PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9939(XX)0000-0

THE a-NUMBERS OF JACOBIANS OF SUZUKI CURVES

HOLLEY FRIEDLANDER, DEREK GARTON, BETH MALMSKOG, RACHEL PRIES, AND COLIN WEIR

Abstract. For $m \in \mathbb{N}$, let S_m be the Suzuki curve defined over $\mathbb{F}_{2^{2m+1}}$. It is well-known that S_m is supersingular, but the p-torsion group scheme of its Jacobian is not known. The a-number is an invariant of the isomorphism class of the p-torsion group scheme. In this paper, we compute a closed formula for the a-number of S_m using the action of the Cartier operator on $H^0(S_m, \Omega^1)$.
Keywords: Suzuki curve, maximal curve, Jacobian, p-torsion, a-number.

1. Introduction

Let $m \in \mathbb{N}$, $q = 2^{2m+1}$, and $q_0 = 2^m$. The *Suzuki curve* $\mathcal{S}_m \subset \mathbb{P}^2$ is defined over $\mathbb{F}_q$ by the homogeneous equation:

$$W^{q_0}(Z^q + ZW^{q-1}) = Y^{q_0}(Y^q + YW^{q-1}).$$

This curve is smooth and irreducible with genus $g = q_0(q-1)$ and it has exactly one point at infinity [8, Proposition 1.1]. The number of points on the Suzuki curve over $\mathbb{F}_q$ is $\#S_m(\mathbb{F}_q) = q^2 + 1$; this number is optimal in that it reaches Serre's improvement to the Hasse-Weil bound [8, Proposition 2.1].

In fact, S_m is the unique $\mathbb{F}_q$-optimal curve of genus g [2]. This shows that S_m is the Deligne-Lusztig variety of dimension 1 associated with the group $Sz(q) = {}^2B_2(q)$ [7, Proposition 4.3]. The curve S_m has the Suzuki group $Sz(q)$ as its automorphism group; the order of $Sz(q)$ is $q^2(q-1)(q^2+1)$ which is very large compared with g. Because of the large number of rational points relative to their genus, the Suzuki curves provide good examples of Goppa codes [4, Section 4.3], [5], [8].

The L-polynomial of S_m is $(1 + \sqrt{2q}t + qt^2)^g$ [7, Proposition 4.3]. It follows that S_m is supersingular for each $m \in \mathbb{N}$. This fact implies that the Jacobian $\mathrm{Jac}(S_m)$ is isogenous to a product of supersingular elliptic curves and that $\mathrm{Jac}(S_m)$ has no 2-torsion points over $\overline{\mathbb{F}}_2$. However, there are still open questions about $\mathrm{Jac}(S_m)$. In this paper, we address one of these by computing a closed formula for the a-number of $\mathrm{Jac}(S_m)$.

The a-number is an invariant of the 2-torsion group scheme $\mathrm{Jac}(S_m)[2]$. Specifically, if α_2 denotes the kernel of Frobenius on the additive group $\mathbb{G}_a$, then the a-number of S_m is $a(m) = \dim_{\overline{\mathbb{F}}_2} \mathrm{Hom}(\alpha_2, \mathrm{Jac}(S_m)[2])$. It equals the dimension of the intersection of $\mathrm{Ker}(F)$ and $\mathrm{Ker}(V)$ on the Dieudonné module of $\mathrm{Jac}(S_m)[2]$. Having a supersingular Newton polygon places constraints upon the a-number but does not determine it. The a-number also gives partial information about the decomposition of $\mathrm{Jac}(S_m)$ into indecomposable principally polarized abelian varieties, see Lemma 5.2, and about the Ekedahl-Oort type of $\mathrm{Jac}(S_m)[2]$, see Section 5.

1991 *Mathematics Subject Classification.* Primary 11G20, 14H40; Secondary 14G50.

In Section 4, we prove that the a-number of S_m is $a(m) = q_0(q_0+1)(2q_0+1)/6$, see Theorem 4.1. The proof uses the action of the Cartier operator on $H^0(S_m, \Omega^1)$ as computed in Section 3.

Author Pries was partially supported by NSF grant DMS-11-01712. We would like to thank the NSF for sponsoring the research workshop for graduate students at Colorado State University in June 2011 where the work on this project was initiated. We would like to thank Amy Ksir and the other workshop participants for their insights and the referee for the quick report and helpful comments.

2. The a-number

Suppose A is a principally polarized abelian variety of dimension g defined over an algebraically closed field k of characteristic $p > 0$. For example, A could be the Jacobian of a k-curve of genus g. Consider the multiplication-by-p morphism $[p] : A \to A$ which is a finite flat morphism of degree p^{2g}. It factors as $[p] = V \circ F$. Here, $F : A \to A^{(p)}$ is the relative Frobenius morphism coming from the p-power map on the structure sheaf; it is purely inseparable of degree p^g. The Verschiebung morphism $V : A^{(p)} \to A$ is the dual of F.

