On the Zeta function of the generalized Suzuki curve

HERIVELTO BORGES [1] **AND MARIANA COUTINHO** [2]

1 Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo
2 Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas

ABSTRACT

Let p be a prime number and, for any $t \geqslant 1$, consider $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ the nonsingular model defined over $\mathbb{F}_q$ of the projective absolutely irreducible plane algebraic curve given in affine coordinates by

$$Y^q - Y = X^{q_0}(X^q - X),$$

where $q_0 = p^t$ and $q = p^{2t-1}$. For p even, $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ is the so-called Deligne-Lusztig curve associated with the Suzuki group, which has remarkable properties, for instance its large automorphism group and its property of being $\mathbb{F}_{q^4}$-maximal. In this work, we address the study of the L-polynomial of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ for p an odd prime number.

Context and notation

Algebraic curves over finite fields is a significant topic of research, in particular because of its connection with other areas of mathematics such as finite geometry, coding theory, cryptography, and number theory.

Let q be a power of the prime number p.

For a (projective, nonsingular, geometrically irreducible, algebraic) curve $\mathcal{Y}$ of genus g defined over the finite field $\mathbb{F}_q$, consider the problem of determining the number $\mathrm{N}_q(\mathcal{Y})$ of $\mathbb{F}_q$-rational points on $\mathcal{Y}$.

Although in such a degree of generality this task is far from to be reached, some effective bounds for this number can be found in the literature. A remarkable example is the Hasse-Weil bound

$$|\mathrm{N}_q(\mathcal{Y}) - (q+1)| \leqslant 2gq^{1/2}.$$

Definition 1. *Curves attaining the previous upper (resp. lower) bound are called $\mathbb{F}_q$-maximal (resp. $\mathbb{F}_q$-minimal).*

The Suzuki curve

For $p = 2$, an important example of a maximal curve is the Deligne-Lusztig curve associated to the Suzuki group $\mathrm{Sz}(q)$ (see (2), (6), (7)), here for simplicity called the Suzuki curve, which is the nonsingular model $\mathcal{Y}_\mathcal{S}$ defined over $\mathbb{F}_q$ of the plane curve

$$\mathcal{S} : Y^q - Y = X^{q_0}(X^q - X), \tag{1}$$

where $q_0 = 2^t$, $q = 2^{2t-1}$, and $t \geqslant 2$.

Indeed, in (6, Proposition 4.3), together with the expression for the Zeta function of $\mathcal{Y}_\mathcal{S}$, the explicit formula for the number of rational points on $\mathcal{Y}_\mathcal{S}$ shows that it is $\mathbb{F}_{q^4}$-maximal.

The Suzuki curve is optimal in the sense that its number of $\mathbb{F}_q$-rational points coincides with the maximum number of $\mathbb{F}_q$-rational points that a curve of its genus can have (see (7, Proposition 2.1)). Moreover, in (4, Theorem 5.1), it is shown that this curve can be characterized by its genus and number of $\mathbb{F}_q$-rational points.

In addition to its maximality and optimality properties, the Suzuki curve is also known for its large automorphism group. Specifically, it is one of the four examples of curves of genus $g \geqslant 2$ having an automorphism group of size greater than or equal to $8g^3$ (see (8), (9, Theorem 11.127)).

The generalized Suzuki curve

Let $p > 2$, $q_0 = p^t$ and $q = p^m$, where m, t are positive integers satisfying the relation $m = 2t - 1$.

If $\mathcal{G}_\mathcal{S}$ is the projective geometrically irreducible (see (3)) plane curve defined over $\mathbb{F}_q$ given in affine coordinates by

$$\mathcal{G}_\mathcal{S} : Y^q - Y = X^{q_0}(X^q - X), \tag{2}$$

then let $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ be its nonsingular model defined over $\mathbb{F}_q$, which is called here the generalized Suzuki curve.

Main results

The objective of this work is to investigate the number of $\mathbb{F}_{q^n}$-rational points on $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$. As a consequence, the L-polynomial over $\mathbb{F}_q$ of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ is recovered.

