Classification of all Galois subcovers of the Skabelund maximal curves

Beelen, Peter; Landi, Leonardo; Montanucci, Maria

Published in:
Journal of Number Theory

Link to article, DOI:
10.1016/j.jnt.2022.07.008

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

Journal of Number Theory 242 (2023) 46–72

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

Classification of all Galois subcovers of the Skabelund maximal curves

Peter Beelen *, Leonardo Landi, Maria Montanucci

Department of Applied Mathematics and Computer Science, Technical University of Denmark, Matematiktovet 303B, 2800 Kgs. Lyngby, Denmark

ARTICLE INFO

Article history:
Received 27 April 2021
Accepted 20 July 2022
Available online 24 August 2022
Communicated by A. Pal

MSC:
11G20
14H25
14H37

Keywords:
Suzuki and Ree curves
Skabelund maximal curves
Genus spectrum of maximal curves

ABSTRACT

In 2017 Skabelund constructed two new examples of maximal curves $\tilde{\mathcal{S}}_q$ and $\tilde{\mathcal{R}}_q$ as covers of the Suzuki and Ree curves, respectively. The resulting Skabelund curves are analogous to the Giulietti–Korchmáros cover of the Hermitian curve. In this paper a complete characterization of all Galois subcovers of the Skabelund curves $\tilde{\mathcal{S}}_q$ and $\tilde{\mathcal{R}}_q$ is given. Calculating the genera of the corresponding curves, we find new additions to the list of known genera of maximal curves over finite fields.

1. Introduction

Let $\mathbb{F}_{Q^2}$ be a finite field with Q^2 elements where Q is a power of a prime p. For an algebraic (projective, absolutely irreducible, nonsingular) curve $\mathcal{C}$ of genus $g(\mathcal{C})$ over $\mathbb{F}_{Q^2}$, the Hasse–Weil bound states that:

$$N(\mathcal{C}) \leq Q^2 + 1 + 2g(\mathcal{C})Q,$$

* Corresponding author.
E-mail addresses: pabe@dtu.dk (P. Beelen), marimo@dtu.dk (M. Montanucci).

https://doi.org/10.1016/j.jnt.2022.07.008

where $N(\mathcal{C})$ denotes the number of rational points of $\mathcal{C}$. The curve $\mathcal{C}$ is called maximal if $N(\mathcal{C}) = Q^2 + 1 + 2g(\mathcal{C})Q$, that is, if $\mathcal{C}$ has the largest possible number of rational points that it can have according to the value $g(\mathcal{C})$ of its genus. Maximal curves have interesting properties and have also been intensively investigated during the last years for their applications in coding theory. Surveys on maximal curves are found in [18,19,21,23,24] and [34, Chapter 10]; see also [16,17,46].

Important examples of maximal curves are the so-called Deligne–Lusztig curves, namely the Hermitian, Suzuki and Ree curves. All these curves have a large automorphism group when compared with their genus, as they do not satisfy the classical Hurwitz bound $|\mathrm{Aut}(\mathcal{C})| \leq 84(g(\mathcal{C}) - 1)$. Also their automorphism groups are well-studied examples of finite 2-transitive groups, namely the projective unitary group $\mathrm{PGU}(3, q)$, the Suzuki group $\mathrm{Sz}(q)$ and the Ree group $\mathrm{Ree}(q)$, respectively. The Deligne–Lusztig curves have been intensively investigated in the last decades. Among other reasons, such as their connection with class field theory (see [37]) and their applications to coding theory, the interest on this class of maximal curves is motivated by the fact that a subcover of a maximal curve over the same field of definition is maximal by a theorem of Serre [36]. This implies that when given a maximal curve $\mathcal{C}$ over $\mathbb{F}_{Q^2}$ with many automorphisms, computing Galois subcovers corresponding to subgroup H of $\mathrm{Aut}(\mathcal{C})$ gives rise to many examples of maximal curves.

Since all maximal subgroups of $\mathrm{PGU}(3, q)$, $\mathrm{Sz}(q)$ and $\mathrm{Ree}(q)$ are known, subgroups of these and the corresponding Galois subcovers have been studied in various papers, see for example [1,3,11,22,41,43]. Many genera of maximal curves have been obtained in this way, adding to the understanding of the genus spectrum of maximal curves.

In [28] Giulietti and Korchmáros introduced a new maximal curve (known as the GK curve) over finite fields $\mathbb{F}_{q^6}$, which are not subcover of the Hermitian curve over the corresponding field for $q > 2$. Surprisingly, the GK curve was constructed as a Galois cover of the Hermitian function field over $\mathbb{F}_{q^2}$. Considering subcovers of the GK curve, gives rise to new genera of maximal curves. Such examples were found initially in [15,31]. Later, the GK curve was generalized in [20] to a family of maximal curves over finite fields $\mathbb{F}_{q^{2n}}$ with n odd. These maximal curves are often called the Garcia–Güneri–Stichtenoth (GGS) curves. All subgroups of the automorphism groups of these curves were classified in [2], but before that several Galois subcovers were already determined in [32].

Recently a second generalization of the GK curve was discovered [5]. As for the GGS curves, for each odd n a maximal curve K_n was found over $\mathbb{F}_{q^{2n}}$. Though the genus of K_n is equal to that of the corresponding GGS curve, their automorphism groups are different. A preliminary study in [5] already revealed that new genera of maximal curves can be obtained by considering Galois subcovers of K_n. A more detailed study of Galois subcovers of the second generalization of the GK function field was provided in [6].

In [45], Skabelund constructed two Galois covers of the Suzuki and Ree curves, $\tilde{\mathcal{S}}_q$ and $\tilde{\mathcal{R}}_q$, reproducing the way in which the GK curve was constructed as a cover of the Hermitian curve on the two other Deligne–Lusztig curves. The curves $\tilde{\mathcal{S}}_q$ and $\tilde{\mathcal{R}}_q$ can be described as follows.

Table 1
New genera from Theorem 2.11 for $s = 1, 2, 3, 4$.

s	Field	Genus
1	$\mathbb{F}_{2^{12}}$	38
2	$\mathbb{F}_{2^{20}}$	104, 534, 604, 614, 3066
3	$\mathbb{F}_{2^{28}}$	9080
4	$\mathbb{F}_{2^{36}}$	3484, 10420, 129160, 135688, 138736, 138952, 138958, 138970, 1806442, 5141854

Table 2
New genera from Theorem 3.10 for $s = 1$.

s	Field	Genus
1	$\mathbb{F}_{3^{18}}$	12942

For any $s \in \mathbb{N}$, $s \geq 1$, let $q_0 = 2^s$, $q = 2q_0^2 = 2^{2s+1}$ and $m = q - 2q_0 + 1$. The Skabelund curve $\tilde{\mathcal{S}}_q$ is given by $\tilde{\mathcal{S}}_q = \mathbb{F}_{q^4}(x, y, t)$, where

$$\begin{cases} y^q + y = x^{q_0}(x^q + x) \\ t^m = x^q + x. \end{cases}$$

The curve $\tilde{\mathcal{S}}_q$ is maximal over the field $\mathbb{F}_{q^4}$. Its automorphism group is $\mathrm{Aut}(\tilde{\mathcal{S}}_q) = \mathrm{Sz}(q) \times C_m$, see [30].