The kernel of $[p]$ is $A[p]$, the p-torsion of A, which is a quasi-polarized BT_1 group scheme. In other words, it is a quasi-polarized finite commutative group scheme annihilated by p, again having morphisms F and V. The rank of $A[p]$ is p^{2g}. These group schemes were classified independently by Kraft (unpublished) [10] and by Oort [13]. A complete description of this topic can be found in [12] or [13].

Two invariants of (the p-torsion of) an abelian variety are the p-rank and a-number. The *p-rank* of A is $r(A) = \dim_{\mathbb{F}_p}(\mathrm{Hom}(\mu_p, A[p]))$, where μ_p is the kernel of Frobenius on the multiplicative group $\mathbb{G}_m$. Then $p^{r(A)}$ is the cardinality of $A[p]\left(\overline{\mathbb{F}}_p\right)$. The *$a$-number* of A is $a(A) = \dim_k(\mathrm{Hom}(\alpha_p, A[p]))$, where α_p is the kernel of Frobenius on the additive group $\mathbb{G}_a$. It is well-known that $1 \leq a(A) + r(A) \leq g$. Another definition for the a-number is

$$a(A) = \dim_{\mathbb{F}_p}(\mathrm{Ker}(F) \cap \mathrm{Ker}(V)).$$

If X is a (smooth, projective, connected) k-curve, then the a-number of $A = \mathrm{Jac}(X)$ equals the dimension of the kernel of the Cartier operator $\mathcal{C}$ on $H^0(X, \Omega^1)$ [11, 5.2.8]. The reason for this is that the action of $\mathcal{C}$ on $H^0(X, \Omega^1)$ is the same as the action of V on $V\mathrm{Jac}(X)[p]$. This is the property that we use to calculate the a-number $a(m)$ of the Jacobian of the Suzuki curve S_m.

3. Regular 1-forms for the Suzuki curves

In this section, we compute the action of the Cartier operator on the vector space of regular 1-forms for the Suzuki curves.

3.1. **Geometry of the Suzuki curves.** Let $m \in \mathbb{N}$, $q = 2^{2m+1}$, and $q_0 = 2^m$. Consider the Suzuki curve $\mathcal{S}_m \subset \mathbb{P}^2$ defined over $\mathbb{F}_q$ by the homogeneous equation:

$$W^{q_0}(Z^q + ZW^{q-1}) = Y^{q_0}(Y^q + YW^{q-1}).$$

The curve S_m is smooth and irreducible and has one point P_∞ at infinity (when $W = Y = 0$ and $Z = 1$). Consider the irreducible affine model of S_m defined by the equation

$$z^q + z = y^{q_0}(y^q + y) \tag{3.1}$$

where $y := Y/W$ and $z := Z/W$.

The following result is well-known, see e.g., [8, Proposition 1.1]. We include an alternative proof that illustrates the geometry of some of the quotient curves of S_m and an important point about the a-number.

Lemma 3.1. *The curve S_m has genus $g = q_0(q-1)$.*

Proof. The set $\mathbb{F}_q^* = \{\mu_1, \ldots, \mu_{q-1}\}$ can be viewed as a set of representatives for the $q-1$ cosets of $\mathbb{F}_2^*$ in $\mathbb{F}_q^*$. The Suzuki curve has affine equation $z^q - z = f(y)$ where $f(y) = y^{q_0+q} + y^{q_0+1} \in \mathbb{F}_2(y)$. For $1 \le i \le q-1$, let Z_i be the Artin-Schreier curve with equation $z_i^2 - z_i = \mu_i f(y)$. As seen in [3, Proposition 1.2], the set $\{Z_i \to \mathbb{P}^1_y \mid 1 \le i \le q-1\}$ is exactly the set of degree 2 covers $Z \to \mathbb{P}^1_y$ which are quotients of $S_m \to \mathbb{P}^1_y$. By [6, Proposition 3], an application of [9, Theorem C], there is an isogeny

$$\mathrm{Jac}\,(S_m) \sim \oplus_{i=1}^{q-1} \mathrm{Jac}\,(Z_i).$$

By Artin-Schreier theory, $\mu_i f(y)$ can be modified by any polynomial of the form $T^2 - T$ for $T \in \overline{\mathbb{F}}_2[y]$ without changing the $\overline{\mathbb{F}}_2$-isomorphism class of the Artin-Schreier cover $Z_i \to \mathbb{P}^1_y$. Thus Z_i is isomorphic to an Artin-Schreier curve with equation $z_i^2 - z_i = h_i(y)$ for some $h_i(y) \in \overline{\mathbb{F}}_2[y]$ with degree $2q_0 + 1 = \max\{(q_0+q)/q_0, q_0+1\}$. For $1 \le i \le q-1$, the curve Z_i is a $\mathbb{Z}/2$-cover of the projective line branched only at ∞, where it is totally ramified. Moreover, the break in the filtration of higher ramification groups in the lower numbering is at index $\deg(h_i(y)) = 2q_0 + 1$. By [14, VI.4.1], the genus of Z_i is q_0. Thus $g = \dim(\mathrm{Jac}(S_m)) = (q-1)\dim(\mathrm{Jac}(Z_i)) = q_0(q-1)$. □

