On the Zeta Functions of an optimal tower over $\mathbb{F}_4$

Alexey Zaytsev,
(Joint work with Gary McGuire)

Claude Shannon Institute and
School of Mathematical Sciences
University College Dublin
Ireland

July 14, 2009

Optimal tower

Let $\mathrm{T}_1 := \mathbb{F}_4(x_1)$ be a rational function field. The second Garcia-Stichtenoth tower over $\mathbb{F}_4$ is defined by

$$\mathrm{T}_n := \mathbb{F}_4(x_1, \ldots, x_n),$$

where

$$x_i^2 + x_i = \frac{x_{i-1}^3}{x_{i-1}^2 + x_{i-1}}.$$

This tower is an optimal tower, i.e.,

$$\lim \frac{N(\mathrm{T}_n)}{g(\mathrm{T}_n)} = \sqrt{4} - 1 = 1 \quad \text{as} \quad n \to \infty.$$

Galois Group and Kani-Rosen decomposition

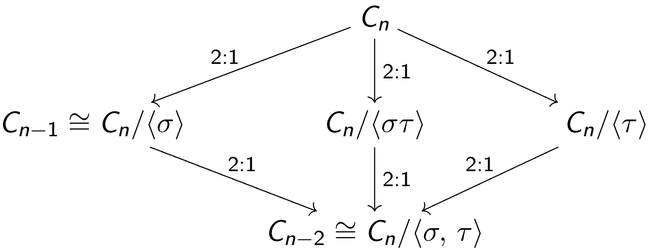
Proposition

If $n \geq 3$, then the extension T_n over T_{n-2} is Galois and

$$\mathrm{Gal}(\mathrm{T}_n/\mathrm{T}_{n-2}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

We will always let C_n denote a curve with function field T_n. The Galois covering $C_n \to C_{n-2}$ implies a decomposition of the Jacobian of the curve C_n. If we denote Galois automorphism group by $\langle \sigma, \tau \rangle$ then we have the following diagram of coverings

Galois Group and Kani-Rosen decomposition



and the following isogeny of Jacobians

$$\mathrm{Jac}(C_n) \times \mathrm{Jac}(C_{n-2})^2 \sim \mathrm{Jac}(C_{n-1}) \times \mathrm{Jac}(C_n/\langle\sigma\tau\rangle) \times \mathrm{Jac}(C_n/\langle\tau\rangle),$$

which implies decomposition of $\mathrm{L}-$polynomials

$$\mathrm{L}_{C_n}(T)\,\mathrm{L}_{C_{n-2}}(T)^2 = \mathrm{L}_{C_{n-1}}(T)\,\mathrm{L}_{C_n/\langle\sigma\tau\rangle}(T)\,\mathrm{L}_{C_n/\langle\tau\rangle}(T).$$

The L-polynomial of T_3

We start with remark that

$$\mathbb{F}_4(C_3/\langle\sigma\tau\rangle) = \mathbb{F}_4(x_1, x_3(x_3 + 1/x_1 + \gamma + 1)),$$

and

$$\mathbb{F}_4(C_3/\langle\tau\rangle) = \mathbb{F}_4(x_1, x_3(x_3 + 1/x_1 + \gamma)),$$

where $\gamma^2 + \gamma + 1 = 0$.
It is not hard to rephrase these quotients in terms of Artin-Schreier extensions, for example

$$\mathbb{F}_4(C_3/\langle\tau\rangle) = \mathbb{F}_4(x_1, u),$$

where u is a root of the polynomial

$$T^2 + T + \left(\frac{x_1^2}{x_1 + 1}\right)\left(\frac{x_1^2}{1 + \gamma^2 x_1^2}\right).$$

The L-polynomial of T_3

The following L-polynomials can be computed:

$$\begin{aligned}
&\mathrm{L}_{\mathrm{T}_1}(T) = \mathrm{L}_{\mathbb{P}^1} = 1, \\
&\mathrm{L}_{C_3/\langle\sigma\rangle}(T) = \mathrm{L}_{\mathrm{T}_2}(T) = 1 + 3T + 4T^2, \\
&\mathrm{L}_{C_3/\langle\sigma\tau\rangle}(T) = 1 + 3T + 4T^2, \\
&\mathrm{L}_{C_3/\langle\tau\rangle}(T) = 1 + 3T + 4T^2.
\end{aligned}$$

