On the Zeta Function of Curves over Finite Fields

Nurdagül Anbar
(joint work with Henning Stichtenoth)

Sabancı University

RICAM, Workshop 2: Algebraic Curves over Finite Fields
11-15 November 2013

L-polynomial of a curve

$\mathcal{X}$: a nice curve over $\mathbb{F}_q$ of genus g.

The Zeta function of $\mathcal{X}$,

$$Z_{\mathcal{X}}(t) = \frac{L_{\mathcal{X}}(t)}{(1-t)(1-qt)},$$

where $L_{\mathcal{X}}(t) \in \mathbb{Z}[t]$ of degree $2g$.

$L_{\mathcal{X}}(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g}$ (L-polynomial of $\mathcal{X}$)

- $a_0 = 1$
- $a_1 = N - (q+1)$, where N is the number of rational points of $\mathcal{X}$
- $a_{2g-i} = q^{g-i} a_i$ for $i = 0, \ldots, g$

L-polynomial of a curve

$\mathcal{X}$: a nice curve over $\mathbb{F}_q$ of genus g.

The Zeta function of $\mathcal{X}$,

$$Z_{\mathcal{X}}(t) = \frac{L_{\mathcal{X}}(t)}{(1-t)(1-qt)},$$

where $L_{\mathcal{X}}(t) \in \mathbb{Z}[t]$ of degree $2g$.

$L_{\mathcal{X}}(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g}$ (L-polynomial of $\mathcal{X}$)

- $a_0 = 1$
- $a_1 = N - (q+1)$, where N is the number of rational points of $\mathcal{X}$
- $a_{2g-i} = q^{g-i} a_i$ for $i = 0, \ldots, g$

L-polynomial of a curve

$\mathcal{X}$: a nice curve over $\mathbb{F}_q$ of genus g.

The Zeta function of $\mathcal{X}$,

$$Z_{\mathcal{X}}(t) = \frac{L_{\mathcal{X}}(t)}{(1-t)(1-qt)} ,$$

where $L_{\mathcal{X}}(t) \in \mathbb{Z}[t]$ of degree $2g$.

$L_{\mathcal{X}}(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g}$ (L-polynomial of $\mathcal{X}$)

- $a_0 = 1$
- $a_1 = N - (q+1)$, where N is the number of rational points of $\mathcal{X}$
- $a_{2g-i} = q^{g-i} a_i$ for $i = 0, \ldots, g$

Some notation

Remember: $\mathcal{X}$ is defined over $\mathbb{F}_q$

$F_d := \mathbb{F}_{q^d}$
$\mathcal{X}_d$: the curve $\mathcal{X}$ over F_d
N_d: the number of rational points of $\mathcal{X}_d$
$S_d := N_d - (q^d + 1)$
B_r: the number of degree r points of $\mathcal{X}$

$L(t) = L_{\mathcal{X}}(t) = 1 + a_1 t + \ldots + a_{2g} t^{2g}$

$$S_d = da_d - \sum_{j=1}^{d-1} S_{d-j} a_j \quad \text{with} \quad S_1 = N_1 - (q+1) = a_1$$

$$rB_r = \sum_{d|r} \mu\left(\frac{r}{d}\right)(q^d + 1 + S_d) \quad \text{for all} \quad r \geq 1 \ ,$$

for all $r \geq 1$, where $\mu(.)$ is the Möbius function.

Some notation

Remember: $\mathcal{X}$ is defined over $\mathbb{F}_q$

$F_d := \mathbb{F}_{q^d}$
$\mathcal{X}_d$: the curve $\mathcal{X}$ over F_d
N_d: the number of rational points of $\mathcal{X}_d$
$S_d := N_d - (q^d + 1)$
B_r: the number of degree r points of $\mathcal{X}$

$L(t) = L_{\mathcal{X}}(t) = 1 + a_1 t + \ldots + a_{2g} t^{2g}$

$$S_d = d a_d - \sum_{j=1}^{d-1} S_{d-j} a_j \text{ with } S_1 = N_1 - (q+1) = a_1$$

$$r B_r = \sum_{d \mid r} \mu\left(\frac{r}{d}\right)(q^d + 1 + S_d) \text{ for all } r \geq 1 ,$$

for all $r \geq 1$, where $\mu(.)$ is the Möbius function.