Remark 3.2. Consider the Artin-Schreier curve $Z_i : z_i^2 - z_i = h_i(y)$ from the proof of Lemma 3.1. By [1, Proposition 3.4], since $\deg(h_i) = 2q_0 + 1 \equiv 1 \bmod 4$, the a-number of Z_i is $q_0/2$. Thus the a-number of $\oplus_{i=1}^{q-1}\mathrm{Jac}(Z_i)$ is $q_0(q-1)/2$, exactly half of the genus of S_m. The fact that $\mathrm{Jac}(S_m)$ is isogenous to $\oplus_{i=1}^{q-1}\mathrm{Jac}(Z_i)$ gives little information about the a-number of S_m since the a-number is not an isogeny invariant.

The Hasse-Weil bound states that a (smooth, projective, connected) curve X of genus g defined over $\mathbb{F}_q$ must satisfy

$$q + 1 - 2g\sqrt{q} \le \#X(\mathbb{F}_q) \le q + 1 + 2g\sqrt{q}.$$

A curve that meets the upper bound is called an $\mathbb{F}_q$-maximal curve.

The number of $\mathbb{F}_q$-points on the Suzuki curve is $\#S_m\,(\mathbb{F}_q) = q^2 + 1$; this means that S_m is not maximal over $\mathbb{F}_q$, but it does have the maximal number of $\mathbb{F}_q$-points possible for a curve of its genus [8, Proposition 2.1]. Analyzing powers of the eigenvalues of Frobenius shows the following.

Lemma 3.3. *The Suzuki curve S_m is $\mathbb{F}_{q^4}$-maximal.*

Proof. The L-polynomial of S_m is $L(S_m, t) = (1 + \sqrt{2q}t + qt^2)^g$ [7, Proposition 4.3]. This factors as $L(S_m, t) = (1 - \alpha t)^g(1 - \overline{\alpha}t)^g$ where $\alpha = q_0(1+i)$. That implies that $\#S_m(\mathbb{F}_{q^4}) = q^4 + 1 - (\alpha^4 + \overline{\alpha}^4)g = q^4 + 1 + 2q^2 g$ which shows that S_m is $\mathbb{F}_{q^4}$-maximal. □

A curve which is maximal over a finite field is supersingular, in that the slopes of the Newton polygon of its L-polynomial all equal $1/2$. Thus S_m is supersingular. The supersingularity condition is equivalent to the condition that $\mathrm{Jac}(S_m)$ is

isogenous to a product of supersingular elliptic curves. A supersingular curve in characteristic 2 has 2-rank 0. This implies, a priori, that the a-number of S_m is at least one.

3.2. **Regular 1-forms.** To compute a basis for the vector space $H^0(S_m, \Omega^1)$ of regular 1-forms on S_m, consider the functions $h_1, h_2 \in \mathbb{F}(S_m)$ given by:

$$h_1 := z^{2q_0} + y^{2q_0+1},$$
$$h_2 := z^{2q_0} y + h_1^{2q_0}.$$

For any $f \in \mathbb{F}(S_m)$, let $v_\infty(f)$ denote the valuation of f at P_∞.

Lemma 3.4. *The functions $y, z, h_1, h_2 \in \mathbb{F}(S_m)$ have no poles except at P_∞ where*

$$v_y := -v_\infty(y) = q, \qquad v_z := -v_\infty(z) = q + q_0,$$
$$v_{h_1} := -v_\infty(h_1) = q + 2q_0, \qquad v_{h_2} := -v_\infty(h_2) = q + 2q_0 + 1.$$

The function $\pi = h_1/h_2$ is a uniformizer at P_∞.

Proof. See [8, Lemma 1.8]. □

The function y is a separating variable so dy is a basis of the 1-dimensional vector space of 1-forms. The next lemma shows that dy is regular.

Lemma 3.5. *The 1-form dy satisfies*

$$v_\infty(dy) = 2g - 2 \quad \textit{and} \quad v_P(dy) = 0$$

for all points $P \in S_m(\overline{\mathbb{F}}_q)$.

