpace of $\mathbb{F}_q^n$.

Definitions

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Definition: A *linear code* C is a linear subpace of $\mathbb{F}_q^n$.

Definition: The *dimension* k of a linear code is its dimension as a vector space

Definitions

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Definition: A *linear code* C is a linear subpace of $\mathbb{F}_q^n$.

Definition: The *dimension* k of a linear code is its dimension as a vector space

Definition: The Hamming distance between two elements of $\mathbb{F}_q^n$ is the number of coefficients on which the two elements differ. The weight of an element, $wt(e)$, is the number of nonzero coefficients.

Definitions

Definition: A *linear code* C is a linear subpace of $\mathbb{F}_q^n$.

Definition: The *dimension* k of a linear code is its dimension as a vector space

Definition: The Hamming distance between two elements of $\mathbb{F}_q^n$ is the number of coefficients on which the two elements differ. The weight of an element, $wt(e)$, is the number of nonzero coefficients.

Definition: The *minimum distance* of a code is the minimum Hamming distance between any two elements of the linear code (equivalently the minimum weight of a codeword)

Encoding

- An *encoding* is a map from a message into the code C

Encoding

- An *encoding* is a map from a message into the code C
- A *generator matrix* is a $k \times n$ matrix whose rows are a basis for C

Encoding

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

- An *encoding* is a map from a message into the code C
- A *generator matrix* is a $k \times n$ matrix whose rows are a basis for C
- A generator matrix gives an encoding:

$$\begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix} \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ b_1 & b_2 & b_3 & b_4 & b_5 \\ c_1 & c_2 & c_3 & c_4 & c_5 \end{pmatrix}$$

Error Checking

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Definition: The *dual* $C^{\perp}$ of a code C is its dual as a vector space under the canonical inner product.

Error Checking

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Definition: The *dual* $C^{\perp}$ of a code C is its dual as a vector space under the canonical inner product.

Definition: A *parity check matrix* M for C is an $(n-k) \times n$ matrix whose rows are a basis for $C^{\perp}$

Error Checking

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Definition: The *dual* $C^{\perp}$ of a code C is its dual as a vector space under the canonical inner product.

Definition: A *parity check matrix* M for C is an $(n-k) \times n$ matrix whose rows are a basis for $C^{\perp}$

Claim: A vector $x := (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ is in C if and only if $Mx = 0$.

Error Checking

Definition: The *dual* $C^{\perp}$ of a code C is its dual as a vector space under the canonical inner product.

Definition: A *parity check matrix* M for C is an $(n-k) \times n$ matrix whose rows are a basis for $C^{\perp}$

Claim: A vector $x := (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ is in C if and only if $Mx = 0$.

Proof.

$(C^{\perp})^{\perp} = C$, so

Error Checking

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Definition: The *dual* $C^{\perp}$ of a code C is its dual as a vector space under the canonical inner product.

Definition: A *parity check matrix* M for C is an $(n-k) \times n$ matrix whose rows are a basis for $C^{\perp}$

Claim: A vector $x := (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ is in C if and only if $Mx = 0$.

Proof.

$(C^{\perp})^{\perp} = C$, so

$$x \in C \Leftrightarrow \langle x, c \rangle = 0 \, \forall c \in C^{\perp}$$

Error Checking

Definition: The *dual* $C^{\perp}$ of a code C is its dual as a vector space under the canonical inner product.

Definition: A *parity check matrix* M for C is an $(n-k) \times n$ matrix whose rows are a basis for $C^{\perp}$

Claim: A vector $x := (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ is in C if and only if $Mx = 0$.

Proof.

$(C^{\perp})^{\perp} = C$, so

$$x \in C \Leftrightarrow \langle x, c \rangle = 0 \, \forall c \in C^{\perp} \Leftrightarrow Mx = 0$$

□

Decoding

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Let C be an $[n, k, d]$ code. If $x \in \mathbb{F}_q^n$ has Hamming distance $\leq (d-1)/2$ from a codeword $c \in C$ then c is the *unique* codeword with minimal distance to x.