The L-polynomial of a curve $\mathcal{Y}$ defined over $\mathbb{F}_q$ encodes information on the order of the group $\mathrm{Pic}_0(\mathbb{F}_q(\mathcal{Y}))$, the zero-degree $\mathbb{F}_q$-divisor class group. Using this fact, some constructions of curves with many rational points are presented in (13). Moreover, considering the $\mathbb{F}_q$-Frobenius endomorphism Φ on the Jacobian variety of $\mathcal{Y}$, then the characteristic polynomial of Φ is described exactly by the reciprocal of the L-polynomial of $\mathcal{Y}$ over $\mathbb{F}_q$, and from its factorization the degree of the Frobenius linear series on $\mathcal{Y}$ is obtained. For further details on this topic, see (9, Sections 9.7 and 9.8).

Our main results are the following.

Theorem 1. *If g denotes the genus of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$, then the number $\mathrm{N}_{q^n}(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$ of $\mathbb{F}_{q^n}$-rational points on $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ is described as follows.*
1. *If $p \mid n$, then*

$$\mathrm{N}_{q^n}(\mathcal{X}_{\mathcal{G}_\mathcal{S}}) = \begin{cases} q^n + 1, \text{ if } n \text{ is odd} \\ q^n + 1 - 2gq^{n/2}, \text{ if } n \text{ is even and } p \equiv 1 \pmod 4 \\ q^n + 1 - 2gq^{n/2}, \text{ if } n \equiv 0 \pmod 4 \text{ and } p \equiv 3 \pmod 4 \\ q^n + 1 + 2gq^{n/2}, \text{ if } n \equiv 2 \pmod 4 \text{ and } p \equiv 3 \pmod 4. \end{cases}$$

2. *If $p \nmid n$, then*

$$\mathrm{N}_{q^n}(\mathcal{X}_{\mathcal{G}_\mathcal{S}}) = \begin{cases} q^n + 1, \text{ if } n \text{ is even} \\ q^n + 1 + 2gq^{n/2}p^{-1/2}\left(\dfrac{(-1)^{(n-1)/2}n}{p}\right), \text{ if } n \text{ is odd} \end{cases},$$

where $\left(\frac{*}{p}\right)$ is the Legendre symbol.

We point out here that for $n = 1$, the number $\mathrm{N}_{q^n}(\mathcal{X}_{\mathcal{G}_\mathcal{S}})$ was already studied in (11) in connection with geometric Goppa codes. Also, for $p = 3$ and considering (5, Proposition 4.2), the curve $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ is $\mathbb{F}_q$-covered by the so-called Ree curve, and then the information on its maximality given by Theorem 1 could be recovered by Serre's result (see (1)).

Now, define

$$\tilde{p}^{1/2} := \begin{cases} p^{1/2}, & \text{if } p \equiv 1 \pmod 4 \\ \mathbf{i}p^{1/2}, & \text{if } p \equiv 3 \pmod 4 \end{cases}. \tag{3}$$

Theorem 2. *If g denotes the genus of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ and $\mathcal{M}_p(T)$ is the minimal polynomial of $-\zeta_p/\tilde{p}^{1/2}$ over $\mathbb{Q}$, where ζ_p is the primitive p-th root of unity $\mathbf{e}^{\frac{2\pi\mathbf{i}}{p}}$, then the L-polynomial $L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}}(T)$ of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ over $\mathbb{F}_q$ is given by*

$$L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}}(T) = \left(p^{p-1}((-1)^{\frac{p+1}{2}} + qT^2) \cdot \mathcal{M}_p(p^{t-1}T)^2\right)^{\frac{g}{p}}.$$

An application of Theorem 2

Based on (13), let $L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_{q^n}}(T)$ be the L-polynomial of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ over $\mathbb{F}_{q^n}$, where $L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_q}(T) = L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}}(T)$, let $J_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}}$ be the Jacobian variety of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$, and consider $J_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}}(\mathbb{F}_{q^n})$ the group of $\mathbb{F}_{q^n}$-rational points on $J_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}}$.