Similarly, for any $s \in \mathbb{N}$, $s \geq 1$, let $q_0 = 3^s$, $q = 3q_0^2 = 3^{2s+1}$ and $m = q - 3q_0 + 1$. The Skabelund curve $\tilde{\mathcal{R}}_q$ is given by $\tilde{\mathcal{R}}_q = \mathbb{F}_{q^6}(x, y, z, t)$, where

$$\begin{cases} y^q - y = x^{q_0}(x^q - x) \\ z^q - z = x^{2q_0}(x^q - x) \\ t^m = x^q - x. \end{cases}$$

$\tilde{\mathcal{R}}_q$ is maximal over $\mathbb{F}_{q^6}$. Its automorphism group is $\mathrm{Aut}(\tilde{\mathcal{R}}_q) = \mathrm{Ree}(q) \times C_m$, see [30]. A partial description of Galois subcovers of $\tilde{\mathcal{S}}_q$ and $\tilde{\mathcal{R}}_q$ was given in [30] where only subgroups of $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$ (resp. $\mathrm{Aut}(\tilde{\mathcal{R}}_q)$), of type $K \times H$ with $K \leq \mathrm{Sz}(q)$ (resp. $K \leq \mathrm{Ree}(q)$) and $H \leq C_m$ were considered.

In this paper, the complete classification of Galois subcovers of $\tilde{\mathcal{S}}_q$ and $\tilde{\mathcal{R}}_q$ is given. The corresponding genera are computed for all values of q, giving new genera of maximal curves for specific values of q (see Tables 1, 2, and 3). To the best of our knowledge the genera given in these tables are new. We have checked that these values are not contained in and cannot be obtained using results from [1–3,5–12,14,15,22,25–27,29,30,32,40–43]. The paper is organized as follows: in section two, we classify Galois subcovers of $\tilde{\mathcal{S}}_q$, while in section three, we achieve this for $\tilde{\mathcal{R}}_q$.

Table 3
New genera for $s = 1$ from Theorems 3.11 and 3.12.

s	Field	Genus
1	$\mathbb{F}_{3^{18}}$	445, 4393

2. Galois subcovers of $\tilde{\mathcal{S}}_q$

In this section, we complete the study of subcovers, initiated in [30], of $\tilde{\mathcal{S}}_q$ of the form $\tilde{\mathcal{S}}_q/H$, where H is a subgroup of $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$, computing the genus of $\tilde{\mathcal{S}}_q/H$. Throughout the section $s \geq 1$ is a fixed integer, $q_0 := 2^s$, $q := 2q_0^2$ and $m := q - 2q_0 + 1$ unless explicitly stated otherwise. It is well known that $\mathrm{Aut}(\mathcal{S}_q) = \mathrm{Sz}(q)$, where $\mathcal{S}_q$ denotes the Suzuki curve, and it was shown in [30] that $\mathrm{Aut}(\tilde{\mathcal{S}}_q) = \mathrm{Sz}(q) \times C_m$. Here $\mathrm{Sz}(q)$ is the Suzuki group over $\mathbb{F}_q$ and $C_m = \langle \tau \rangle$, with $\tau(x) = x$, $\tau(y) = y$, and $\tau(t) = \lambda t$, where $\lambda \in \mathbb{F}_{q^4}$ is an element of multiplicative order m. We start by proving the following proposition, which is a refinement of Lemma 3.3 from [45].

Proposition 2.1. *Every automorphism of $\mathcal{S}_q$ can be lifted to an automorphism of $\tilde{\mathcal{S}}_q$ defined over $\mathbb{F}_q$ in a unique way. The resulting collection of automorphisms forms a group isomorphic to* $\mathrm{Sz}(q)$.

Proof. The proof from [45] mentions that automorphisms $\psi_{abc} \in \mathrm{Aut}(\mathcal{S}_q)$ defined by $\psi_{abc}(x) = ax + b$ and $\psi_{abc}(y) = a^{q_0+1}y + b^{q_0}x + c$, with $a \in \mathbb{F}_q^*$ and $b, c \in \mathbb{F}_q$, can be lifted to automorphisms ψ of $\tilde{\mathcal{S}}_q$ by defining $\psi(t) = \alpha t$, where $\alpha^m = a$ for a suitably chosen $\alpha \in \mathbb{F}_{q^4}$, and that the automorphism $\phi \in \mathrm{Aut}(\mathcal{S}_q)$ defined by $\phi(x) = z/w$ and $\phi(y) = y/w$ can be lifted to an automorphism of $\tilde{\mathcal{S}}_q$ by defining $\phi(t) = t/w$. Here $z := y^{2q_0} + x^{2q_0+1}$ and $w := xy^{2q_0} + z^{2q_0}$. Since the ψ_{abc} and ϕ generate $\mathrm{Aut}(\mathcal{S}_q)$, it is then concluded in [45] that any automorphism in $\mathrm{Aut}(\mathcal{S}_q)$ can be lifted to one of $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$ when the field of definition is extended to $\mathbb{F}_{q^4}$. However, it is clear that the lift of ϕ is actually defined over $\mathbb{F}_q$. Moreover, since $\gcd(m, q-1) = 1$, the m-th power map acts as a permutation on $\mathbb{F}_q^*$, implying that for each $a \in \mathbb{F}_q^*$ the equation $\alpha^m = a$ has a unique solution in $\alpha \in \mathbb{F}_q^*$. Choosing this α to lift ψ_{abc}, we obtain a lift of ψ_{abc} defined over $\mathbb{F}_q$. Using as in [45] that the ψ_{abc} and ϕ generate $\mathrm{Aut}(\mathcal{S}_q)$, it follows that any automorphism $\sigma \in \mathcal{S}_q$ can be lifted to an automorphism $\tilde{\sigma} \in \tilde{\mathcal{S}}_q$ defined over $\mathbb{F}_q$. Moreover, it follows from the above procedure that $\tilde{\sigma}(t) = f(x, y)t$ for some function $f(x, y)$ on $\mathcal{S}_q$ defined over $\mathbb{F}_q$. All lifts of σ are of the form $\tilde{\sigma}\tau^k$ for $k = 0, \ldots, m-1$, then $\tilde{\sigma}\tau^k(t) = f(x, y)\lambda^k t$, which is defined over $\mathbb{F}_q$ if and only if $\tau^k = \mathrm{id}_{C_m}$. This proves the first part of the proposition as well as the fact that $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$ contains exactly $|\mathrm{Sz}(q)|$ many elements defined over $\mathbb{F}_q$. The natural map from these elements to $\mathrm{Aut}(\mathcal{S}_q)$ "forgetting" the action on t, is a bijective group homomorphism, whence the second part of the proposition follows. □

We will call the lift of $\sigma \in \mathrm{Aut}(\mathcal{S}_q)$ described in Proposition 2.1 the $\mathbb{F}_q$-rational lift of σ. With slight abuse of notation, we denote this lift again by σ and think of $\mathrm{Sz}(q)$ as a

subset of $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$. The fact already proved in [30] that $\mathrm{Aut}(\tilde{\mathcal{S}}_q) = \mathrm{Sz}(q) \times C_m$ now also follows quite easily: indeed have constructed a natural copy of $\mathrm{Sz}(q)$ inside $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$, τ commutes with any element in $\mathrm{Sz}(q)$, and any element in $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$ is of the form $\sigma\tau^k$ for $\sigma \in \mathrm{Sz}(q)$.

Any non-trivial subgroup of $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$ is contained in one of its maximal subgroups, it is sufficient to consider subgroups of maximal subgroups. Since $\mathrm{Aut}(\tilde{\mathcal{S}}_q) = \mathrm{Sz}(q) \times C_m$, the following simple lemma will be very convenient.