Therefore

$$\mathrm{L}_{\mathrm{T}_3}(T) = (1 + 3T + 4T^2)^3.$$

The L-polynomial of T_5

The decomposition of Jacobian into isogeny factors has the form

$$\mathrm{Jac}(\mathrm{C}_3)^2 \times \mathrm{Jac}(\mathrm{C}_5) \sim \mathrm{Jac}(C_4) \times \mathrm{Jac}(C_5/\langle \sigma\tau \rangle) \times \mathrm{Jac}(C_5/\langle \tau \rangle),$$

where

$$\mathbb{F}_4(C_5/\langle \sigma\tau \rangle) = \mathbb{F}_4(x_1, x_2, x_3, u_0),$$

$$\mathbb{F}_4(C_5/\langle \tau \rangle) = \mathbb{F}_4(x_1, x_2, x_3, u_1).$$

where u_0 and u_1 are roots of polynomials

$$T^2 + T + \left(\frac{x_3^2}{x_3 + 1}\right)\left(\frac{x_3^2}{1 + \gamma^2 x_3^2}\right),$$

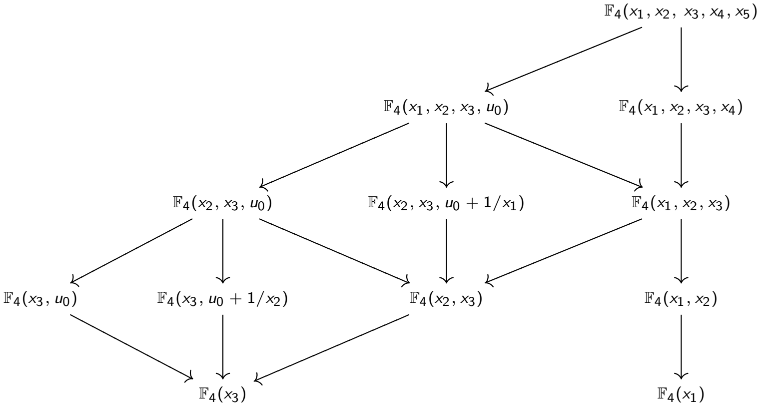
and

$$T^2 + T + \left(\frac{x_3^2}{x_3 + 1}\right)\left(\frac{x_3^2}{1 + \gamma^2 x_3^2 + x_3^2}\right),$$

respectively.

The L-polynomial of T_5

Therefore we have the following diagram of extensions of degree 2:



The L-polynomial of T_5

Therefore

$$\mathrm{L}_{\mathrm{T}_5}(\mathrm{L}_{\mathrm{T}_3})^2 = \mathrm{L}_{\mathbb{F}_4(x_1,x_2,x_3,u_0)}\mathrm{L}_{\mathbb{F}_4(x_1,x_2,x_3,x_4)}\mathrm{L}_{\mathbb{F}_4(x_1,x_2,x_3,u_1)},$$
$$\mathrm{L}_{\mathbb{F}_4(x_1,x_2,x_3,u_0)}(\mathrm{L}_{\mathbb{F}_4(x_2,x_3)})^2 = \mathrm{L}_{\mathbb{F}_4(x_2,x_3,u_0)}\mathrm{L}_{\mathbb{F}_4(x_1,x_2,x_3)}\mathrm{L}_{\mathbb{F}_4(x_2,x_3,u_0+1/x_1)}.$$

From previous step we know that

$$\mathrm{L}_{\mathrm{T}_3}(T) = (1+3T+4T^4)^3$$
$$\mathrm{L}_{\mathrm{T}_4}(T) = (1-T+4T^2)^2(1+3T+4T^2)^7.$$

So in order to compute $\mathrm{L}_{\mathrm{T}_5}$ we need to compute $\mathrm{L}_{\mathbb{F}_4(x_2,x_3,u_0)}$ and $\mathrm{L}_{\mathbb{F}_4(x_2,x_3,u_0+1/x_1)}$.
Using the computer system Magma we compute these polynomials and hence

$$\mathrm{L}_{\mathrm{T}_5}(T) = (1-T+4T^2)^4(1+3T+4T^2)^{11}$$
$$(1+T+4T^2)^2(1+2T+T^2+8T^3+16T^4)^2.$$