The following result relates the L-polynomial of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ over $\mathbb{F}_{q^n}$ and the cardinality of $J_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}}(\mathbb{F}_{q^n})$.

Theorem 3 (9, Theorem 9.70)**.** $\#J_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}}(\mathbb{F}_{q^n}) = L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_{q^n}}(1)$.

As a consequence, we have the lemma below.

Lemma 4. *The subgroup generated by the $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ is a proper subgroup of $J_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}}(\mathbb{F}_{q^2})$.*

Therefore, from the proof of the main result of (13), the following holds.

Proposition 5. *For each divisor i of $L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}/\mathbb{F}_{q^2}}(1)/L_{\mathcal{X}_{\mathcal{G}_\mathcal{S}}}(1)$ there exists an étale cover of $\mathcal{X}_{\mathcal{G}_\mathcal{S}}$ of degree i with at least $i(q^2+1)$ rational points over $\mathbb{F}_{q^2}$ and genus $i(g-1)+1$.*

Acknowledgments

The first author was supported by FAPESP (Brazil), grant 2017/04681-3. The second author was partially supported by CAPES (Brazil), grant 1501502, CNPq (Brazil), grant 154359/2016-5, and FAPESP (Brazil), grant 2018/23839-0.

Bibliography

(1) AUBRY, Y.; PERRET, M. Divisibility of zeta functions of curves in a covering. *Archiv der Mathematik*, v. 82, p. 205–213, 2004.

(2) DELIGNE, P.; LUSZTIG, G. Representations of reductive groups over finite fields. *Annals of Mathematics*, v. 103, p. 103–161, 1976.

(3) DEOLALIKAR, V. Determining irreducibility and ramification groups for an additive extension of the rational function fields. *Journal of Number Theory*, v. 97, p.269–286, 2002.

(4) FUHRMANN, R.; TORRES, F. On Weierstrass points and optimal curves. *Supplemento ai Rendiconti del Circolo matematico di Palermo*, v. 51, p. 25–46, 1998.

(5) GARCIA, A.; STICHTENOTH, H. Elementary abelian p-extensions of algebraic function fields. *Manuscripta Mathematica*, v. 72, p. 67–79, 1991.

(6) HANSEN, J. P. Deligne-Lusztig varieties and group codes. In: STICHTENOTH, H.; TSFASMAN, M. A. (Eds.) *Coding Theory and Algebraic Geometry: Proceedings of the International Workshop held in Luminy, France, June 17-21, 1991*. Berlin, Heidelberg: Springer-Verlag, 1992. p. 63–81.

(7) HANSEN, J. P.; STICHTENOTH, H. Group codes on certain algebraic curves with many rational points. *Applicable Algebra in Engineering, Communication and Computing*, v. 1, p. 67–77, 1990.

(8) HENN, H. W. Funktionenkörper mit groβer Automorphismengruppe. *Journal für die reine und angewandte Mathematik*, v. 302, p. 96–115, 1978.

(9) HIRSCHFELD, J. W. P.; KORCHMÁROS, G.; TORRES, F. *Algebraic Curves over a Finite Field*. Princeton: Princeton University Press, 2008.

(10) MCGUIRE, G.; YILMAZ, E. On the zeta functions of supersingular curves. *Finite Fields and Their Applications*, v. 54, p. 65–79, 2018.

(11) PEDERSEN, J. P.; SØRENSEN, A. B. Codes from certain Algebraic Function Fields with many Rational Places. *Mat-Report 1990-11*, Technical University of Denmark.

(12) TORRES, F. The approach of Stöhr-Voloch to the Hasse-Weil bound with applications to optimal curves and plane arcs. `https://arxiv.org/abs/math/0011091`, 2000.

(13) VOLOCH, J. F. Jacobians of curves over finite fields. *Rocky Mountain Journal of Mathematics*, v. 30, p. 755–759, 2000.