Lemma 2.2. *Let $H \subseteq G$ be a subgroup of a direct product of groups $G = G_1 \times G_2$ and for $i = 1, 2$, define $\pi_i : H \to G_i$ as $\pi_i(g_1, g_2) = g_i$. If H is a maximal subgroup of G, then either $H = H_1 \times G_2$, with H_1 a maximal subgroup of G_1, or $H = G_1 \times H_2$, with H_2 a maximal subgroup of G_2, or $|H|$ is a multiple of $\mathrm{lcm}(|G_1|, |G_2|)$ and for $i = 1, 2$, $|\ker(\pi_i)|$ is a multiple of $|G_{3-i}|/\gcd(|G_1|, |G_2|)$.*

Proof. Let $H \subset G_1 \times G_2$ be a maximal subgroup and for $i = 1, 2$ write $H_i = \mathrm{im}(\pi_i)$. It is clear that $H \subseteq H_1 \times H_2$. Since H is maximal, either $H = H_1 \times H_2$ or $H_1 \times H_2 = G_1 \times G_2$. In the former case, we deduce from the maximality of H that either $H_1 = G_1$ and H_2 is a maximal subgroup of G_2, or H_1 is a maximal subgroup of G_1 and $H_2 = G_2$. In the latter case, we see that $G_i = H_i \cong H/\ker(\pi_i)$, where we used the isomorphism theorem. This implies that $|H|$ is both a multiple of $|G_1|$ and of $|G_2|$ and hence of the least common multiple of the two. Since more specifically $|H| = |\ker(\pi_i)| \cdot |G_i|$, we also see that $|\ker(\pi_i)|$ is a multiple of $\mathrm{lcm}(|G_1|, |G_2|)/|G_i| = |G_{3-i}|/\gcd(|G_1|, |G_2|)$ for $i = 1, 2$. □

It is trivial that the maximal subgroups of $C_m = \langle \tau \rangle$ are all of the form $\langle \tau^p \rangle$, where p is a prime dividing m. The maximal subgroups of the Suzuki group are well known and classified up to conjugation in the following theorem. See [39] Theorem 4.12 or [33], Theorem 3.1 for details.

Theorem 2.3. *Up to conjugation, the Suzuki group $\mathrm{Sz}(q)$ has the following maximal subgroups.*

1. *The Frobenius group F of order $q^2(q-1)$.*
2. *The dihedral group B_0 of order $2(q-1)$.*
3. *The normalizer N_- of a cyclic Singer group Σ_- with $|\Sigma_-| = q - 2q_0 + 1$ and $|N_-| = 4 \cdot |\Sigma_-|$.*
4. *The normalizer N_+ of a cyclic Singer group Σ_+ with $|\Sigma_+| = q + 2q_0 + 1$ and $|N_+| = 4 \cdot |\Sigma_+|$.*
5. *The Suzuki groups $\mathrm{Sz}(\hat{q})$ for $q = \hat{q}^h$, with $1 < h < 2s + 1$ and h a prime.*

Further, any subgroup of $\mathrm{Sz}(q)$ is either isomorphic to $\mathrm{Sz}(\hat{q})$ for $q = \hat{q}^k$ and $1 \leq k < 2s+1$ or conjugated to a subgroup of one of $F, B_0, N_-, or N_+$.

Lemma 2.2 and Theorem 2.3 allow us to describe all maximal subgroups of $\mathrm{Aut}(\tilde{\mathcal{S}}_q) = \mathrm{Sz}(q) \times C_m$. Actually, we obtain the following slightly stronger result on subgroups of $\mathrm{Sz}(q) \times C_m$:

Corollary 2.4. *Any subgroup $H \subset \mathrm{Sz}(q) \times C_m$ is either of the form $\mathrm{Sz}(q) \times C_n$, with $n|m$ and $C_n \subseteq C_m$ the unique subgroup of order n, or contained in $M \times C_m$ with M a maximal subgroup of $\mathrm{Sz}(q)$.*

Proof. Let H be a subgroup of $\mathrm{Sz}(q) \times C_m$. According to Lemma 2.2, we can conclude that one of the following three cases will hold: either it is contained in $M \times C_m$ with M a maximal subgroup of $\mathrm{Sz}(q)$, or contained in $\mathrm{Sz}(q) \times C_{m/p}$ with p a prime dividing m and $C_{m/p}$ the unique subgroup of C_m of order m/p, or contained in a maximal subgroup K for which $|\ker(\pi_2)|$ is a multiple of $|\mathrm{Sz}(q)|/m$.

In the first case, there is nothing left to prove. Now consider the third case. Since $\ker(\pi_2) = K \cap (\mathrm{Sz}(q) \times \{\mathrm{id}_{C_m}\})$, it can be identified with a subgroup of $\mathrm{Sz}(q)$. However, Theorem 2.3 implies that the only subgroup of $\mathrm{Sz}(q)$ that has cardinality a multiple of $|\mathrm{Sz}(q)|/m = (q + 2q_0 + 1)q^2(q-1)$ is $\mathrm{Sz}(q)$ itself. Hence $\ker(\pi_2) = \mathrm{Sz}(q) \times \{\mathrm{id}_{C_m}\} \subseteq K$, which implies that $K = \mathrm{Sz}(q) \times C_{m/p}$ for some p dividing m. Hence we arrive at the same conclusion as in the second case and should consider the case that H is a subgroup of $\mathrm{Sz}(q) \times C_{m/p}$. If $H = \mathrm{Sz}(q) \times C_{m/p}$, we are done. Otherwise a similar application of Lemma 2.2 and Theorem 2.3 shows that in this case either H is contained in $M \times C_{m/p}$ for some maximal subgroup M of $\mathrm{Sz}(q)$, or that H is a subgroup of $\mathrm{Sz}(q) \times C_{m/(pp')}$ for some prime p' dividing m/p. In the first case or in case that $H = \mathrm{Sz}(q) \times C_{m/(pp')}$, we are done, otherwise we continue dividing prime factors of m out till we arrive at the case that H is contained in $\mathrm{Sz}(q) \times \{\mathrm{id}_{C_m}\}$. At this point, we see that either $H = \mathrm{Sz}(q) \times \{\mathrm{id}_{C_m}\}$, or contained in $M \times \{\mathrm{id}_{C_m}\}$ for some maximal subgroup M of $\mathrm{Sz}(q)$. This proves the corollary. □

In [30], the genus of the quotient curve $\tilde{\mathcal{S}}_q/H$ is computed when H is one of following subgroups of $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$:

- $F \times C_m$ or one of its subgroups;
- $N_+ \times C_m$ or one of its subgroups;
- $N_- \times C_m$ or one of its subgroups of the form $K \times C_n$ with K subgroup of N_- and n dividing m;
- $\mathrm{Sz}(\hat{q}) \times C_n$ for suitable $\hat{q}$ and for n dividing m.