Some recursively defined functions over $\mathbb{Z}$:

$\sigma_0 := 0$ and for all $r \geq 1$,

$$\sigma_r(T_1, \ldots, T_r) := rT_r - \sum_{j=1}^{r-1} \sigma_{r-j}(T_1, \ldots, T_{r-j}) \cdot T_j$$

$$\beta_r(T_1, \ldots, T_r) := \sum_{d|r} \mu(\frac{r}{d})\sigma_d(T_1, \ldots, T_d) + \sum_{d|r} \mu(\frac{r}{d})(q^d + 1)$$

$$\varphi_r(T_1, \ldots, T_{r-1}) := rT_r - \beta_r(T_1, \ldots, T_r)$$

$$\sigma_r(a_1, \ldots, a_r) = S_r = N_r - (q^r + 1) \quad \text{and} \quad \beta_r(a_1, \ldots, a_r) = rB_r$$

$$\implies ra_r = \varphi_r(a_1, \ldots, a_{r-1}) + rB_r$$

Some recursively defined functions over $\mathbb{Z}$:

$\sigma_0 := 0$ and for all $r \geq 1$,

$$\sigma_r(T_1, \ldots, T_r) := rT_r - \sum_{j=1}^{r-1} \sigma_{r-j}(T_1, \ldots, T_{r-j}) \cdot T_j$$

$$\beta_r(T_1, \ldots, T_r) := \sum_{d|r} \mu\left(\frac{r}{d}\right)\sigma_d(T_1, \ldots, T_d) + \sum_{d|r} \mu\left(\frac{r}{d}\right)(q^d + 1)$$

$$\varphi_r(T_1, \ldots, T_{r-1}) := rT_r - \beta_r(T_1, \ldots, T_r)$$

$$\sigma_r(a_1, \ldots, a_r) = S_r = N_r - (q^r + 1) \quad \text{and} \quad \beta_r(a_1, \ldots, a_r) = rB_r$$

$$\Longrightarrow ra_r = \varphi_r(a_1, \ldots, a_{r-1}) + rB_r$$

Some recursively defined functions over $\mathbb{Z}$:

$\sigma_0 := 0$ and for all $r \geq 1$,

$$\sigma_r(T_1, \ldots, T_r) := rT_r - \sum_{j=1}^{r-1} \sigma_{r-j}(T_1, \ldots, T_{r-j}) \cdot T_j$$

$$\beta_r(T_1, \ldots, T_r) := \sum_{d|r} \mu(\frac{r}{d})\sigma_d(T_1, \ldots, T_d) + \sum_{d|r} \mu(\frac{r}{d})(q^d + 1)$$

$$\varphi_r(T_1, \ldots, T_{r-1}) := rT_r - \beta_r(T_1, \ldots, T_r)$$

$$\sigma_r(a_1, \ldots, a_r) = S_r = N_r - (q^r + 1) \quad \text{and} \quad \beta_r(a_1, \ldots, a_r) = rB_r$$

$$\Longrightarrow ra_r = \varphi_r(a_1, \ldots, a_{r-1}) + rB_r$$

Necessary conditions on the coefficients of L-polynomial

Theorem

Let $\mathcal{X}$ be a non-singular, absolutely irreducible, projective curve defined over $\mathbb{F}_q$ and let $L_{\mathcal{X}}(t) = 1 + a_1 t + \ldots + a_{2g} t^{2g}$ be its L-polynomial. Then the inequalities

$$ra_r \geq \varphi_r(a_1, \ldots, a_{r-1})$$

hold for $r = 1, \ldots, g$.

Example

$a_1 \geq -(q+1)$

$2a_2 \geq a_1^2 + a_1 - (q^2 - q)$

$3a_3 \geq -a_1^3 + a_1 + 3a_1 a_2 - (q^3 - q)$

$4a_4 \geq -a_1^4 - a_1^2 - 4a_1^2 a_2 + 4a_1 a_3 + 2a_2 - (q^4 - q^2)$

Necessary conditions on the coefficients of L-polynomial

Theorem

Let $\mathcal{X}$ be a non-singular, absolutely irreducible, projective curve defined over $\mathbb{F}_q$ and let $L_{\mathcal{X}}(t) = 1 + a_1 t + \ldots + a_{2g} t^{2g}$ be its L-polynomial. Then the inequalities

$$ra_r \geq \varphi_r(a_1, \ldots, a_{r-1})$$

hold for $r = 1, \ldots, g$.