Recall that, if T is a function field, $\mathrm{Pic}^0(\mathrm{T})$ is isomorphic to the Jacobian of the curve corresponding to T. Let u be a root of a polynomial $T^2 + T + \frac{x_n^4}{(x_n+1)(1+\gamma^2 x_n^2)}$, then we set

$$F_n := \mathbb{F}_4(x_1, \ldots, x_n, u),$$
$$X_n := \mathrm{Pic}^0(\mathbb{F}_4(x_1, \ldots, x_n, u)),$$
$$F_{n,1} := \mathbb{F}_4(x_2, \ldots, x_n, u + 1/x_1),$$
$$X_{n,1} := \mathrm{Pic}^0(\mathbb{F}_4(x_2, \ldots, x_n, u + 1/x_1)),$$
$$\mathrm{J}_n := \mathrm{Pic}^0(\mathrm{T}_n) \cong \mathrm{Jac}(C_n).$$

Recurrence relations and the general zeta function

The isomorphisms and isogenies of abelian varieties for any $m \geq 1$:

1. $X_n \cong \mathrm{Pic}^0(\mathbb{F}_4(x_m, \ldots, x_{m+n-1}, w))$, where w is a root of a polynomial $T^2 + T + \dfrac{x^4_{n+m-1}}{(x_{n+m-1}+1)(1+\gamma^2 x_n^2)}$,

Recurrence relations and the general zeta function

The isomorphisms and isogenies of abelian varieties for any $m \geq 1$:

1. $X_n \cong \mathrm{Pic}^0(\mathbb{F}_4(x_m, \ldots, x_{m+n-1}, w))$, where w is a root of a polynomial $T^2 + T + \dfrac{x_{n+m-1}^4}{(x_{n+m-1}+1)(1+\gamma^2 x_n^2)}$,
2. $X_n \sim \mathrm{Pic}^0(\mathbb{F}_4(x_m, \ldots, x_{m+n-1}, t))$, where t is a root of a polynomial $T^2 + T + \dfrac{x_{n+m-1}^4}{(x_{n+m-1}+1)(1+(\gamma+1)^2 x_n^2)}$,

Recurrence relations and the general zeta function

The isomorphisms and isogenies of abelian varieties for any $m \geq 1$:

1. $X_n \cong \mathrm{Pic}^0(\mathbb{F}_4(x_m, \ldots, x_{m+n-1}, w))$, where w is a root of a polynomial $T^2 + T + \dfrac{x_{n+m-1}^4}{(x_{n+m-1}+1)(1+\gamma^2 x_n^2)}$,
2. $X_n \sim \mathrm{Pic}^0(\mathbb{F}_4(x_m, \ldots, x_{m+n-1}, t))$, where t is a root of a polynomial $T^2 + T + \dfrac{x_{n+m-1}^4}{(x_{n+m-1}+1)(1+(\gamma+1)^2 x_n^2)}$,
3. $X_{n,1} \cong \mathrm{Pic}^0(\mathbb{F}_4(x_{m+1}, \ldots, x_{m+n-1}, w + 1/x_m))$,

The isomorphisms and isogenies of abelian varieties for any $m \geq 1$:

1. $X_n \cong \mathrm{Pic}^0(\mathbb{F}_4(x_m, \ldots, x_{m+n-1}, w))$, where w is a root of a polynomial $T^2 + T + \frac{x_{n+m-1}^4}{(x_{n+m-1}+1)(1+\gamma^2 x_n^2)}$,
2. $X_n \sim \mathrm{Pic}^0(\mathbb{F}_4(x_m, \ldots, x_{m+n-1}, t))$, where t is a root of a polynomial $T^2 + T + \frac{x_{n+m-1}^4}{(x_{n+m-1}+1)(1+(\gamma+1)^2 x_n^2)}$,
3. $X_{n,1} \cong \mathrm{Pic}^0(\mathbb{F}_4(x_{m+1}, \ldots, x_{m+n-1}, w + 1/x_m))$,
4. $X_{n,1} \sim \mathrm{Pic}^0(\mathbb{F}_4(x_{m+1}, \ldots, x_{m+n-1}, t + 1/x_m))$,