Corollary 2.4 implies that the only cases where the genus of $\tilde{\mathcal{S}}_q/H$ has not been computed yet are if H is one of the missing subgroups of $N_- \times C_m$ or a subgroup of $B_0 \times C_m$. To complete these cases, we use the same approach as in [30]. For a subgroup H of $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$, let g_H be the genus of the quotient curve $\tilde{\mathcal{S}}_q/H$. By the Riemann–Hurwitz formula (see [46], Theorem 3.4.13) applied to the cover $\tilde{\mathcal{S}}_q \to \tilde{\mathcal{S}}_q/H$, we have

$$(q^2+1)(q-2) = |H| \cdot (2g_H - 2) + \Delta_H,$$

where $|H|$ is the order of H and Δ_H is the degree of the different divisor. By the Hilbert's different formula, Δ_H can be expressed as

$$\Delta_H = \sum_{\substack{\omega \in H \\ \omega \neq \mathrm{id}}} \iota(\omega),$$

where

$$\iota(\omega) = \sum_{\substack{P \in \tilde{\mathcal{S}}_q \\ \omega(P) = P}} |\{i \in \mathbb{Z}_{\geq 0} \,:\, \omega \in H_P^{(i)}\}|$$

and $H_P^{(i)}$ is the i-th ramification group of the Galois cover $\tilde{\mathcal{S}}_q \to \tilde{\mathcal{S}}_q/H$ at P. See [46], Definition 3.8.4 and Theorem 3.8.7 for details. For each $\omega \in \mathrm{Aut}(\tilde{\mathcal{S}}_q)$, the quantity $\iota(\omega)$ is in principle computed in [30], Theorem 26; however, this theorem contains a mistake and for the convenience of the reader we give the correct formulation as well as a proof of the corrected part. For a group element $g \in G$, we denote by $\mathrm{ord}(g)$ the order of g.

Theorem 2.5. *Let* $\{\mathrm{id}_{\mathrm{Sz}(q)}\} \times C_m = \langle \tau \rangle$. *Then* $\iota(\tau^k) = q^2 + 1$ *for all* $k = 1, \ldots, m-1$. *Further, let* $\sigma \in \mathrm{Sz}(q) \times \{\mathrm{id}_{C_m}\}$, $\sigma \neq \mathrm{id}$. *Then exactly one of the following cases occurs:*

1. $\mathrm{ord}(\sigma) = 2$, $\iota(\sigma) = m(2q_0+1)+1$, *and* $\iota(\sigma\tau^k) = 1$ *for all* $k = 1, \ldots, m-1$;
2. $\mathrm{ord}(\sigma) = 4$, $\iota(\sigma) = m+1$, *and* $\iota(\sigma\tau^k) = 1$ *for all* $k = 1, \ldots, m-1$;
3. $\mathrm{ord}(\sigma) \mid (q-1)$, $\iota(\sigma\tau^k) = 2$ *for all* $k = 0, \ldots, m-1$;
4. $\mathrm{ord}(\sigma) \mid (q+2q_0+1)$, $\iota(\sigma\tau^k) = 0$ *for all* $k = 0, \ldots, m-1$;
5. $\mathrm{ord}(\sigma) \mid (q-2q_0+1)$, $\iota(\sigma) = 0$, $\iota(\sigma\tau^j) = m$ *for exactly four distinct* $j \in \{1, \ldots, m-1\}$, *and* $\iota(\sigma\tau^j) = 0$ *for all other* j *between* 1 *and* $m-1$.

Proof. Only the statements about $\iota(\sigma\tau^j)$ for $j = 1, \ldots, m-1$ in the fifth item need a proof, the rest of the theorem being identical to [30], Theorem 26.

Let $\sigma \in \Sigma_- \setminus \{\mathrm{id}\}$. Then σ fixes an $\mathbb{F}_{q^4}$-rational, not $\mathbb{F}_q$-rational, point P of the Suzuki curve $\mathcal{S}_q$. This point P will have certain affine coordinates $(x(P), y(P)) = (a, b)$ and σ also fixes all the q-Frobenius conjugates of P, (a^{q^j}, b^{q^j}) where $j = 1, 2, 3$. We have seen that $\mathrm{Sz}(q)$ can be lifted to a subgroup of $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$. We denote the corresponding lift of $\sigma \in \mathrm{Sz}(q)$ again by σ for convenience.

First we calculate the possibilities for $\sigma(t)$, where $t^m = x^q + x$. The orbit of m points above (a^{q^j}, b^{q^j}) where $j = 0, 1, 2, 3$ in the cover $\tilde{\mathcal{S}}_q \to \mathcal{S}_q$ is

$$O_j := \{(a^{q^j}, b^{q^j}, (\mu^i c)^{q^j}) \mid \mu^m = 1,\ i = 0, \ldots, m-1,\ c^m = a^q + a\}.$$

Note that

$$(x^q + x)_{\mathcal{S}_q} = \sum_{\alpha^q+\alpha=\beta^q+\beta=0} P_{(\alpha,\beta)} - q^2 P_\infty.$$

Since $o := \{P_{(\alpha,\beta)} \mid \alpha^q + \alpha = \beta^q + \beta = 0\} \cup \{P_\infty\}$ is an orbit of $\mathrm{Aut}(\mathcal{S}_q)$, the result is

$$(\sigma(x^q + x))_{\mathcal{S}_q} = \sum_{\substack{\alpha^q+\alpha=\beta^q+\beta=0 \\ \alpha\neq\alpha_1,\ \beta\neq\beta_1}} P_{(\alpha,\beta)} + P_\infty - q^2 P_{(\alpha_1,\beta_1)},$$

with $P_{(\alpha_1,\beta_1)} = \sigma(P_\infty)$. Hence

$$\left(\frac{\sigma(x^q + x)}{x^q + x}\right)_{\mathcal{S}_q} = (q^2+1)(P_\infty - P_{(\alpha_1,\beta_1)}) = \left(\tilde{w}^{-m}\right)_{\mathcal{S}_q},$$

where

$$\tilde{w} = \alpha_1(\alpha_1^{2q_0}x + z + \beta_1^{2q_0}) + \beta_1^{2q_0}x + w + \beta_1^2 + \alpha_1^{2q_0+2},$$

with $z := y^{2q_0} + x^{2q_0+1}$ and $w := xy^{2q_0} + z^{2q_0}$, see equation (6) in [4]. We may conclude that there exists a constant $\delta \in \mathbb{F}_q^*$ such that

$$\sigma(t)^m = \sigma(x^q + x) = \delta\frac{x^q + x}{\tilde{w}^m} = \delta\left(\frac{t}{\tilde{w}}\right)^m,$$

so that $\sigma(t) = \gamma t/\tilde{w}$, for some $\gamma \in \mathbb{F}_{q^4}^*$ such that $\gamma^m = \delta$.

Note that this implies for all $k = 0, \ldots, m-1$,

$$\sigma\tau^k(x) = \sigma(x),\ \sigma\tau^k(y) = \sigma(y),\ \sigma\tau^k(t) = \gamma\lambda^k\frac{t}{\tilde{w}},$$

where $\lambda \in \mathbb{F}_{q^4}^*$ is an element of multiplicative order m.