Decoding

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Let C be an $[n, k, d]$ code. If $x \in \mathbb{F}_q^n$ has Hamming distance $\leq (d-1)/2$ from a codeword $c \in C$ then c is the *unique* codeword with minimal distance to x.

Definition: A *decoding* is an algorithm, given $a \in \mathbb{F}_q^n$ and the guarantee that $a = c + e$ for some $c \in C$ and $e \in \mathbb{F}_q^n$ with weight $\leq (d-1)/2$, to recover c.

Bounds

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

To maximize code efficacy:

- Should d be higher or lower with respect to n?

Bounds

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

To maximize code efficacy:

- Should d be higher or lower with respect to n?
- Should k be higher or lower with respect to n?

Bounds

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

To maximize code efficacy:

- Should d be higher or lower with respect to n?
- Should k be higher or lower with respect to n?

Theorem (Singleton Bound): for all linear codes

$$k + d \leq n + 1$$

Bounds

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

To maximize code efficacy:

- Should d be higher or lower with respect to n?
- Should k be higher or lower with respect to n?

Theorem (Singleton Bound): for all linear codes

$$k + d \leq n + 1$$

Proof.

Let

$$V := \{(a_1, ..., a_n) \in \mathbb{F}_q^n \mid a_i = 0 \, \forall i \geq d\}$$

Bounds

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

To maximize code efficacy:

- Should d be higher or lower with respect to n?
- Should k be higher or lower with respect to n?

Theorem (Singleton Bound): for all linear codes

$$k + d \leq n + 1$$

Proof.

Let

$$V := \{(a_1, ..., a_n) \in \mathbb{F}_q^n \mid a_i = 0 \, \forall i \geq d\}$$

So $\dim(V) = d - 1$ and $V \cap C = \emptyset$, so

Bounds

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

To maximize code efficacy:

- Should d be higher or lower with respect to n?
- Should k be higher or lower with respect to n?

Theorem (Singleton Bound): for all linear codes

$$k + d \leq n + 1$$

Proof.

Let

$$V := \{(a_1, ..., a_n) \in \mathbb{F}_q^n \mid a_i = 0 \, \forall i \geq d\}$$

So $\dim(V) = d - 1$ and $V \cap C = \emptyset$, so

$$\begin{aligned} n = \dim(\mathbb{F}_q^n) \geq \dim(V + C) &= \dim(V) + \dim(C) \\ &= (d - 1) + k \end{aligned}$$

Bounds

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

To maximize code efficacy:

- Should d be higher or lower with respect to n?
- Should k be higher or lower with respect to n?

Theorem (Singleton Bound): for all linear codes

$$k + d \leq n + 1$$

Proof.

Let

$$V := \{(a_1, ..., a_n) \in \mathbb{F}_q^n \mid a_i = 0 \, \forall i \geq d\}$$

So $\dim(V) = d - 1$ and $V \cap C = \emptyset$, so

$$\begin{aligned} n = \dim(\mathbb{F}_q^n) \geq \dim(V + C) &= \dim(V) + \dim(C) \\ &= (d - 1) + k \end{aligned}$$

Example: Reed-Solomon Codes

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Let $n = q - 1$ and $\mathbb{F}_q = \{0, 1, \alpha, \ldots, \alpha^{n-1}\}$. Choose $k \leq n$, and define

$$L_k = \{f \in \mathbb{F}_q[X] \mid \deg f \leq k - 1\}$$

Example: Reed-Solomon Codes

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Let $n = q - 1$ and $\mathbb{F}_q = \{0, 1, \alpha, \ldots, \alpha^{n-1}\}$. Choose $k \leq n$, and define

$$L_k = \{f \in \mathbb{F}_q[X] \mid \deg f \leq k - 1\}$$

Define

$$C_{RS} = \{(f(1), f(\alpha), \ldots, f(\alpha^{n-1}) \mid f \in L_k\}$$

Example: Reed-Solomon Codes

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Let $n = q - 1$ and $\mathbb{F}_q = \{0, 1, \alpha, \ldots, \alpha^{n-1}\}$. Choose $k \leq n$, and define

$$L_k = \{f \in \mathbb{F}_q[X] \mid \deg f \leq k - 1\}$$

Define

$$C_{RS} = \{(f(1), f(\alpha), \ldots, f(\alpha^{n-1}) \mid f \in L_k\}$$

Claim: C_{RS} is an $[n, k, n - k + 1]$ code.