Recurrence relations and the general zeta function

The isomorphisms and isogenies of abelian varieties for any $m \geq 1$:

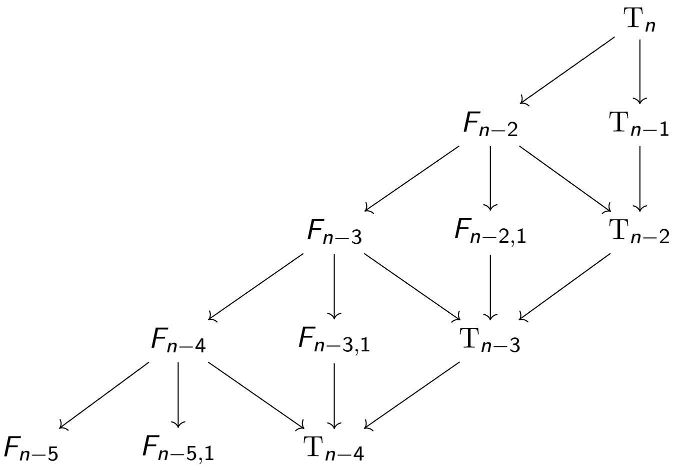
1. $X_n \cong \mathrm{Pic}^0(\mathbb{F}_4(x_m, \ldots, x_{m+n-1}, w))$, where w is a root of a polynomial $T^2 + T + \dfrac{x_{n+m-1}^4}{(x_{n+m-1}+1)(1+\gamma^2 x_n^2)}$,
2. $X_n \sim \mathrm{Pic}^0(\mathbb{F}_4(x_m, \ldots, x_{m+n-1}, t))$, where t is a root of a polynomial $T^2 + T + \dfrac{x_{n+m-1}^4}{(x_{n+m-1}+1)(1+(\gamma+1)^2 x_n^2)}$,
3. $X_{n,1} \cong \mathrm{Pic}^0(\mathbb{F}_4(x_{m+1}, \ldots, x_{m+n-1}, w + 1/x_m))$,
4. $X_{n,1} \sim \mathrm{Pic}^0(\mathbb{F}_4(x_{m+1}, \ldots, x_{m+n-1}, t + 1/x_m))$,
5. $\mathrm{J}_n \cong \mathrm{Pic}^0(\mathbb{F}_4(x_m, \ldots, x_{m+n-1}))$, with $n \geq 1$.

The isomorphisms and isogenies of abelian varieties for any $m \geq 1$:

1. $X_n \cong \mathrm{Pic}^0(\mathbb{F}_4(x_m, \dots, x_{m+n-1}, w))$, where w is a root of a polynomial $T^2 + T + \dfrac{x_{n+m-1}^4}{(x_{n+m-1}+1)(1+\gamma^2 x_n^2)}$,
2. $X_n \sim \mathrm{Pic}^0(\mathbb{F}_4(x_m, \dots, x_{m+n-1}, t))$, where t is a root of a polynomial $T^2 + T + \dfrac{x_{n+m-1}^4}{(x_{n+m-1}+1)(1+(\gamma+1)^2 x_n^2)}$,
3. $X_{n,1} \cong \mathrm{Pic}^0(\mathbb{F}_4(x_{m+1}, \dots, x_{m+n-1}, w + 1/x_m))$,
4. $X_{n,1} \sim \mathrm{Pic}^0(\mathbb{F}_4(x_{m+1}, \dots, x_{m+n-1}, t + 1/x_m))$,
5. $\mathrm{J}_n \cong \mathrm{Pic}^0(\mathbb{F}_4(x_m, \dots, x_{m+n-1}))$, with $n \geq 1$.
6. Owing to an inclusion $\mathbb{F}_4(x_2, \dots, x_n) \subset \mathbb{F}_4(x_2, \dots, x_n, u + 1/x_1)$ there exist an isogeny $X_{n,1} \sim \mathrm{J}_{n-1} \times \mathrm{Y}_{n,1}$, where $\mathrm{Y}_{n,1}$ is an abelian variety.

Recurrence relations and the general zeta function

up to isomorphism, diagram of extensions of degree 2.