Proof. Recall that π is a uniformizer at P_∞. To take the valuation of dy at P_∞, we first rewrite $dy = f(x, y)d\pi$ for some $f(y, z) \in \mathbb{F}_q(y, z)$. Note that

$$d\pi = d\left(\frac{h_1}{h_2}\right) = \frac{h_2\, dh_1 - h_1\, dh_2}{h_2^2} = \frac{h_2\, y^{2q_0} - h_1\, z^{2q_0}}{h_2^2} dy.$$

Since $v_\infty(h_2^2) = -2(q + 2q_0 + 1)$ and

$$\begin{aligned} v_\infty(h_2\, y^{2q_0} - h_1\, z^{2q_0}) &= \min\{-2q_0 v_y - v_{h_2}, -2q_0 v_z - v_{h_1}\} \\ &= -2q_0 v_z - v_{h_1} \\ &= -4q_0^3 - 4q_0^2 - 2q_0, \end{aligned}$$

we see that

$$\begin{aligned} v_\infty(dy) &= v_\infty\left(\frac{h_2^2}{h_2\, y^{2q_0} - h_1\, z^{2q_0}} d\pi\right) \\ &= -2q - 4q_0 - 2 - \left(-4q_0^3 - 4q_0^2 - 2q_0\right) \\ &= 4q_o^3 - 2q_0 - 2 \\ &= 2g - 2. \end{aligned}$$

We next show that dy has no zero or pole at any affine point of S_m. Note that, for any $a \in \overline{\mathbb{F}}_q$, the polynomial $z^q + z + a$ splits into distinct factors in $\overline{\mathbb{F}}_q(z)$, so there are exactly q points of $S_m(\overline{\mathbb{F}}_q)$ lying over any $y_0 \in \mathbb{A}^1_y(\overline{\mathbb{F}}_q)$. Since

$$\left[\overline{\mathbb{F}}_q(y, z) : \overline{\mathbb{F}}_q(y)\right] = q,$$

the $\overline{\mathbb{F}}_q$-Galois cover $S_m \to \mathbb{P}^1_y$ is unramified at all affine points of S_m. Consequently, for any point $P \in S_m(\overline{\mathbb{F}}_q)$ lying over $a \in \mathbb{A}^1_y(\overline{\mathbb{F}}_q)$, we see that $v_P(y-a) = 1$. Thus, $y-a$ is a uniformizer at P and $v_P(dy) = 0$, proving the proposition. □

By Lemma 3.5, finding a basis for $H^0(S_m, \Omega^1)$ is equivalent to finding a basis for $L((dy))$, since $(dy) = (2g-2)P_\infty$ is the canonical divisor. To do this, we make use of the relations:

$$z^2 = yh_1 + h_2, \quad h_1^{q_0} = z + y^{q_0+1}, \quad h_2^{q_0} = h_1 + zy^{q_0}, \tag{3.2}$$

which can be verified by direct substitution, and the following proposition.

Proposition 3.6. [8, Proposition 1.5] *Let SG be the semigroup*

$$\langle q, q+q_0, q+2q_0, q+2q_0+1 \rangle .$$

Then $\#\{n \in SG \mid 0 \le n \le 2g-2\} = g$.

We now have all the required information to find a basis of $H^0(S_m, \Omega^1)$.

Proposition 3.7. *The following set is a basis of $H^0(S_m, \Omega^1)$:*

$$\mathcal{B} := \left\{ y^a z^b h_1^c h_2^d \, dy \;\middle|\; (a,b,c,d) \in \mathcal{E} \right\}$$

where $\mathcal{E}$ is the set of $(a,b,c,d) \subset \mathbb{Z}^4$ satisfying

$$0 \le b \le 1, \quad 0 \le c \le q_0 - 1, \quad 0 \le d \le q_0 - 1,$$
$$av_y + bv_z + cv_{h_1} + dv_{h_2} \le 2g-2.$$

Proof. To prove linear independence, it suffices to prove that all elements in our basis have distinct valuations at P_∞. Suppose $y^a z^b h_1^c h_2^d \, dy \in \mathcal{B}$ and $y^{a'} z^{b'} h_1^{c'} h_2^{d'} \, dy \in \mathcal{B}$ have the same valuation at P_∞; we will show they are equal. Comparing their valuations at P_∞, we must have that

$$(a-a')v_y + (b-b')v_z + (c-c')v_{h_1} + (d-d')v_{h_2} = 0 \tag{3.3}$$

Now consider Equation (3.3) modulo q_0. As q_0 divides v_y, v_z and v_{h_1},

$$(d-d') \equiv 0 \bmod q_0.$$

As $0 \le d, d' < q_0$, it must be the case that $d = d'$. Substituting $d - d' = 0$ into Equation (3.3) and reducing modulo $2q_0$ yields that

$$(b-b')q_0 \equiv 0 \bmod 2q_0.$$

However, as $0 \le b, b' \le 1$, it must also be the case that $b = b'$. Simplifying (3.3) and reducing modulo $q = 2q_o^2$ yields that

$$(c-c')(q-2q_0) = (c-c')2q_0 \equiv 0 \bmod 2q_0^2.$$

Since $0 \le c, c' \le q_0 - 1$, we find that $c = c'$; so $a = a'$ as well.