Proof.

1. $L_k \to C_{RS}$ is an injective $\mathbb{F}_q$-linear map

Example: Reed-Solomon Codes

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Let $n = q - 1$ and $\mathbb{F}_q = \{0, 1, \alpha, \ldots, \alpha^{n-1}\}$. Choose $k \leq n$, and define

$$L_k = \{f \in \mathbb{F}_q[X] \mid \deg f \leq k - 1\}$$

Define

$$C_{RS} = \{(f(1), f(\alpha), \ldots, f(\alpha^{n-1}) \mid f \in L_k\}$$

Claim: C_{RS} is an $[n, k, n - k + 1]$ code.

Proof.

1. $L_k \to C_{RS}$ is an injective $\mathbb{F}_q$-linear map
2. A polynomial of degree $k - 1$ has at most $k - 1$ zeros, so $d \geq n - k + 1$

Example: Reed-Solomon Codes

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Let $n = q - 1$ and $\mathbb{F}_q = \{0, 1, \alpha, \ldots, \alpha^{n-1}\}$. Choose $k \leq n$, and define

$$L_k = \{f \in \mathbb{F}_q[X] \mid \deg f \leq k - 1\}$$

Define

$$C_{RS} = \{(f(1), f(\alpha), \ldots, f(\alpha^{n-1}) \mid f \in L_k\}$$

Claim: C_{RS} is an $[n, k, n - k + 1]$ code.

Proof.

1. $L_k \to C_{RS}$ is an injective $\mathbb{F}_q$-linear map
2. A polynomial of degree $k - 1$ has at most $k - 1$ zeros, so $d \geq n - k + 1$
3. By the Singleton bound, $d \leq n - k + 1$

Definition

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Given:

- X a curve of genus g over $\mathbb{F}_q$ with function field F

Definition

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Given:

- X a curve of genus g over $\mathbb{F}_q$ with function field F
- $P_1, \ldots, P_n$ distinct places of F of degree one

Definition

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Given:

- X a curve of genus g over $\mathbb{F}_q$ with function field F
- $P_1, \ldots, P_n$ distinct places of F of degree one
- $D := P_1 + \cdots + P_n$ a divisor of X

Definition

Given:

- X a curve of genus g over $\mathbb{F}_q$ with function field F
- $P_1, \ldots, P_n$ distinct places of F of degree one
- $D := P_1 + \cdots + P_n$ a divisor of X
- G a divisor of X such that $\operatorname{Supp} G \cap \operatorname{Supp} D = \emptyset$

Define

$$\mathcal{C}_{\mathscr{L}}(D, G) := \{(x(P_1), \ldots, x(P_n)) \mid x \in \mathscr{L}(G)\} \subset \mathbb{F}_q^n$$

Definition

Given:

- X a curve of genus g over $\mathbb{F}_q$ with function field F
- $P_1, \ldots, P_n$ distinct places of F of degree one
- $D := P_1 + \cdots + P_n$ a divisor of X
- G a divisor of X such that $\operatorname{Supp} G \cap \operatorname{Supp} D = \emptyset$

Define

$$\mathcal{C}_{\mathscr{L}}(D, G) := \{(x(P_1), \ldots, x(P_n)) \mid x \in \mathscr{L}(G)\} \subset \mathbb{F}_q^n$$

Claim: $k = \ell(G) - \ell(G - D)$ and $d \geq n - \deg G$.

