Algebro-Geometric Trace Codes

Phong Le

Department of Mathematics
Niagara University

January 2012/Joint Mathematics Meeting

Algebraic Curves over $\mathbb{F}_{p^a}$

- p is a prime
- $q = p^a$, a power of p
- $\mathbb{F}_q$ is the field of q elements
- $\mathbb{F}_{q^m}$ is the field extension of $\mathbb{F}_q$ of degree m
- X is an projective curve of genus g over $\mathbb{F}_{q^m}$
- $\mathbb{F}_{q^m}(X)$ is the function field of X over $\mathbb{F}_{q^m}$

Divisors

- Fix a divisor $G = \sum n_Q Q$, $Q \in X$, $n_Q \in \mathbb{Z} \setminus \{0\}$.
- $\deg(G) = \sum n_Q$
- Split G into positive and negative parts:

$$G^+ = \sum_{n_Q > 0} n_Q Q$$

$$G^- = \sum_{n_Q < 0} n_Q Q$$

$$G = G^+ + G^-$$

Divisor to Vector Space

For $f \in \mathbb{F}_{q^m}(X)$. We can generate a divisor by locating the zeros and poles of the function.

- The divisor of a function f is denoted (f).
- If $Q \in X$ is a zero of f with multiplicity n_Q then $n_Q Q$ appears in (f).
- If $P \in X$ is a pole of f with multiplicity n_P then $-n_P P$ appears in (f).

Example

Let $X = \mathbb{P}^1$ the projective curve. Let $f(x) = x$.

$$(f) = 0 - \infty.$$

Divisor to Vector Space

For $f \in \mathbb{F}_{q^m}(X)$. We can generate a divisor by locating the zeros and poles of the function.

- The divisor of a function f is denoted (f).
- If $Q \in X$ is a zero of f with multiplicity n_Q then $n_Q Q$ appears in (f).
- If $P \in X$ is a pole of f with multiplicity n_P then $-n_P P$ appears in (f).

Example

Let $X = \mathbb{P}^1$ the projective curve. Let $f(x) = x$.

$$(f) = 0 - \infty.$$

$\mathcal{L}(G)$

For a divisor G we can generate a vector space of functions:

$$\mathcal{L}(G) := \{f \in \mathbb{F}_{q^m}(X) \mid (f) + G \geq 0\} \cup \{0\}$$

- These are functions who have at least as many zeros as G and at worst as many poles as G.
- G^+ bounds the multiplicity and location of the poles
- G^- determine the required multiplicity and location of zeros
- This is a vector space, but not a terribly code friendly one.

Algebro-Geometric Codes

Let $D = \{P_1, \ldots, P_n\}$ be $\mathbb{F}_{q^m}$ rational points of X away from G^+. Usually we just take $D = X \setminus Supp(G^+)$.

$$C = C(D, G) := \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_{q^m}^n.$$

Theorem (Riemann-Roch)

If $2g - 2 < \deg(G) < n$:

$$\dim_{\mathbb{F}_{q^m}}(\mathcal{L}(G)) = \deg(G) + 1 - g.$$

Furthermore, when $\deg(G) < n$ we know the dimension of C is the same as the dimension of $\mathcal{L}(G)$.

Algebro-Geometric Codes

Let $D = \{P_1, \ldots, P_n\}$ be $\mathbb{F}_{q^m}$ rational points of X away from G^+. Usually we just take $D = X \setminus Supp(G^+)$.

$$C = C(D, G) := \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_{q^m}^n.$$

Theorem (Riemann-Roch)

If $2g - 2 < \deg(G) < n$*:*

$$\dim_{\mathbb{F}_{q^m}}(\mathcal{L}(G)) = \deg(G) + 1 - g.$$

Furthermore, when $\deg(G) < n$ we know the dimension of C is the same as the dimension of $\mathcal{L}(G)$.

The Trace Map

Define the trace function to be $Tr : \mathbb{F}_{q^m} \mapsto \mathbb{F}_q$ where

$$Tr(x) = x + x^q + \ldots + x^{q^{m-2}} + x^{q^{m-1}}.$$

This is necessarily an element of $\mathbb{F}_q$.

Example

Let t be a generator of $\mathbb{F}_{7^3}$ where t satisfies the polynomial $x^3 + 6x^2 + 4$.

$$Tr(x) = x + x^7 + x^{49}$$

$$Tr(t) = t + t^7 + t^{49} = 1$$

$$Tr(2t+1) = (2t+1) + (2t+1)^7 + (2t+1)^{49} = 5$$

The Trace Map

Define the trace function to be $Tr : \mathbb{F}_{q^m} \mapsto \mathbb{F}_q$ where

$$Tr(x) = x + x^q + \ldots + x^{q^{m-2}} + x^{q^{m-1}}.$$

This is necessarily an element of $\mathbb{F}_q$.