We claim that the above set also spans $L((dy))$. Clearly the valuations at P_∞ of

$$\left\{ y^a z^b h_1^c h_2^c \mid av_y + bv_z + cv_{h_1} + dv_{h_2} \le 2g-2 \right\}$$

are equal to $\{n \in SG \mid 0 \le n \le 2g-2\}$, which is a set of size g by Proposition 3.6. Rewriting elements of the above set in terms of our basis will not change their valuation at P_∞. Thus we can use the relations in Equation (3.2) to see that $\mathcal{B}$ also contains an element for each of the g possible valuations at P_∞. By the previous paragraphs, each valuation occurs exactly once. By Riemann-Roch, $\ell((dy)) = g$, so $\mathcal{B}$ is a basis. □

3.3. **Action of the Cartier operator.** The (modified) Cartier operator $\mathcal{C}$ is the semi-linear map $\mathcal{C} : H^0(S_m, \Omega^1) \to H^0(S_m, \Omega^1)$ which annihilates exact 1-forms, preserves logarithmic ones, and is p^{-1}-linear. In characteristic 2, the Cartier operator $\mathcal{C}$ acts on 1-forms according to the following properties: (see e.g., [15, Section 2.2.5]).

(1) $\mathcal{C}$ is 1/2-linear; i.e., $\mathcal{C}$ is additive and $\mathcal{C}(f^2\omega) = f\,\mathcal{C}(\omega)$.
(2) $\mathcal{C}(y^j\,dy) = \begin{cases} 0, & \text{if } j \equiv 0 \bmod 2 \\ y^{e-1}\,dy & \text{if } j = 2e-1. \end{cases}$
(3) $\mathcal{C}(\omega) = 0$ if and only if ω is exact; i.e., if and only if $\omega = df$ for some $f \in \mathbb{F}_q(S_m)$.
(4) $\mathcal{C}(\omega) = \omega$ if and only if $\omega = df/f$ for some $f \in \mathbb{F}_q(S_m)$.

Any 1-form $\omega \in H^0(S_m, \Omega^1)$ can be written in the form $\omega = (f^2 + g^2 y)dy$, as $\mathrm{char}(\mathbb{F}_q) = 2$. Then

$$\mathcal{C}((f^2 + g^2 y)dy) = g\,dy. \tag{3.4}$$

By these properties, it is clear that

$$\mathcal{C}(y^{2e_1+r_1} z^{2e_2+r_2} h_1^{2e_3+r_3} h_2^{2e_4+r_4}\,dy) = y^{e_1} z^{e_2} h_1^{e_3} h_2^{e_4}\,\mathcal{C}(y^{r_1} z^{r_2} h_1^{r_3} h_2^{r_4}\,dy). \tag{3.5}$$

Hence to compute the action of $\mathcal{C}$ on $H^0(S_m, \Omega^1)$, we need only compute $\mathcal{C}$ on the 16 monomials in y, z, h_1, h_2 of degree less than or equal to one in each variable. Table 1 shows this action, where each $\mathcal{C}(f\,dy)$ is written in terms of the original basis using the curve Equation (3.1).

TABLE 1

f	$\mathcal{C}(f dy)$
1	0
y	dy
z	$y^{q_0/2}\,dy$
h_1	$y^{q_0}\,dy$
h_2	$\left((yh_1)^{q_0/2} + h_2^{q_0}\right)\,dy$
yz	$h_1^{q_0/2}\,dy$
yh_1	$\left((yh_1)^{q_0/2} + h_2^{q_0}\right)\,dy$
zh_1	$(yh_2)^{q_0/2}\,dy$
zh_2	$(h_1h_2)^{q_0/2}\,dy$
h_1h_2	$(h_1 + zy^{q_0})\,dy$
yzh_1	$\left(y^{q_0/2}z + (h_1h_2)^{q_0/2}\right)\,dy$
yzh_2	$\left(zh_1^{q_0/2} + y^{q_0/2+1}h_2^{q_0/2}\right)\,dy$
zh_1h_2	$\left(zy^{q_0/2}h_2^{q_0/2} + h_1^{q_0/2+1}\right)\,dy$
yh_1h_2	$\left((yh_1)^{q_0/2}z + h_2^{q_0/2}z\right)\,dy$
yzh_1h_2	$\left(y^{q_0/2}h_2 + zh_1^{q_0/2}h_2^{q_0/2}\right)\,dy$