Now let $\tilde{P} \in O_0$ be a point lying above P in the cover $\tilde{\mathcal{S}}_q \to \mathcal{S}_q$ and write $(a, b, c) := (x(\tilde{P}), y(\tilde{P}), t(\tilde{P}))$. Suppose that k is chosen such that $\sigma \circ \tau^k$ fixes $\tilde{P}$. Since C_m acts on O_1 faithfully in a cyclic way, such k exists and is unique. Then $c = \gamma\lambda^k c/\tilde{w}(a, b)$ and hence

$$\gamma\lambda^k = \tilde{w}(a, b).$$

Clearly this implies that $\sigma\tau^k$ fixes the orbit O_0 point-wise, as the t-coordinate of the points in O_0 is of type $\mu^j c$ for $j = 0, \ldots, m-1$. We want to show that no point in O_i is fixed by $\sigma\tau^k$ for $i = 1, 2, 3$. This is equivalent to showing that $\gamma\lambda^k c^{q^i}/\tilde{w}(a^{q^i}, b^{q^i}) \neq c^{q^i}$ as again the t-coordinate of all the other points in O_i is a constant multiple of c^{q^i}. Since $\tilde{w}(a^q, b^q) = \tilde{w}(a, b)^q$, the obtained quantity is equal to c^{q^i} if and only if

$$\tilde{w}(a, b) = \gamma\lambda^k = \tilde{w}(a, b)^{q^i},$$

that is, if and only if $\tilde{w}(a,b) \in \mathbb{F}_{q^i}$.

Now note that $\tilde{w}(a,b)^m = (\gamma\lambda^k)^m = \delta$ for some $\delta \in \mathbb{F}_q^*$. Since for $i = 1,2,3$, $\gcd(q^i - 1, m) = 1$, we see for $i = 1,2,3$ that $\tilde{w}(a,b) \in \mathbb{F}_{q^i}$ implies that $\tilde{w}(a,b) \in \mathbb{F}_q$. However, as we will see in a moment, the function $\tilde{w}^q + \tilde{w}$ has only $\mathbb{F}_q$-rational zeros, so this cannot occur. Indeed, a direct computation shows that

$$\tilde{w}^q + \tilde{w} = (x^q + x)[\alpha_1^{q_0}(x + \alpha_1) + \beta_1 + y]^{2q_0}.$$

Hence any zero of $\tilde{w}^q + \tilde{w}$ is a zero of $x^q + x$, which are $\mathbb{F}_q$-rational, or a zero of $\tilde{y} := \alpha_1^{q_0}(x + \alpha_1) + \beta_1 + y$, which describes the tangent line of $\mathcal{S}_q$ at P_{α_1,β_1}. Since $\tilde{y}^q + \tilde{y} = (x + \alpha_1)^{q_0}(x^q + x)$, any zero of $\tilde{y}^q + \tilde{y}$, and hence of $\tilde{y}$, is $\mathbb{F}_q$-rational as well.

We may conclude that $\iota(\sigma\tau^k) = m$. Starting with a point in one of the other orbits O_1, O_2, O_3, one can similarly find a unique k, a different one for each orbit, such that $\iota(\sigma\tau^k) = m$. □

We will now supplement this theorem with a result, which is very convenient from a computational perspective. More precisely, in the fifth case of Theorem 2.5, we determine the four special values of j mentioned there in case σ is the $\mathbb{F}_q$-rational lift of an automorphism of $\mathcal{S}_q$.

Proposition 2.6. *Let σ be the $\mathbb{F}_q$-rational lift of an element of $\mathrm{Aut}(\mathcal{S}_q)$ of order $q-2q_0+1$. Then there exists a choice of the generator τ of C_m such that the four values of j for which $\iota(\sigma\tau^j) = m$ are $q^d \bmod m$ for $d = 0,1,2,3$.*

Proof. From the proof of Theorem 2.5, we see that given σ that fixes $P = P_{(a,b)}$, there exists $\gamma \in \mathbb{F}_{q^4}$ such that $\sigma(t) = \gamma t/\tilde{w}$, where $\gamma^m \in \mathbb{F}_q^*$. However, since σ is assumed to be the $\mathbb{F}_q$-rational lift of an element of $\mathrm{Aut}(\mathcal{S}_q)$, we may conclude that $\gamma \in \mathbb{F}_q^*$.

The value of k such that $\sigma\tau^k$ fixes all points $\tilde{P} \in O_0$ of $\tilde{\mathcal{S}}_q$ lying above P satisfies $\gamma\lambda^k = \tilde{w}(a,b)$. We claim that $i := \gcd(k,m) = 1$. If this is not the case, then $(\sigma\tau^k)^{m/i} = \sigma^{m/i} \neq \mathrm{id}$ would fix all points $\tilde{P}$, but this is not possible, since $\iota(\sigma^{m/i}) = 0$ according to Theorem 26 in [30] (or see item five in Theorem 2.5). Hence $\overline{\tau} := \tau^k$ is a generator of C_m and by construction $\sigma\overline{\tau}$ fixes all $\tilde{P} \in O_0$. Redefining τ as $\overline{\tau}$ and λ as λ^k, we obtain that $\gamma\lambda = \tilde{w}(a,b)$. Now let k_d for $d = 1,2,3$ satisfy $\gamma\lambda^{k_d} = \tilde{w}(a,b)^{q^d}$. Then $\sigma\tau^{k^d}$ fixes orbit O_d point-wise, but no other points. We then obtain

$$\lambda^{k_d} = \gamma^{-1}\gamma\lambda^{k_d} = \gamma^{-1}\tilde{w}(a,b)^{q^d} = \gamma^{-1}(\gamma\lambda)^{q^d} = \gamma^{q^d-1}\lambda^{q^d} = \lambda^{q^d}, \quad \text{for } d = 1,2,3,$$

where in the last equality we used that $\gamma^{q-1} = 1$, since $\gamma \in \mathbb{F}_q^*$. Since λ has multiplicative order m, the proposition follows. □

Remark 2.7. The mistake in [30] was that there it was claimed that if $\mathrm{ord}(\sigma) \mid (q-2q_0+1)$, then $\iota(\sigma\tau^j) = 4m$ for exactly one $j \in \{1,\ldots,m-1\}$ and $\iota(\sigma\tau^j) = 0$ for all other $j \in \{0,1,\ldots,m-1\}$. However, in [30] in this particular situation only subgroups were

considered containing either all four or none of the possible elements with $\iota(\sigma\tau^j) = m$. Therefore the corresponding contribution to the different Δ_H was correctly taken to be $4m$ or 0, implying that as far as genus computations are concerned, all the results obtained in [30] are correct. In particular the results from Propositions 38, 39, 40, and 42 in [30] are correct.

The fact that in Theorem 2.5 only the order of σ is important, makes the last part of Theorem 2.3 particularly useful in combination with Lemma 2.2: any subgroup of $\mathrm{Sz}(q)$ that is not contained in the first four listed maximal subgroups, is isomorphic to $\mathrm{Sz}(\hat{q})$ and as far as genus computations are involved only the isomorphism class matters. Therefore, we can take the natural $\mathrm{Sz}(\hat{q}) \subseteq \mathrm{Sz}(q)$ obtained by restricting the field to $\mathbb{F}_{\hat{q}}$. Combining this with Lemma 2.2 and the cases already treated in [30], we see that in order to deal with all subgroups of $\mathrm{Sz}(q) \times C_m$, we only need to deal with subgroups of $B_0 \times C_m$ and $N_- \times C_m$. We will start with the second case. Since N_- contains an element of order m, we will also need to consider subgroups of a group of the form $C_m \times C_m$, which we deal with in the next subsection first.

2.1. Description of subgroups of $C_m \times C_m$

In this subsection we give a for us convenient description of all subgroups of the direct product $C_m \times C_m$. The results in this subsection are valid for any value of m. We denote by σ and τ two elements of $C_m \times C_m$ such that $\langle \sigma, \tau \rangle = C_m \times C_m$. Note that necessarily $\mathrm{ord}(\sigma) = \mathrm{ord}(\tau) = m$. We start by describing a convenient set of generators of a subgroup of $C_m \times C_m$.