Theorem

If $n \geq 3$ then there exists the following isogeny

$$X_n \sim \mathrm{J}_n \times X_1 \times X_{2,1} \times \mathrm{Y}_{3,1} \times \ldots \times \mathrm{Y}_{n,1}.$$

Therefore

Corollary

If $n \geq 5$ then there are an isogenies

$$\mathrm{J}_n \sim X_1^{2n-3} \times X_{2,1}^{2n-6} \times \mathrm{Y}_{3,1}^{2n-8} \times \cdots \times \mathrm{Y}_{n-2,1}^{2}$$

Decomposition of $\mathrm{Pic}^0(\mathrm{T}_n)$ and the L-polynomial of T_n.

Corollary

The L-polynomial of the function field T_n has the following factorization

$$\mathrm{L}_{\mathrm{T}_n} = \mathrm{L}_{X_1}^{2n-3} \times \mathrm{L}_{X_{2,1}}^{2n-6} \times \mathrm{L}_{\mathrm{Y}_{3,1}}^{2n-8} \times \cdots \times \mathrm{L}_{\mathrm{Y}_{n-2,1}}^{2},$$

or more precisely

$$\mathrm{L}_{\mathrm{T}_n} = (T^2 + T + 4)^{2n-8}(T^2 + 3T + 4)^{12n-49}(T^2 - T + 4)^{6n-26}$$
$$(T^4 + 2T^3 + T^2 + 8T + 16)^{6n-24}$$
$$(T^6 + T^5 - T^4 + 3T^3 - 4T^2 + 16T + 64)^{2n-10}\mathrm{L}_{Y_{5,1}}^{2n-12} \cdots \mathrm{L}_{Y_{n-2,1}}^{2}$$

The order of the finite group

$$\#\mathrm{Pic}^0(\mathrm{T}_n)(\mathbb{F}_4) = 2^{58n-243}3^{2n-8}5^{2n-10}\mathrm{L}_{Y_{5,1}}^{2n-12}(1)\ldots\mathrm{L}_{Y_{n-2,1}}^{2}(1).$$

Dimension of $Y_{n,1}$

A crucial role in the computation of the Zeta function of T_{n+2} is the Zeta function of the factor $Y_{n,1}$.

Theorem

$$\dim(Y_{n,1}) = \begin{cases} 2^{n-1}, & \text{if } n \text{ is even} \\ 2^{n-1} - 2^{(n-3)/2}, & \text{if } n \text{ is odd.} \end{cases}$$

As a corollary we get the degree of the characteristic polynomial of Frobenius endomorphism of an abelian variety $Y_{n,1}$.

Corollary

Let $\mathrm{L}_{Y_{n,1}}$ be the L*-polynomial of an abelian variety $Y_{n,1}$. Then*

$$\deg(\mathrm{L}_{Y_{n,1}}) = \begin{cases} 2^{n}, & \text{if } n \text{ is even} \\ 2^{n} - 2^{(n-1)/2}, & \text{if } n \text{ is odd.} \end{cases}$$

The Tower is Ordinary

We prove that J_m is ordinary by showing that the p-rank is equal to the genus of $\tilde{\mathrm{T}}_n$, where $\tilde{\mathrm{T}}_n$ is a Galois closure of T_n over T_1. We use the Deuring-Shafaravich formula, which states that if E/F is a finite Galois extension of function fields in characteristic p, and the Galois group is a p-group, then

$$r_p(E) - 1 = [E : F](r_p(F) - 1) + \sum_P (e(P) - 1)$$

where $r_p(E)$ denotes the p-rank of E, and $e(P)$ denotes the ramification index.

We apply this to the tower $\tilde{\mathrm{T}}_n$, where is it known that the Galois group of $\tilde{\mathrm{T}}_n/\tilde{\mathrm{T}}_1$ is a p-group and

$$g(\tilde{\mathrm{T}}_n) = [\tilde{\mathrm{T}}_n : \mathrm{T}_1](p - p^{3-n} - p^{2-n}) + 1.$$

Theorem

We have

$$r_p(\tilde{\mathrm{T}}_n) = [\tilde{\mathrm{T}}_n : \mathrm{T}_1](p - p^{3-n} - p^{2-n}) + 1.$$

In particular, $\tilde{\mathrm{T}}_n$ is ordinary.

Corollary

The second Garcia-Stichtenoth tower is ordinary.

Thank you for your attention!