Example 3.8. We illustrate the computation for $zh_1h_2\,dy$. Direct computation yields

$$\begin{aligned}\mathcal{C}\left(zh_1h_2\,dy\right) &= \mathcal{C}\left(zh_1\left(yz^{2q_0}+h_1^{2q_0}\right)\,dy\right)\\ &= z^{q_0}\,\mathcal{C}\left(zyh_1\,dy\right)+h_1^{q_0}\,\mathcal{C}\left(zh_1\,dy\right)\\ &= \left(y^{q_0/2}z^{q_0+1}+h_1^{q_0/2}h_2^{q_0/2}z^{q_0}+h_1^{q_0}y^{q_0/2}h_2^{q_0/2}\right)\,dy.\end{aligned}$$

To write this expression in terms of the original basis, we identify the monomials with the highest pole order at infinity. Since

$$v_\infty(h_1^{q_0/2}h_2^{q_0/2}z^{q_0}) = v_\infty(h_1^{q_0}y^{q_0/2}h_2^{q_0/2}) = -4q_0^3-3q_0^2-q_0/2 < -\left(2g-2\right),$$

these two terms may be simplified. Using Equation 3.2,

$$\begin{aligned}&h_1^{q_0/2}h_2^{q_0/2}z^{q_0}+h_1^{q_0}y^{q_0/2}h_2^{q_0/2}\\ &\qquad = h_1^{q_0/2}h_2^{q_0/2}\left(y^{q_0/2}h_1^{q_0/2}+h_2^{q_0/2}\right)+y^{q_0/2}h_1^{q_0}h_2^{q_0/2} = h_1^{q_0/2}h_2^{q_0}.\end{aligned}$$

The final expression follows by rewriting z^{q_0+1} and $h_2^{q_0}$ in terms of lower order basis elements using Equation (3.2).

Remark 3.9. To compute $\mathcal{C}\left(\omega\right)$ for a general element $\omega\in\mathcal{B}$, simply apply Equation (3.5) and use the table above; in nearly all cases the direct result will again be in terms of the basis $\mathcal{B}$. The only exception is when $\omega = zh_1^{q_0-1}h_2\,dy$. In this case we have:

$$\begin{aligned}\mathcal{C}\left(h_1^{q_0-2}\cdot zh_1h_2\,dy\right) &= h_1^{q_0/2-1}\,\mathcal{C}\left(zh_1h_2\right)\\ &= \left(zy^{q_0/2}h_1^{q_0/2-1}h_2^{q_0/2}+h_1^{q_0}\right)\,dy.\end{aligned}$$

Using Equation (3.2), one can obtain an expression in terms of the original basis.

4. The a-number for Suzuki curves

We now have the tools to compute a closed form formula for the a-number $a(m)$. The calculation amounts to counting lattice points in polytopes in $\mathbb{R}^3$, which is a hard problem in general. In our case, however, the values v_y, v_{h_1}, and v_{h_2} are so similar that the polytopes in question are nearly regular; this makes our counting problem much easier.

Theorem 4.1. *Let $a(m)$ and $g(m)$ be the a-number and genus of S_m respectively. Then*

$$a(m) = \frac{q_0(q_0+1)(2q_0+1)}{6}.$$

In particular,

$$\frac{1}{6} < \frac{a(m)}{g(m)} < \frac{1}{6}+\frac{1}{2^{m+1}}.$$

Proof. Recall from Section 2 that $a(m)$ is the dimension of the kernel of $\mathcal{C}$ on $H^0(S_m,\Omega^1)$. By Equation (3.4), $a(m)$ is the dimension of the vector space of regular 1-forms of the form $f^2\,dy$. Since f^2 can have a pole only at P_∞, and since the order of the pole can be at most $2g-2$, we see that $a(m) = \ell((g-1)P_\infty)$. Moreover, squaring is a homomorphism, so

$$\ell((g-1)P_\infty) = \#\left\{\omega\in\mathcal{B}\mid v_\infty(\omega)\le g-1\right\}.$$

By Section 3, this number is exactly

$$\#\left\{(a,b,c,d) \in \mathcal{E} \mid v_y a + v_z b + v_{h_1} c + v_{h_2} d \leq g-1\right\};$$

here we use the notation $\mathcal{E}$ as we did in Proposition 3.7. Recall that $b \in \{0,1\}$. When $b=0$, we must count $\{(a,c,d) \in \mathbb{N}^3 \mid a+c+d \leq q_0 - 1\}$. This follows from the fact that that

$$q_0 - 1 = \frac{g-1}{v_{h_2}} < \frac{g-1}{v_{h_1}} < \frac{g-1}{v_y} < q_0.$$

For $b=1$, we must count $\{(a,c,d) \in \mathbb{N}^3 \mid a+c+d \leq q_0 - 2\}$ since

$$q_0 - 2 < \frac{g-1-v_z}{v_{h_2}} < \frac{g-1-v_z}{v_{h_1}} < \frac{g-1-v_z}{v_y} < q_0 - 1.$$