Lemma 2.8. *Let $m \geq 1$ be an integer, C_m a cyclic group of order m, and H a subgroup of $C_m \times C_m$. Then there exist unique positive integers n_1 and n_2 and a nonnegative integer a such that:*

1. *$n_1 | m$ and $n_2 | m$,*
2. *$0 \leq a < n_2$ and $n_1 n_2 | am$,*
3. *$H = \langle \sigma^{n_1}\tau^a, \tau^{n_2} \rangle$.*

Proof. Let $H \subseteq C_m \times C_m$ be a subgroup. Define n_1 to be the smallest positive integer for which there exists an integer a such that $\sigma^{n_1}\tau^a \in H$. Now let $\sigma^c\tau^d \in H$, for certain integers c and d. If $c = sn_1 + r$, with $r, s \in \mathbb{Z}$ and $0 \leq r < n_1$, then $\sigma^{c-sn_1}\tau^{d-sa} \in H$. The definition of n_1 implies that $r = c - sn_1 = 0$ and hence that n_1 divides c. In particular n_1 divides m, since $\sigma^m = \mathrm{id} \in H$. Further let n_2 be the smallest positive integer such that $\tau^{n_2} \in H$. Note that similar to n_1, the integer n_2 divides any d for which $\tau^d \in H$ and in particular, n_2 divides m. Moreover, from their definitions, we see that both n_1 and n_2 are uniquely determined once H is specified.

Multiplying $\sigma^{n_1}\tau^a$ with a suitable power of τ^{n_2}, we may assume that $0 \leq a < n_2$. The exponent a thus obtained is unique, since if $\sigma^{n_1}\tau^a$ and $\sigma^{n_1}\tau^{a'}$ both are in H, then $\tau^{a-a'} \in H$, implying that $a \equiv a' \pmod{n_2}$. This implies that either $a = a'$ or that $a' \geq n_2$. Note that since $(\sigma^{n_1}\tau^a)^{m/n_1} = \tau^{am/n_1} \in H$, we also obtain that am/n_1 is a multiple of n_2. All that remains to be shown is that $H = \langle \sigma^{n_1}\tau^a, \tau^{n_2} \rangle$. However, if $\sigma^c\tau^d \in H$, then we have seen that n_1 divides c. Hence for a suitably chosen integer i, we have $(\sigma^c\tau^d)(\sigma^{n_1}\tau^a)^i = \tau^{d+ia} \in H$. But then n_2 divides $d + ia$, implying that $\sigma^c\tau^d \in \langle \sigma^{n_1}\tau^a, \tau^{n_2} \rangle$. □

The uniqueness part of the previous lemma justifies the following definition.

Definition 2.9. Let $H \subset C_m \times C_m$ be a subgroup and n_1, n_2, a be as in Lemma 2.8. We call the triple (n_1, n_2, a) the standard exponents of H.

As in the theory of finitely generated $\mathbb{Z}$-modules, one can simplify the description of H even further if one can replace the generators σ and τ with other generators of $C_m \times C_m$. This would result in an even simpler description where a is equal to zero and n_1 divides n_2. However, as Theorem 2.5 shows, the roles of σ and τ are quite different, which is we have less freedom. Note that $|H| = m^2/(n_1 n_2)$, since the elements of H all can uniquely be written in the form $(\sigma^{n_1}\tau^a)^i(\tau^{n_2})^j$ with $0 \leq i < m/n_1$ and $0 \leq j < m/n_2$.

2.2. Subgroups of $N_- \times C_m$

As before, let $m = q - 2q_0 + 1$ and consider the maximal subgroup $N_- \times C_m$ of $\mathrm{Aut}(\tilde{\mathcal{S}}_q)$, where N_- is the normalizer of Σ_- in $\mathrm{Sz}(q)$. The group N_- has order $4m$ and is isomorphic to $C_m \rtimes C_4$, where the semidirect product is defined by the homomorphism $\varphi : C_4 \to \mathrm{Aut}(C_m)$ mapping ζ, a fixed generator of C_4, to the automorphism $\omega \mapsto \zeta\omega\zeta^{-1} = \omega^q$. See [35], Theorem 3.10, Chapter XI for details. The group $N_- \times C_m$ is therefore isomorphic to $(C_m \rtimes C_4) \times C_m$ and can be presented as

$$\langle \zeta, \sigma, \tau \mid \mathrm{ord}(\zeta) = 4, \mathrm{ord}(\sigma) = \mathrm{ord}(\tau) = m, \zeta\sigma\zeta^{-1} = \sigma^q, \zeta\tau = \tau\zeta, \sigma\tau = \tau\sigma \rangle.$$

It is easy to see that all elements of order two in $N_- \times C_m$ are those of the form $\sigma^i\zeta^2$, while the elements of order four are those of the form $\sigma^i\zeta$ or $\sigma^i\zeta^3$. Finally, N_- has a maximal subgroup D_- isomorphic to the dihedral group of order $2m$, containing Σ_-. The group $D_- \times C_m = \langle \zeta^2, \sigma, \tau \rangle$ is isomorphic to $(C_m \rtimes C_2) \times C_m$.

The genera of the quotient curves $\tilde{\mathcal{S}}_q/H$ for H subgroup of $N_- \times C_m$ of the form $(C_{n_1} \rtimes C_4) \times C_{n_2}$, $(C_{n_1} \rtimes C_2) \times C_{n_2}$, and $C_{n_1} \times C_{n_2}$, with n_1 and n_2 divisors of m, were computed in Propositions 38, 39, 40 from [30]. To find which subgroups of $N_- \times C_m$ are missing, we first give the following proposition.

Proposition 2.10. *Let H be a subgroup of $N_- \times C_m$. Then there exist divisors n_1 and n_2 of m such that one of the following holds:*

1. $H \subseteq \Sigma_- \times C_m$,
2. H *is conjugated to* $\langle \sigma^{m/n_1}, \tau^{m/n_2}, \zeta^2 \rangle \cong (C_{n_1} \rtimes C_2) \times C_{n_2}$, *or*
3. H *is conjugated to* $\langle \sigma^{m/n_1}, \tau^{m/n_2}, \zeta \rangle \cong (C_{n_1} \rtimes C_4) \times C_{n_2}$.

Proof. It is clear that the subgroup $\Sigma_- \times C_m$ is normal in $N_- \times C_m$ and that the quotient group is cyclic of order four. Now let H be a subgroup of $N_- \times C_m$ and consider the group homomorphism $\phi : H \to (N_- \times C_m)/(\Sigma_- \times C_m)$. Then $\ker(\phi) = H \cap (\Sigma_- \times C_m)$ and therefore $H/(H \cap (\Sigma_- \times C_m))$ is a subgroup of a cyclic group of order four. Therefore the index of $H \cap (\Sigma_- \times C_m)$ in H is in $\{1, 2, 4\}$. Since $H \cap (\Sigma_- \times C_m)$ itself has odd cardinality, the Schur–Zassenhaus theorem implies that $H \cap (\Sigma_- \times C_m)$ has a complement K in H. Moreover, K is isomorphic to $H/(H \cap (\Sigma_- \times C_m))$. We now distinguish three cases.

Case 1, $[H : (H \cap (\Sigma_- \times C_m))] = 1$. In this case $H = H \cap (\Sigma_- \times C_m)$ and hence $H \subseteq \Sigma_- \times C_m$.