Example

$a_1 \geq -(q+1)$
$2a_2 \geq a_1^2 + a_1 - (q^2 - q)$
$3a_3 \geq -a_1^3 + a_1 + 3a_1 a_2 - (q^3 - q)$
$4a_4 \geq -a_1^4 - a_1^2 - 4a_1^2 a_2 + 4a_1 a_3 + 2a_2 - (q^4 - q^2)$

The converse of the Theorem

Problem:

Let $(a_1, a_2, \ldots, a_m) \in \mathbb{Z}^m$ satisfying $ra_r \geq \varphi_r(a_1, \ldots, a_{r-1})$ for all $r = 1, \ldots, m$. Is there a curve $\mathcal{X}$ of genus g over $\mathbb{F}_q$ whose L-polynomial has the form

$$L(t) = 1 + a_1 t + a_2 t^2 + \ldots + a_m t^m + \ldots \quad ?$$

Not in general!

Hasse-Weil Theorem: $L(t) = \prod_{k=1}^{2g}(1 - w_k t)$ with $| w_k | = \sqrt{q}$

$$\Longrightarrow | a_r | \leq \binom{2g}{r} \cdot \sqrt{q^r} \quad \text{for } r = 1, \ldots, g .$$

The converse of the Theorem

Problem:

Let $(a_1, a_2, \ldots, a_m) \in \mathbb{Z}^m$ satisfying $ra_r \geq \varphi_r(a_1, \ldots, a_{r-1})$ for all $r = 1, \ldots, m$. Is there a curve $\mathcal{X}$ of genus g over $\mathbb{F}_q$ whose L-polynomial has the form

$$L(t) = 1 + a_1 t + a_2 t^2 + \ldots + a_m t^m + \ldots \quad ?$$

Not in general!

Hasse-Weil Theorem: $L(t) = \prod_{k=1}^{2g}(1 - w_k t)$ with $\mid w_k \mid = \sqrt{q}$

$$\Longrightarrow \mid a_r \mid \leq \binom{2g}{r} \cdot \sqrt{q^r} \quad \text{for } r = 1, \ldots, g\ .$$

The converse of the Theorem

Problem:

Let $(a_1, a_2, \ldots, a_m) \in \mathbb{Z}^m$ satisfying $ra_r \geq \varphi_r(a_1, \ldots, a_{r-1})$ for all $r = 1, \ldots, m$. Is there a curve $\mathcal{X}$ of genus g over $\mathbb{F}_q$ whose L-polynomial has the form

$$L(t) = 1 + a_1 t + a_2 t^2 + \ldots + a_m t^m + \ldots \quad ?$$

Not in general!

Hasse-Weil Theorem: $L(t) = \prod_{k=1}^{2g}(1 - w_k t)$ with $\mid w_k \mid = \sqrt{q}$

$$\Longrightarrow \mid a_r \mid \leq \binom{2g}{r} \cdot \sqrt{q^r} \quad \text{for } r = 1, \ldots, g \ .$$

Theorem (A., Stichtenoth)

Let $a_1, \ldots, a_m$ be integers such that $ra_r \geq \varphi_r(a_1, \ldots, a_{r-1})$ for $r = 1, \ldots, m$. Then there is an integer $g_0 \geq m$ such that for all $g \geq g_0$, there exists a curve over $\mathbb{F}_q$ of genus g whose L-polynomial has the form

$$L(t) \equiv 1 + a_1 t + \ldots + a_m t^m \mod t^{m+1}$$

Sketch of the proof

Remember: $ra_r = \varphi_r(a_1, \ldots, a_{r-1}) + rB_r$ for $r \geq 1$.

Step 1:
For all $m \geq 1$ and all $(a_1, \ldots, a_{m-1}) \in \mathbb{Z}^{m-1}$,

$$\varphi_m(a_1, \ldots, a_{m-1}) \equiv 0 \mod m .$$

Step 2:
Define $b_r := r^{-1}(ra_r - \varphi_r(a_1, \ldots, a_{r-1}))$ for $r = 1, \ldots, m$.

Equivalent statement:

Let $b_1, \ldots, b_m$ be non-negative integers. Then there is a constant $g_0 \geq m$ such that for all integers $g \geq g_0$ there exists a curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus g such that $\mathcal{X}$ has exactly b_r points of degree r, for $r = 1, \ldots, m$.