Example

Let t be a generator of $\mathbb{F}_{7^3}$ where t satisfies the polynomial $x^3 + 6x^2 + 4$.

$$Tr(x) = x + x^7 + x^{49}$$

$$Tr(t) = t + t^7 + t^{49} = 1$$

$$Tr(2t+1) = (2t+1) + (2t+1)^7 + (2t+1)^{49} = 5$$

AG Trace Code

$$C = C(D,G) := \{(f(P_1),\dots,f(P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_{q6m}^n.$$

Let *TrC* denote the trace of C:

$$TrC := \{(Tr(f(P_1)),\dots,Tr(f(P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

TrC is a vector space over $\mathbb{F}_q$.

Main Question

What is the dimension of *TrC*? Or, what sorts of constraints can we put on *TrC* so that we can find or bound the dimension?

AG Trace Code

$$C = C(D, G) := \{(f(P_1), \dots, f(P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_{q6m}^n.$$

Let *TrC* denote the trace of C:

$$TrC := \{(Tr(f(P_1)), \dots, Tr(f(P_n)) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

TrC is a vector space over $\mathbb{F}_q$.

Main Question

What is the dimension of *TrC*? Or, what sorts of constraints can we put on *TrC* so that we can find or bound the dimension?

Recap

- Curve X of genus g defined over $\mathbb{F}_{p^a}$
- Divisor $G = \sum n_Q Q$ on X
- G splits into positive and negative coefficient parts $G = G^+ + G^-$
- Set of points $D = \{P_1, \ldots, P_n\}$ away from G^+
- $C(G, D) = \{(f(P_1), \ldots, f(P_n) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_{q^m}^n$
- $TrC = \{(Tr(f(P_1)), \ldots, Tr(f(P_n))) \mid f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n$

The Kernel K

Viewing Tr as a $\mathbb{F}_a$-linear map we can generate an exact sequence:

$$0 \to K \to C \to TrC \to 0$$

K consists of all elements who trace to zero.

$$\dim_{\mathbb{F}_a}(TrC) = m(\dim_{\mathbb{F}_{q^m}}(C) - \dim_{\mathbb{F}_{q^m}}(K))$$

Since Riemann-Roch gives us conditions for determining $\dim_{\mathbb{F}_{q^m}}(C)$ we may turn our focus on K.

Note

It is easier to think of K as a subspace of $\mathcal{L}(G)$ and not as a subspace of $C(G, D)$ so that's what I'll do even though this is technically incorrect.

The Kernel K

Viewing Tr as a $\mathbb{F}_a$-linear map we can generate an exact sequence:

$$0 \to K \to C \to TrC \to 0$$

K consists of all elements who trace to zero.

$$\dim_{\mathbb{F}_a}(TrC) = m(\dim_{\mathbb{F}_{q^m}}(C) - \dim_{\mathbb{F}_{q^m}}(K))$$

Since Riemann-Roch gives us conditions for determining $\dim_{\mathbb{F}_{q^m}}(C)$ we may turn our focus on K.

Note

It is easier to think of K as a subspace of $\mathcal{L}(G)$ and not as a subspace of $C(G, D)$ so that's what I'll do even though this is technically incorrect.

The First Ingredient

Theorem (Hilbert 90 for Traces)

For $\alpha \in \mathbb{F}_{q^m}$ we have $Tr(\alpha) = 0$ if and only if $\alpha = \beta^q - \beta$ for some $\beta \in \mathbb{F}_{q^m}$.

$$E := \{f = h^q - h \mid f \in \mathcal{L}(G), h \in \mathbb{F}_{q^m}(X)\} \subseteq K$$

Question

What is the dimension of E and when is $E = K$?

The First Ingredient

Theorem (Hilbert 90 for Traces)

For $\alpha \in \mathbb{F}_{q^m}$ we have $Tr(\alpha) = 0$ if and only if $\alpha = \beta^q - \beta$ for some $\beta \in \mathbb{F}_{q^m}$.

$$E := \{f = h^q - h \mid f \in \mathcal{L}(G), h \in \mathbb{F}_{q^m}(X)\} \subseteq K$$

Question

What is the dimension of E and when is $E = K$?

The First Ingredient

Theorem (Hilbert 90 for Traces)

For $\alpha \in \mathbb{F}_{q^m}$ we have $Tr(\alpha) = 0$ if and only if $\alpha = \beta^q - \beta$ for some $\beta \in \mathbb{F}_{q^m}$.

$$E := \{f = h^q - h \mid f \in \mathcal{L}(G), h \in \mathbb{F}_{q^m}(X)\} \subseteq K$$

Question

What is the dimension of E and when is $E = K$?

The dimension of E

- $G = G^+ + G^-$
- $[G/q] := \sum_{n_Q>0}[n_Q/q]Q + \sum_{n_Q<0} n_Q Q$
- $[G/q]$ reduces the maximum number of poles a function is allowed to have.
- If $h \in \mathcal{L}([G/q])$ then $h^q - h \in E \subseteq \mathcal{L}(G)$.
- When is $\mathcal{L}([G/q]) \xrightarrow{h^q-h} \mathcal{L}(G)$ surjective?