Case 2, $[H : (H \cap (\Sigma_- \times C_m))] = 2$. In this case the complement K contains an element of order two and H cannot contain an element of order four. Moreover, $\sigma^{-j}(\sigma^i\zeta^2)\sigma^j = \sigma^{i+j(q^2-1)}\zeta^2$. Since $\gcd(q^2-1, m) = 1$, we can choose j such that $\sigma^{-j}(\sigma^i\zeta^2)\sigma^j = \zeta^2$. Hence replacing H by a suitable conjugate, we may assume that ζ^2 is an element of H. If $\sigma^i\tau^j\zeta^2 \in H$, then $\sigma^i\tau^j \in H$. Moreover, if $\sigma^i\tau^j \in H$, then

$$H \ni \zeta^2(\sigma^i\tau^j)\zeta^2(\sigma^i\tau^j)^{-1} = \zeta^2\sigma^i\zeta^2\sigma^{-i} = \sigma^{i(q^2-1)}.$$

Since $\gcd(q^2-1, m) = 1$ and $\mathrm{ord}(\sigma) = m$, this implies that $\sigma^i \in H$. Hence whenever $\sigma^i\tau^j\zeta^e \in H$, with $e = 0, 2$, then $\sigma^i \in H$ and hence $\tau^j \in H$. This shows that H is of the form as in case two of the proposition.

Case 3, $[H : (H \cap (\Sigma_- \times C_m))] = 4$. This case is very similar to the previous one. After a suitable conjugation, we may assume that $\zeta \in H$. Then if $\sigma^i\tau^j\zeta^e \in H$, with $e = 0, 1, 2, 3$, practically the same computation as before shows that $\sigma^i \in H$ and $\tau^j \in H$. Hence H is of the form as in case three of the proposition. □

This proposition shows that in order to complete the case of subgroups of $N_- \times C_m$, we only need to consider subgroups of $\Sigma_- \times C_m$. Therefore, we now turn our attention to those. It will be convenient to define $v_p(n) := \max\{e : p^e \text{ divides } n\}$, where $n \in \mathbb{Z}$.

Theorem 2.11. *Let H be a subgroup of $\Sigma_- \times C_m = \langle \sigma, \tau \rangle$ with standard exponents (n_1, n_2, a). Suppose that $m = p_1^{e_1} \cdots p_r^{e_r}$, with $p_1, \ldots, p_r$ mutually distinct prime numbers and $e_1, \ldots, e_r$ positive integers. For $d \in \{0, 1, 2, 3\}$, write $\nu_{d,\ell} = \min\{v_{p_\ell}(n_1 q^d - a), v_{p_\ell}(n_2)\}$. The genus of the quotient curve $\tilde{\mathcal{S}}_q/H$ is*

$$g_H = \frac{(q^2+1)(q-2) - \Delta_H}{2|H|} + 1,$$

with $|H| = m^2/(n_1 n_2)$ and

$$\Delta_H = \left(\frac{m}{n_2} - 1\right) \cdot (q^2+1) + \sum_{d=0}^{3} \left(\frac{m \prod_{\ell=1}^{r} p_\ell^{\nu_{d,\ell}}}{n_1 n_2} - 1\right) \cdot m.$$

Proof. The expression for the genus g_H follows from the Riemann–Hurwitz formula and it has already been noted that $|H| = m^2/(n_1 n_2)$. Therefore, all that remains to be done is to compute the quantity Δ_H. Recall that

$$\Delta_H = \sum_{\substack{\omega \in H \\ \omega \neq \mathrm{id}}} \iota(\omega) = \sum_{\substack{\alpha>0, \\ \sigma^\alpha \in H}} \iota(\sigma^\alpha) + \sum_{\substack{\beta>0, \\ \tau^\beta \in H}} \iota(\tau^\beta) + \sum_{\substack{\alpha>0, \beta>0, \\ \sigma^\alpha \tau^\beta \in H}} \iota(\sigma^\alpha \tau^\beta)$$

and that $\iota(\sigma^\alpha) = 0$ for all $\alpha = 1, \ldots, m-1$ and $\iota(\tau^\beta) = q^2+1$ for all $\beta = 1, \ldots, m-1$ from Theorem 2.5.

The elements of H can uniquely be written in the form $(\sigma^{n_1}\tau^a)^i(\tau^{n_2})^j$ with $0 \leq i < m/n_1$ and $0 \leq j < m/n_2$. Hence the number of elements in H of the form $\tau^\beta \neq \mathrm{id}$ is exactly $m/n_2 - 1$. What remains to be done is to determine the number of elements in $H \setminus \{\mathrm{id}\}$ of the form $\sigma^\alpha \tau^\beta$ such that $\iota(\sigma^\alpha \tau^\beta) = m$. From Theorem 2.5 and Proposition 2.6, we conclude that this is equal to the number of triples (i, j, d), with $d = 0, 1, 2, 3$, $1 \leq i < m/n_1$, and $0 \leq j < m/n_2$, such that

$$jn_2 \equiv i(n_1 q^d - a) \pmod{m}. \tag{1}$$

We will first for each d count the number of solutions (i, j) to congruence (1) satisfying $0 \leq i < m$ and $0 \leq j < m$. In order to do this, we use the factorization of m into prime numbers: $m = p_1^{e_1} \cdots p_r^{e_r}$. The congruence $jn_2 \equiv i(n_1 q^d - a) \pmod{p_\ell^{e_\ell}}$ is equivalent to the congruence $j(n_2/p_\ell^{\nu_{d,\ell}}) \equiv i(n_1 q^d - a)/p_\ell^{\nu_{d,\ell}} \pmod{p_\ell^{e_\ell - \nu_{d,\ell}}}$. By definition of $\nu_{d,\ell}$, both $n_2/p_\ell^{\nu_{d,\ell}}$ and $(n_1 q^d - a)/p_\ell^{\nu_{d,\ell}}$ are integers and at least one of them is not divisible by p_ℓ and therefore has an inverse modulo powers of p_ℓ. This means that either i or j can be chosen arbitrarily between 0 and $p_\ell^{e_\ell} - 1$, while the other variable then is determined uniquely modulo $p_\ell^{e_\ell - \nu_{d,\ell}}$. This means that the congruence $jn_2 \equiv i(n_1 q^d - a) \pmod{p_\ell^{e_\ell}}$ has exactly $p_\ell^{e_\ell + \nu_{d,\ell}}$ many solutions (i, j) with $0 \leq i < p_\ell^{e_\ell}$ and $0 \leq j < p_\ell^{e_\ell}$. Using the Chinese remainder theorem, we see that congruence (1) for a given d has exactly $\prod_\ell p_\ell^{e_\ell + \nu_{d,\ell}} = m \prod_\ell p_\ell^{\nu_{d,\ell}}$ many solutions (i, j) satisfying $0 \leq i < m$, and $0 \leq j < m$.