Some Nice Properties

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

If $\deg G < n$ then

1. $k = \ell(G) \geq \deg(G) + 1 - g$ (Riemann-Roch)

Some Nice Properties

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

If $\deg G < n$ then

1. $k = \ell(G) \geq \deg(G) + 1 - g$ (Riemann-Roch)
2. $\mathscr{L}(G) \to \mathcal{C}_{\mathscr{L}}(D, G)$ is injective

Some Nice Properties

If $\deg G < n$ then

1. $k = \ell(G) \geq \deg(G) + 1 - g$ (Riemann-Roch)
2. $\mathscr{L}(G) \to \mathcal{C}_{\mathscr{L}}(D, G)$ is injective
3. For a basis $\{x_1, \ldots, x_k\}$ of $\mathscr{L}(G)$, the matrix:

$$\begin{pmatrix} x_1(P_1) & x_1(P_2) & \ldots & x_1(P_n) \\ x_2(P_1) & x_2(P_2) & \ldots & x_2(P_n) \\ \ldots & \ldots & \ldots & \ldots \\ x_n(P_1) & x_n(P_2) & \ldots & x_n(P_n) \end{pmatrix}$$

is a generator matrix for $\mathcal{C}_{\mathscr{L}}$.

Bounds

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

If $\deg G < n$ then $k \geq \deg(G) + 1 - g$ and $d \geq n - \deg G$ so

Bounds

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

If $\deg G < n$ then $k \geq \deg(G) + 1 - g$ and $d \geq n - \deg G$ so

$$k + d \geq n + 1 - g$$

Bounds

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

If $\deg G < n$ then $k \geq \deg(G) + 1 - g$ and $d \geq n - \deg G$ so

$$k + d \geq n + 1 - g$$

But recall that

$$k + d \leq n + 1$$

Bounds

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

If $\deg G < n$ then $k \geq \deg(G) + 1 - g$ and $d \geq n - \deg G$ so

$$k + d \geq n + 1 - g$$

But recall that

$$k + d \leq n + 1$$

So for genus 0 curves,

$$k + d = n + 1$$

Bounds

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

If $\deg G < n$ then $k \geq \deg(G) + 1 - g$ and $d \geq n - \deg G$ so

$$k + d \geq n + 1 - g$$

But recall that

$$k + d \leq n + 1$$

So for genus 0 curves,

$$k + d = n + 1$$

Unfortunately, for genus zero curves, $n \leq q + 1$, so over a fixed alphabet, we can't send very large messages.

Bounds

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

If $\deg G < n$ then $k \geq \deg(G) + 1 - g$ and $d \geq n - \deg G$ so

$$k + d \geq n + 1 - g$$

But recall that

$$k + d \leq n + 1$$

So for genus 0 curves,

$$k + d = n + 1$$

Unfortunately, for genus zero curves, $n \leq q + 1$, so over a fixed alphabet, we can't send very large messages.

Goal of coding theory: To construct *asymptotically good curves*

Asymptotically Good Curves

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Definition: For an $[n, k, d]$ code:

$R = k/n$ is called the *information rate*, and

$\delta = d/n$ is called the *relative distance*

Asymptotically Good Curves

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Definition: For an $[n, k, d]$ code:

$$R = k/n \text{ is called the } \textit{information rate}, \text{ and}$$
$$\delta = d/n \text{ is called the } \textit{relative distance}$$

Theorem (Gilbert-Varshamov bound): For any fixed q and $\delta \leq 1 - 1/q$, and an arbitrarily small $\epsilon > 0$ there exists an infinite family of codes with

$$R \geq 1 - h_q(\delta) - \epsilon$$

where $h_q(x)$ is the entropy function:

$$h_q(x) := x log_q(q-1) - x log_q(x) - (1-x) log_q(1-x)$$

Residues of Differentials

Let P be a place of F with local parameter t.

Residues of Differentials

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Let P be a place of F with local parameter t.

Claim: Any $x \in F$ can be written uniquely as $\sum_{i=m}^{\infty} a_i t^i$ with $a_i \in \mathbb{F}_q$ for some integer m.

Residues of Differentials

Let P be a place of F with local parameter t.