Sketch of the proof

Remember: $ra_r = \varphi_r(a_1, \ldots, a_{r-1}) + rB_r$ for $r \geq 1$.

Step 1:
For all $m \geq 1$ and all $(a_1, \ldots, a_{m-1}) \in \mathbb{Z}^{m-1}$,

$$\varphi_m(a_1, \ldots, a_{m-1}) \equiv 0 \mod m \ .$$

Step 2:
Define $b_r := r^{-1}(ra_r - \varphi_r(a_1, \ldots, a_{r-1}))$ for $r = 1, \ldots, m$.

Equivalent statement:

Let $b_1, \ldots, b_m$ be non-negative integers. Then there is a constant $g_0 \geq m$ such that for all integers $g \geq g_0$ there exists a curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus g such that $\mathcal{X}$ has exactly b_r points of degree r, for $r = 1, \ldots, m$.

Sketch of the proof

Remember: $ra_r = \varphi_r(a_1, \ldots, a_{r-1}) + rB_r$ for $r \geq 1$.

Step 1:
For all $m \geq 1$ and all $(a_1, \ldots, a_{m-1}) \in \mathbb{Z}^{m-1}$,

$$\varphi_m(a_1, \ldots, a_{m-1}) \equiv 0 \mod m \ .$$

Step 2:
Define $b_r := r^{-1}(ra_r - \varphi_r(a_1, \ldots, a_{r-1}))$ for $r = 1, \ldots, m$.

Equivalent statement:

Let $b_1, \ldots, b_m$ be non-negative integers. Then there is a constant $g_0 \geq m$ such that for all integers $g \geq g_0$ there exists a curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus g such that $\mathcal{X}$ has exactly b_r points of degree r, for $r = 1, \ldots, m$.

Sketch of the proof

Remember: $ra_r = \varphi_r(a_1, \ldots, a_{r-1}) + rB_r$ for $r \geq 1$.

Step 1:
For all $m \geq 1$ and all $(a_1, \ldots, a_{m-1}) \in \mathbb{Z}^{m-1}$,

$$\varphi_m(a_1, \ldots, a_{m-1}) \equiv 0 \mod m \, .$$

Step 2:
Define $b_r := r^{-1}(ra_r - \varphi_r(a_1, \ldots, a_{r-1}))$ for $r = 1, \ldots, m$.

Equivalent statement:

Let $b_1, \ldots, b_m$ be non-negative integers. Then there is a constant $g_0 \geq m$ such that for all integers $g \geq g_0$ there exists a curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus g such that $\mathcal{X}$ has exactly b_r points of degree r, for $r = 1, \ldots, m$.

The proof of Step 2:

The proof is by construction.

- For given $b_1, \ldots, b_m$, there exists a curve $\mathcal{Y}$ over $\mathbb{F}_q$ with $B_1(\mathcal{Y}) \geq b_1, \ldots, B_m(\mathcal{Y}) \geq b_m$.

- Define the sets
S_1 consisting of exactly b_r points of degree r for $r = 1, \ldots, m$
$S_2 := \{Q \in \mathcal{Y} \mid Q \notin S_1 \text{ and } \deg Q \leq m\}$

- Construct an Artin-Schreier cover $\widetilde{\mathcal{Y}}$ such that each $P \in S_1$ totally ramifies and each $Q \in S_2$ gets inert.

The proof of Step 2:

The proof is by construction.

- For given $b_1, \dots, b_m$, there exists a curve $\mathcal{Y}$ over $\mathbb{F}_q$ with $B_1(\mathcal{Y}) \geq b_1, \dots, B_m(\mathcal{Y}) \geq b_m$.

- Define the sets
S_1 consisting of exactly b_r points of degree r for $r = 1, \dots, m$
$S_2 := \{Q \in \mathcal{Y} \mid Q \notin S_1 \text{ and } \deg Q \leq m\}$

- Construct an Artin-Schreier cover $\widetilde{\mathcal{Y}}$ such that each $P \in S_1$ totally ramifies and each $Q \in S_2$ gets inert.

The proof of Step 2:

The proof is by construction.

- For given $b_1, \ldots, b_m$, there exists a curve $\mathcal{Y}$ over $\mathbb{F}_q$ with $B_1(\mathcal{Y}) \geq b_1, \ldots, B_m(\mathcal{Y}) \geq b_m$.