Using these two facts, we obtain

$$\begin{aligned} a(m) =& \#\left\{(a,c,d) \in \mathbb{N}^3 \mid a+c+d \leq q_0 - 1\right\} \\ &+ \#\left\{(a,c,d) \in \mathbb{N}^3 \mid a+c+d \leq q_0 - 2\right\} \\ =& \sum_{i=2}^{q_0+1} \binom{i}{2} + \sum_{i=2}^{q_0} \binom{i}{2} \\ =& 1 + \sum_{i=2}^{q_0} \left(\binom{i+1}{2} + \binom{i}{2} \right) \\ =& \sum_{i=1}^{q_0} i^2, \end{aligned}$$

which equals the formula in the first statement.

To prove the second statement, simply note that

$$\frac{1}{6} < \frac{q_0(q_0+1)(2q_0+1)}{6q_0(q-1)} = \frac{1}{6} \cdot \frac{q_0^2 + \frac{3}{2}q_0 + \frac{1}{2}}{q_0^2 - \frac{1}{2}} < \frac{1}{6}\left(1 + \frac{3}{q_0}\right).$$

□

5. Open questions

Here are two open questions about $\mathrm{Jac}(S_m)$.

Question 5.1. What is the decomposition of $\mathrm{Jac}(S_m)$ into indecomposable principally polarized abelian varieties?

Theorem 4.1 gives partial information about Question 5.1, namely an upper bound on the number of factors appearing in the decomposition, because of the following fact.

Lemma 5.2. *Suppose A is a principally polarized abelian variety with p-rank 0 and a-number a. If A decomposes as the direct sum of t principally polarized abelian varieties, then $t \leq a$.*

Proof. Write $A \simeq \oplus_{i=1}^{t} A_i$ where each A_i is a principally polarized abelian variety. For $1 \leq i \leq t$, consider the p-torsion group scheme $A_i[p]$. The a-number of $A_i[p]$ is at least 1 since its p-rank is 0. Thus the a-number of A is at least t. □

To state the second question, we need some more notation.

The Ekedahl-Oort type of a principally polarized abelian variety A over k is defined by the interaction between the Frobenius F and Verschiebung V operators on the p-torsion group scheme $A[p]$. It determines the isomorphism class of $A[p]$ and its invariants such as the a-number. To define the Ekedahl-Oort type, recall that the isomorphism class of a symmetric BT_1 group scheme $\mathbb{G}$ over k can be encapsulated into combinatorial data. This topic can be found in [13]. If $\mathbb{G}$ has rank p^{2g}, then there is a *final filtration* $N_1 \subset N_2 \subset \cdots \subset N_{2g}$ of $\mathbb{G}$ as a k-vector space which is stable under the action of V and F^{-1} such that $i = \dim(N_i)$. The *Ekedahl-Oort type* of $\mathbb{G}$, also called the *final type*, is $\nu = [\nu_1, \ldots, \nu_r]$ where $\nu_i = \dim(V(N_i))$. The Ekedahl-Oort type of $\mathbb{G}$ is canonical, even if the final filtration is not.

There is a restriction $\nu_i \leq \nu_{i+1} \leq \nu_i + 1$ on the final type. Moreover, all sequences satisfying this restriction occur. This implies that there are 2^g isomorphism classes of symmetric BT_1 group schemes of rank p^{2g}. The p-rank is $\max\{i \mid \nu_i = i\}$ and the a-number equals $g - \nu_g$.

Question 5.3. What is the Ekedahl-Oort type of $\mathrm{Jac}(S_m)[2]$? Equivalently, what is the covariant Dieudonné module of $\mathrm{Jac}(S_m)[2]$?

Theorem 4.1 gives partial information about Question 5.3, by limiting the possible final types. For the group scheme $\mathrm{Jac}(S_m)[2]$, the Ekedahl-Oort type satisfies that $\nu_1 = 0$ and $\nu_g = q_0(10q_0+7)(q_0-1)/6$. In particular, $\mathrm{Jac}(S_m)$ is not supersepecial since $a(m) \neq g(m)$. This implies that $\mathrm{Jac}(S_m)$ is not isomorphic to the product of supersingular elliptic curves; it is only isogenous to the product of supersingular elliptic curves.

In the next example, we give some more information about the Ekedahl-Oort type of $\mathrm{Jac}(S_1)[2]$ (the case $m = 1$).