Claim: Any $x \in F$ can be written uniquely as $\sum_{i=m}^{\infty} a_i t^i$ with $a_i \in \mathbb{F}_q$ for some integer m.

Definition: For any differential ω of F, write

$$\omega = f\,\mathrm{d}t$$

$$f = \sum_{i=m}^{\infty} a_i t^i$$

Define $res_P(\omega) := a_{-1}$

Residues of Differentials

Let P be a place of F with local parameter t.

Claim: Any $x \in F$ can be written uniquely as $\sum_{i=m}^{\infty} a_i t^i$ with $a_i \in \mathbb{F}_q$ for some integer m.

Definition: For any differential ω of F, write

$$\omega = f\,\mathrm{d}t$$

$$f = \sum_{i=m}^{\infty} a_i t^i$$

Define $res_P(\omega) := a_{-1}$

Claim: Residue is well-defined.

Another Algebraic Geometry Code

Given:

- $P_1, \ldots, P_n$ distinct places of F of degree one
- $D = P_1 + \cdots + P_n$ a divisor of X
- G a divisor of X such that $\operatorname{Supp} G \cap \operatorname{Supp} D = \emptyset$

as before, define

$$\mathcal{C}_\Omega(D, G) := \{(res_{P_1}(\omega), \ldots, res_{P_n}(\omega)) \mid \omega \in \Omega_F(G - D)\}$$

Duals

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Proposition: $C_\Omega(D, G) = C_{\mathscr{L}}(D, G)^\perp$

Duals

Proposition: $C_\Omega(D, G) = C_{\mathscr{L}}(D, G)^\perp$

Proposition: There exists a Weil Differential η which can be explicitly computed such that

$$C_\Omega(D, G)^\perp = C_{\mathscr{L}}(D, G) = C_\Omega(D, D - G + (\eta))$$

Hermitian Codes

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Let

- $F := \mathbb{F}_{q^2}(x, y)$ with $y^q + y = x^{q+1}$

Hermitian Codes

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Let

- $F := \mathbb{F}_{q^2}(x, y)$ with $y^q + y = x^{q+1}$
- $P_{\alpha,\beta}$ be the unique place such that $x(P_{\alpha,\beta}) = \alpha$ and $y(P_{\alpha,\beta}) = \beta$ and P_∞ be the common pole of x and y.

Hermitian Codes

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Let

- $F := \mathbb{F}_{q^2}(x, y)$ with $y^q + y = x^{q+1}$
- $P_{\alpha,\beta}$ be the unique place such that $x(P_{\alpha,\beta}) = \alpha$ and $y(P_{\alpha,\beta}) = \beta$ and P_∞ be the common pole of x and y.
- $D = \sum_{\beta^q+\beta=\alpha^{q+1}} P_{\alpha,\beta}$

For each $0 < r < q^3 + q^2 - q - 2$ define

$$C_r := C_{\mathscr{L}}(D, rP_\infty)$$

Generating Hermitian Codes

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Proposition: For each $r \geq 0$, the elements of the form $x^i y^j$ with

- $0 \leq i$
- $0 \leq j \leq q-1$
- $iq + j(q+1) \leq r$

form a basis for $\mathscr{L}(rP_\infty)$

Generating Hermitian Codes

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Proposition: For each $r \geq 0$, the elements of the form $x^i y^j$ with

- $0 \leq i$
- $0 \leq j \leq q-1$
- $iq + j(q+1) \leq r$

form a basis for $\mathscr{L}(rP_\infty)$

Corollary: The generating matrix for C_r is the matrix whose rows are $(\alpha^i \beta^j)_{\beta^q+\beta=\alpha^{q+1}}$ where i and j satisfy the above conditions.

Bounds

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Let $N(r)$ be the number of pairs i, j satisfying the properties previously mentioned.