- Define the sets
S_1 consisting of exactly b_r points of degree r for $r = 1, \ldots, m$
$S_2 := \{Q \in \mathcal{Y} \mid Q \notin S_1 \text{ and } \deg Q \leq m\}$

- Construct an Artin-Schreier cover $\widetilde{\mathcal{Y}}$ such that each $P \in S_1$ totally ramifies and each $Q \in S_2$ gets inert.

The proof of Step 2:

The proof is by construction.

- For given $b_1, \ldots, b_m$, there exists a curve $\mathcal{Y}$ over $\mathbb{F}_q$ with $B_1(\mathcal{Y}) \geq b_1, \ldots, B_m(\mathcal{Y}) \geq b_m$.

- Define the sets
S_1 consisting of exactly b_r points of degree r for $r = 1, \ldots, m$
$S_2 := \{Q \in \mathcal{Y} \mid Q \notin S_1 \text{ and } \deg Q \leq m\}$

- Construct an Artin-Schreier cover $\widetilde{\mathcal{Y}}$ such that each $P \in S_1$ totally ramifies and each $Q \in S_2$ gets inert.

Special Case: $m = 1$

Theorem

Let b be a non-negative integer. Then there are constants $\alpha(q) > 0$ and $\beta(q)$ such that for all integers $g \geq \alpha(q)b + \beta(q)$, there exists a curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus g having exactly b rational points.

Basis step: Curves with many rational points

- the Garcia-Stichtenoth tower (q: square)
- the Elkies et al. class field tower

Remark: (q: square)

Let $p = \mathrm{char}\mathbb{F}_q$ and q be a square. Then g_0 can be defined as $4p(p+11)b$.

Special Case: $m = 1$

Theorem

Let b be a non-negative integer. Then there are constants $\alpha(q) > 0$ and $\beta(q)$ such that for all integers $g \geq \alpha(q)b + \beta(q)$, there exists a curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus g having exactly b rational points.

Basis step: Curves with many rational points

- the Garcia-Stichtenoth tower (q: square)
- the Elkies et al. class field tower

Remark: (q: square)

Let $p = \mathrm{char}\mathbb{F}_q$ and q be a square. Then g_0 can be defined as $4p(p+11)b$.

Special Case: $m = 1$

Theorem

Let b be a non-negative integer. Then there are constants $\alpha(q) > 0$ and $\beta(q)$ such that for all integers $g \geq \alpha(q)b + \beta(q)$, there exists a curve $\mathcal{X}$ over $\mathbb{F}_q$ of genus g having exactly b rational points.

Basis step: Curves with many rational points

- the Garcia-Stichtenoth tower (q: square)
- the Elkies et al. class field tower

Remark: (q: square)

Let $p = \mathrm{char}\mathbb{F}_q$ and q be a square. Then g_0 can be defined as $4p(p + 11)b$.

Remark:

Elkis et al.: For any q, there exists a sequence of curves $\mathcal{X}_i$ over $\mathbb{F}_q$ with

$$\lim_{g \to \infty} \frac{N(\mathcal{X}_i)}{g(\mathcal{X}_i)} = c_q \ ,$$

where $c_q > 0$ is a constant depending only on q.

A., Stichtenoth: For any q, there exists a constant δ_q depending only on q such that for any $c \in [0, \delta_q]$ there exists a sequence of curves $\mathcal{X}_i$ over $\mathbb{F}_q$ with

$$\lim_{g \to \infty} \frac{N(\mathcal{X}_i)}{g(\mathcal{X}_i)} = c \ .$$

Remark:

Elkis et al.: For any q, there exists a sequence of curves $\mathcal{X}_i$ over $\mathbb{F}_q$ with

$$\lim_{g \to \infty} \frac{N(\mathcal{X}_i)}{g(\mathcal{X}_i)} = c_q \ ,$$

where $c_q > 0$ is a constant depending only on q.

A., Stichtenoth: For any q, there exists a constant δ_q depending only on q such that for any $c \in [0, \delta_q]$ there exists a sequence of curves $\mathcal{X}_i$ over $\mathbb{F}_q$ with

$$\lim_{g \to \infty} \frac{N(\mathcal{X}_i)}{g(\mathcal{X}_i)} = c \ .$$

Thanks for your attention!