One way to force surjectivity is to install further controls on the poles:

Proposition

When $\#Supp(G^-) \leq 1$,

$$\dim_{\mathbb{F}_q} E = \dim_{\mathbb{F}_q} \mathcal{L}[G/q] - \dim_{\mathbb{F}_q}(\mathbb{F}_q \cap \mathcal{L}[G/q]).$$

These dimensions are much more accessible via Riemann-Roch.

Side Question

Is there any other sort of restriction on G we can devise that will give us an easy formula for the dimension of E?

One way to force surjectivity is to install further controls on the poles:

Proposition

When $\# Supp(G^-) \leq 1$,

$$\dim_{\mathbb{F}_q} E = \dim_{\mathbb{F}_q} \mathcal{L}[G/q] - \dim_{\mathbb{F}_q}(\mathbb{F}_q \cap \mathcal{L}[G/q]).$$

These dimensions are much more accessible via Riemann-Roch.

Side Question

Is there any other sort of restriction on G we can devise that will give us an easy formula for the dimension of E?

The Second Ingredient

Theorem (Bombieri's estimate(1966))

Let X be a complete, geometrically irreducible, nosingular curve of genus g, defined over $\mathbb{F}_{q^m}$. Let $f \in \mathbb{F}_{q^m}(X)$, $f \neq h^p - h$ for $h \in \overline{\mathbb{F}_p}(X)$, with pole divisor $(f)_\infty$ on X. Then

$$\left| \sum_{P \in X(\mathbb{F}_{q^m}) \setminus (f)_\infty} \zeta_p^{Tr_{q^m/p}(f(P))} \right| \leq (2g - 2 + t + \deg(f)_\infty) q^{m/2}.$$

where $\zeta_p = \exp(2\pi i/p)$ is a primitive p-th root of unity and t is the number of distinct poles of f on X.

Note that on the LHS we take the full trace down to the prime field.

Key Lemma

If we choose an $f \in K \setminus E$ then the LHS must be maximized. This leads to the following lemma and proposition:

Lemma

Suppose $K \neq E$. Then there is an $f \in K \setminus E$ that is not of the form $h^p - h$ for h in $\overline{\mathbb{F}_p}(X)$.

Proposition

If

$$\#X(\mathbb{F}_{q^m}) > (2g - 2 + \deg(G^+))q^{m/2} + \#Supp(G^+)(q^{m/2} + 1)$$

then $K = E$.

Key Lemma

If we choose an $f \in K \setminus E$ then the LHS must be maximized. This leads to the following lemma and proposition:

Lemma

Suppose $K \neq E$. Then there is an $f \in K \setminus E$ that is not of the form $h^p - h$ for h in $\overline{\mathbb{F}_p}(X)$.

Proposition

If

$$\#X(\mathbb{F}_{q^m}) > (2g - 2 + \deg(G^+))q^{m/2} + \#Supp(G^+)(q^{m/2} + 1)$$

then $K = E$.

Main Theorem

Theorem (Wan, L-)

Let $2g - 2 \leq \deg([G/q])$ *and* $\deg(G) < n$. *Assume the following:*

$$\#Supp(G^-) \leq 1,$$

$$\#X(\mathbb{F}_{q^m}) > (2g - 2 + \deg(G^+))q^{m/2} + Supp(G^+)(q^{m/2} + 1)$$

Under these conditions we have:

$$\dim_{\mathbb{F}_q}(TrC) = m(\deg(G) - \deg([G/q])) + \delta,$$

where

$$\delta = \begin{cases} 1 & \text{if} \#Supp(G^-) = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Example

For a smooth projective curve X of genus g defined over $\mathbb{F}_{q^m}$, let $G = kP_\infty$ for $k \in \mathbb{Z}_{\geq 0}$. By the Hasse-Weil bound we have

$$|\#X(\mathbb{F}_{q^m}) - (q^m + 1)| \leq 2gq^{m/2}.$$

By the second condition we want

$$\#X(\mathbb{F}_{q^m}) > (2g - 2 + k)q^{m/2} + (q^{m/2} + 1).$$

Combining these two inequalities, we see that the second condition is satisfied when

$$q^{m/2} - 4g + 1 > k.$$

Example: Continued

We obtain the following:

Corollary

For X a smooth projective curve over $\mathbb{F}_{q^m}$ and $G = kP_\infty$. if $2g - 2 \leq [k/q]$ and $k < \min(n, q^{m/2} - 4g + 1)$ then

$$\dim_{\mathbb{F}_q} TrC = m(k - [k/q]) + 1.$$

Credits

- A generalization of work done by Marcel Van der Vlugt: *A New Upper Bound for the Dimension of Trace Codes.* Bull. London Math. Soc. 23 (1991), 395-400.
- Joint work with Daqing Wan
- preprint can be found on my website

Thank You!

http://math.uci.edu/~ple