Example 5.4. If $m = 1$ then $q_0 = 2$, $q = 8$, and $g = 14$. By Section 3.3, the image of $\mathcal{C}$ on $H^0(S_m, \Omega^1)$ is spanned by the nine 1-forms

$$\{dy, ydy, h_1dy, y^2dy, yh_1dy, yh_2, (z+y^3)dy, h_1h_2dy, y^2zdy\}.$$

The image of $\mathcal{C}^2$ on $H^0(S_m, \Omega^1)$ is spanned by the four 1-forms

$$\{dy, y^2dy, (z+y^3)dy, (h_1+y^2z)dy\}.$$

Also $\mathcal{C}^3$ trivializes $H^0(S_m, \Omega^1)$. Thus $\nu_1 = \nu_2 = \nu_3 = \nu_4 = 0$, and $\nu_9 = 4$, and $\nu_{14} = 9$. The combinatorial restrictions on the final type imply that $\nu_{10} = 5$, $\nu_{11} = 6$, $\nu_{12} = 7$, and $\nu_{13} = 8$. This leaves only five possibilities for the final type, and thus for the isomorphism class of $\mathrm{Jac}(S_1)[2]$.

References

1. Arsen Elkin and Rachel Pries, *Ekedahl-oort strata of hyperelliptic curves in characteristic 2*, arXiv:1007.1226.
2. Rainer Fuhrmann and Fernando Torres, *On Weierstrass points and optimal curves*, Rend. Circ. Mat. Palermo (2) Suppl. (1998), no. 51, 25–46. MR 1631013 (99e:11081)
3. Arnaldo García and Henning Stichtenoth, *Elementary abelian p-extensions of algebraic function fields*, Manuscripta Math. **72** (1991), no. 1, 67–79. MR 1107453 (92j:11139)
4. Massimo Giulietti and Gábor Korchmáros, *On automorphism groups of certain Goppa codes*, Des. Codes Cryptogr. **47** (2008), no. 1-3, 177–190. MR 2375466 (2009d:94156)
5. Massimo Giulietti, Gábor Korchmáros, and Fernando Torres, *Quotient curves of the Suzuki curve*, Acta Arith. **122** (2006), no. 3, 245–274. MR 2239917 (2007g:11069)

6. Darren Glass and Rachel Pries, *Hyperelliptic curves with prescribed p-torsion*, Manuscripta Math. **117** (2005), no. 3, 299–317. MR 2154252 (2006e:14039)
7. Johan P. Hansen, *Deligne-Lusztig varieties and group codes*, Coding theory and algebraic geometry (Luminy, 1991), Lecture Notes in Math., vol. 1518, Springer, Berlin, 1992, pp. 63–81. MR 1186416 (94e:94024)
8. Johan P. Hansen and Henning Stichtenoth, *Group codes on certain algebraic curves with many rational points*, Appl. Algebra Engrg. Comm. Comput. **1** (1990), no. 1, 67–77. MR 1325513 (96e:94023)
9. E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989), no. 2, 307–327. MR 1000113 (90h:14057)
10. H. Kraft, *Kommutative algebraische p-gruppen (mit anwendungen auf p-divisible gruppen und abelsche varietäten)*, manuscript, University of Bonn, September 1975, 86 pp.
11. K.-Z. Li and F. Oort, *Moduli of supersingular abelian varieties*, Lecture Notes in Mathematics, vol. 1680, Springer-Verlag, Berlin, 1998. MR MR1611305 (99e:14052)
12. B. Moonen, *Group schemes with additional structures and Weyl group cosets*, Moduli of abelian varieties (Texel Island, 1999), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 255–298. MR MR1827024 (2002c:14074)
13. F. Oort, *A stratification of a moduli space of abelian varieties*, Moduli of abelian varieties (Texel Island, 1999), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 345–416. MR 2002b:14055
14. Henning Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR 2464941 (2010d:14034)
15. Michael Tsfasman, Serge Vlăduţ, and Dmitry Nogin, *Algebraic geometric codes: basic notions*, Mathematical Surveys and Monographs, vol. 139, American Mathematical Society, Providence, RI, 2007. MR 2339649 (2009a:94055)

University of Massachusetts–Amherst, Amherst, MA 01003
E-mail address: holleyf@math.umass.edu

University of Wisconsin–Madison, Madison, WI 53706
E-mail address: garton@math.wisc.edu

Wesleyan University, Middletown, CT 06457
E-mail address: emalmskog@wesleyan.edu

Colorado State University, Fort Collins, CO 80521
E-mail address: pries@math.colostate.edu

University of Calgary, Calgary, AB, Canada, T2N 1N4
E-mail address: cjweir@ucalgary.ca