Proposition:

$$n = q^3$$

$$k = \dim C_r = \begin{cases} N(r) & 0 \leq r < q^3 \\ n - N(r) & q^3 \leq r \leq q^3 + q^2 - q - 2 \end{cases}$$

$$d \geq n - r$$

Numerical Example: $q = 2$

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Let $\mathbb{F}_4 = \{0, 1, a, a+1\}$, C defined by $y^2z + yz^2 + x^3$, i.e. $F = Frac(\mathbb{F}_q[x, y, z]/(y^2z + yz^2 + x^3))$

Numerical Example: $q = 2$

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Let $\mathbb{F}_4 = \{0, 1, a, a+1\}$, C defined by $y^2z + yz^2 + x^3$, i.e. $F = Frac(\mathbb{F}_q[x, y, z]/(y^2z + yz^2 + x^3))$

Rational points:

$[(0:0:1), (0:1:0), (0:1:1), (1:a:1), (1:a+1:1), (a:a:1), (a:a+1:1), (a+1:a:1), (a+1:a+1:1)]$

Numerical Example: $q = 2$

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Let $\mathbb{F}_4 = \{0, 1, a, a+1\}$, C defined by $y^2z + yz^2 + x^3$, i.e. $F = Frac(\mathbb{F}_q[x, y, z]/(y^2z + yz^2 + x^3))$

Rational points:
$[(0:0:1), (0:1:0), (0:1:1), (1:a:1), (1:a+1:1), (a:a:1), (a:a+1:1), (a+1:a:1), (a+1:a+1:1)]$

Let $r = 5$. Then the basis for $\mathscr{L}(r(0:1:0))$ is

$$\{1, x, y, x^2, xy\}$$

Numerical Example: generating matrix

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Generating matrix for C:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & a & a+1 & a & a+1 & a & 0 \\ 0 & 0 & 1 & 1 & a & a & a+1 & 0 \\ 0 & 0 & a & a+1 & a+1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & a+1 & a+1 & a & 0 \end{pmatrix}$$

Numerical Example: generating matrix

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Generating matrix for C:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & a & a+1 & a & a+1 & a & 0 \\ 0 & 0 & 1 & 1 & a & a & a+1 & 0 \\ 0 & 0 & a & a+1 & a+1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & a+1 & a+1 & a & 0 \end{pmatrix}$$

Sum of third and fifth rows is

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

So $d = 3$.

Decoding Overview

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Fix $t \geq 0$ and let $a = c + e$ with $c \in C_\Omega$ and $wt(e) \leq t$

Decoding Overview

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Fix $t \geq 0$ and let $a = c + e$ with $c \in C_\Omega$ and $wt(e) \leq t$

We want an algorithm to compute c given a

Decoding Overview

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Fix $t \geq 0$ and let $a = c + e$ with $c \in C_\Omega$ and $wt(e) \leq t$

We want an algorithm to compute c given a

Write $e = (e_1, \ldots, e_n)$

Decoding Overview

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Fix $t \geq 0$ and let $a = c + e$ with $c \in C_\Omega$ and $wt(e) \leq t$

We want an algorithm to compute c given a

Write $e = (e_1, \ldots, e_n)$

Algorithm Steps:

1. Construct $f \in F$ such that $f(P_i) = 0$ when $e_i \neq 0$.

Decoding Overview

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Fix $t \geq 0$ and let $a = c + e$ with $c \in C_\Omega$ and $wt(e) \leq t$

We want an algorithm to compute c given a

Write $e = (e_1, \ldots, e_n)$

Algorithm Steps:

1. Construct $f \in F$ such that $f(P_i) = 0$ when $e_i \neq 0$.
2. Compute e_i for all i such that $f(P_i) = 0$.

Decoding Overview

Fix $t \geq 0$ and let $a = c + e$ with $c \in C_\Omega$ and $wt(e) \leq t$

We want an algorithm to compute c given a

Write $e = (e_1, \ldots, e_n)$

Algorithm Steps:

1. Construct $f \in F$ such that $f(P_i) = 0$ when $e_i \neq 0$.
2. Compute e_i for all i such that $f(P_i) = 0$.
3. Since $e_i = 0$ for all i such that $f(P_i) \neq 0$, we have computed e. Then $c = a - e$.

Algorithm Conditions

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Let G_1 be a divisor such that

- $\text{Supp}\, G_1 \cap \text{Supp}\, D = \emptyset$
- $\deg G_1 < \deg G - (2g-2) - t$
- $\ell(G_1) > t$

Algorithm Conditions

Let G_1 be a divisor such that

- $\operatorname{Supp} G_1 \cap \operatorname{Supp} D = \emptyset$
- $\deg G_1 < \deg G - (2g-2) - t$
- $\ell(G_1) > t$

and let

$$[a, f] := \sum_{i=1}^{n} a_i \cdot f(P_i)$$

Algorithm Conditions

Let G_1 be a divisor such that

- $\operatorname{Supp} G_1 \cap \operatorname{Supp} D = \emptyset$
- $\deg G_1 < \deg G - (2g-2) - t$
- $\ell(G_1) > t$

and let

$$[a, f] := \sum_{i=1}^{n} a_i \cdot f(P_i)$$

Fix bases

$$\{f_1, \ldots, f_\ell\} \text{ of } \mathscr{L}(G_1)$$
$$\{g_1, \ldots, g_k\} \text{ of } \mathscr{L}(G - G_1)$$
$$\{h_1, \ldots, h_m\} \text{ of } \mathscr{L}(G)$$

Algorithm Specifics

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Proposition: *For each* $1 \leq \rho \leq k$, *the linear system*

$$\sum_{\lambda=1}^{\ell} [a, f_\lambda g_\rho] \cdot x_\lambda = 0$$

has a nontrivial solution $(\alpha_1, \ldots, \alpha_\ell)$.

Algorithm Specifics

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Proposition: *For each* $1 \leq \rho \leq k$, *the linear system*

$$\sum_{\lambda=1}^{\ell} [a, f_\lambda g_\rho] \cdot x_\lambda = 0$$

has a nontrivial solution $(\alpha_1, \ldots, \alpha_\ell)$.

Let

$$f := \sum_{\lambda=1}^{\ell} \alpha_\lambda f_\lambda$$

Then $f(P_i) = 0$ whenever $e_i \neq 0$

Algorithm Specifics

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Proposition: *For each* $1 \leq \mu \leq m$, *the linear system*

$$\sum_{\{i \mid f(P_i)=0\}} h_\mu(P_i) \cdot z_i = [a, h_\mu]$$

has a unique solution agreeing with e *on all* i *such that* $f(P_i) = 0$.

Algorithm Specifics

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Proposition: *For each* $1 \leq \mu \leq m$, *the linear system*

$$\sum_{\{i \mid f(P_i)=0\}} h_\mu(P_i) \cdot z_i = [a, h_\mu]$$

has a unique solution agreeing with e *on all* i *such that* $f(P_i) = 0$.

Conclusion: Solving the two linear systems completely computes e and hence we can recover $c = a - e$.

Decoding Hermitian Codes

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Proposition: The dual of C_r is $C_{q^3+q^2-q-2-r}$

Decoding Hermitian Codes

Algebraic Geometry Codes

Shelly Manber

Linear Codes

Algebraic Geometry Codes

Example: Hermitian Codes

Decoding

Proposition: The dual of C_r is $C_{q^3+q^2-q-2-r}$

Corollary: $C_{\mathscr{L}}(D, rP_\infty) = C_\Omega(D, (q^3 + q^2 - q - 2 - r)P_\infty)$

Decoding Hermitian Codes

Algebraic Geometry Codes
Shelly Manber
Linear Codes
Algebraic Geometry Codes
Example: Hermitian Codes
Decoding

Proposition: The dual of C_r is $C_{q^3+q^2-q-2-r}$

Corollary: $C_{\mathscr{L}}(D, rP_\infty) = C_\Omega(D, (q^3 + q^2 - q - 2 - r)P_\infty)$

We can decode $C_\Omega(D, (q^3 + q^2 - q - 2 - r)P_\infty)$ with the algorithm given.