Now note that if (i, j) is such a solution, then for any integers A and B, the pair $(i + m/n_1 A \bmod m, j + m/n_2 B - ma/(n_1 n_2) A \bmod m)$ also is a solution (note that $n_1 n_2$ divides ma by Lemma 2.8). This means that any solution (i, j) to congruence (1) gives rise to $n_1 n_2$ solutions when A and B are chosen such that $0 \leq A < n_1$ and $0 \leq B < n_2$. Moreover any such a set of $n_1 n_2$ solutions contains exactly one solution pair (i, j) satisfying $0 \leq i < m/n_1$ and $0 \leq j < m/n_2$. We may therefore conclude that the number of solutions (i, j) to congruence (1) satisfying $0 \leq i < m/n_1$ and $0 \leq j < m/n_2$ is equal to $m \prod_\ell p_\ell^{\nu_{d,\ell}}/(n_1 n_2)$. Disregarding the solution $(0, 0)$, we conclude that the number of elements $h \in H \setminus \{\mathrm{id}\}$ for which $\iota(h) = m$ equals $m \prod_\ell p_\ell^{\nu_{d,\ell}}/(n_1 n_2) - 1$. The result now follows. □

This completes the study of the genera of the quotient curves $\tilde{\mathcal{S}}_q/H$ for H subgroup of $N_- \times C_m$. The following genera, obtained using Theorem 2.11 for $s = 1, 2, 3, 4$, are new to the best of our knowledge.

2.3. Subgroups of $B_0 \times C_m$

Let B_0 be the maximal subgroup of $\mathrm{Sz}(q)$ of order $2(q-1)$, isomorphic to the dihedral group D_{q-1}, corresponding to the second case in Theorem 2.3. Since $q-1$ and m are coprime, all subgroups of $B_0 \times C_m$ are either of the form $C_d \times C_n$ or of the form $D_d \times C_n$, with d dividing $q-1$ and n dividing m. Conversely, for each d dividing $q-1$ and n dividing m there exists a subgroup of $B_0 \times C_m$ isomorphic to $C_d \times C_n$ and a subgroup of $B_0 \times C_m$ isomorphic to $D_d \times C_n$.

Theorem 2.12. *Let H be a subgroup of $B_0 \times C_m$. If $H \cong C_d \times C_n$ for some d dividing $q-1$ and n dividing m, then the genus of the quotient curve $\tilde{\mathcal{S}}_q/H$ is*

$$g_H = \frac{(q^2+1)(q-n-1) - 2(d-1)n}{2dn} + 1.$$

If $H \cong D_d \times C_n$ for some d dividing $q-1$ and n dividing m, then the genus of the quotient curve $\tilde{\mathcal{S}}_q/H$ is

$$g_H = \frac{(q^2+1)(q-n-1) - dm(2q_0+1) - 3dn + 2n}{4dn} + 1.$$

Proof. If $H \cong C_d \times C_n$, then $\Delta_H = (n-1)\cdot(q^2+1) + (d-1)n \cdot 2$ from Theorem 2.5. The expression for g_H follows from the Riemann–Hurwitz formula.

Assume $H \cong D_d \times C_n$ now. Let $\mathfrak{s}$ be an element of D_d of order 2. As a set, H can be expressed as disjoint union of subsets as follows:

$$H = (C_d \times C_n) \cup (\mathfrak{s}C_d \times \{\mathrm{id}_{C_n}\}) \cup (\mathfrak{s}C_d \times (C_n \setminus \{\mathrm{id}_{C_n}\})).$$

From the previous case and from Theorem 2.5, Δ_H can be obtained as

$$\Delta_H = (n-1)\cdot(q^2+1) + (d-1)n \cdot 2 + d \cdot (m(2q_0+1)+1) + d(n-1)\cdot 1.$$

The conclusion follows from the Riemann–Hurwitz formula. □

No new genera are found for $s = 1, 2, 3, 4$ using Theorem 2.12.

3. Galois subcovers of $\tilde{R}_q$

Whereas we in the previous section studied Galois subcovers $\tilde{\mathcal{S}}_q$ of the form $\tilde{\mathcal{S}}_q/H$, we now deal with the case of the Ree curve $\mathcal{R}_q$ and the associated Skabelund curve

$\tilde{\mathcal{R}}_q$. Throughout this section let $s \geq 1$ be a fixed integer, $q_0 := 3^s$, $q := 3q_0^2$ and $m := q - 3q_0 + 1$. In this subsection, τ denotes the automorphism of $\tilde{\mathcal{R}}_q$ fixing x, y, and z, while mapping t to λt, with $\lambda \in \mathbb{F}_{q^6}$ an element of multiplicative order m. It will convenient to define ten functions w_i, $i = 1, \ldots, 10$, on the Ree curve that were introduced in [44].

$$
\begin{array}{lll}
w_1 := x^{3q_0+1} - y^{3q_0} & w_2 := xy^{3q_0} - z^{3q_0} & w_3 := xz^{3q_0} - w_1^{3q_0} \\
w_4 := xw_2^{q_0} - yw_1^{q_0} & v := xw_3^{q_0} - zw_1^{q_0} & w_5 := yw_3^{q_0} - zw_2^{q_0} \\
w_6 := v^{3q_0} - w_2^{3q_0} + xw_4^{3q_0} & w_7 := yw_2^{q_0} - xw_3^{q_0} - w_6^{3q_0} & w_8 := w_5^{3q_0} + xw_7^{3q_0} \\
w_9 := w_2^{q_0}w_4 - yw_6^{q_0} & w_{10} := zw_6^{q_0} - w_3^{q_0}w_4 &
\end{array}
$$

These functions were used in [13] to obtain a smooth embedding of the Ree curve in thirteen-dimensional projective space. For future reference, we collect some facts on the function w_8 in the form of two lemmas.

Lemma 3.1. *Let $P_{(0,0,0)}$, respectively P_∞, be the common zero, respectively the only pole of the functions x, y and z on the Ree curve. Then*

$$(w_8) = (q+1)(q+3q_0+1)(P_{(0,0,0)} - P_\infty) = \frac{q^3+1}{m}(P_{(0,0,0)} - P_\infty).$$

Proof. From [44, Equation (A18)] $v_{P_\infty}(w_8) = -(q+1)(q+3q_0+1)$ and P_∞ is the only pole of w_8 as it is a polynomial in x, y and z. The lemma follows by proving that $v_{P_{(0,0,0)}}(w_8) = (q+1)(q+3q_0+1)$. However, this follows directly from the defining equations for the functions w_i and v using the strict triangle equality and the fact that $v_{P_{(0,0,0)}}(x) = 1$, $v_{P_{(0,0,0)}}(y) = q_0 + 1$, and $v_{P_{(0,0,0)}}(z) = 2q_0 + 1$, which in turn can be deduced from the defining equation of $\mathcal{R}_q$. □

Lemma 3.2. *All zeroes of the function $w_8^q - w_8$ on the curve $\mathcal{R}_q$ are $\mathbb{F}_q$-rational.*

Proof. We can use the definitions of the functions w_i recalled above and the relations between them given in [44, Appendix A] to find a contradiction assuming that a zero P of $w_8^q - w_8$ which is not $\mathbb{F}_q$-rational exists. From [44, Equation (A18)] $w_8^q - w_8 = w_7^{3q_0}(x^q - x)$ so P is also a zero of w_7. This implies together with the definition of w_8 that w_5 also vanishes at P. From [44, Equation (A16)] and the defining equations of $\mathcal{R}_q$, $w_7^q - w_7 = w_2^{q_0}(y^q - y) - w_3^{q_0}(x^q - x) = (w_2x - w_3)^{q_0}(x^q - x)$, so that P is also a zero of $w_2x - w_3$. This shows that P is a common zero of $w_2x - w_3$, w_5, and w_7. From the definition of w_5 we have

$$0 = w_5(P) = (yw_3^{q_0} - zw_2^{q_0})(P) = (yx^{q_0}w_2^{q_0} - zw_2^{q_0})(P) = w_2^{q_0}(P) \cdot (yx^{q_0} - z)(P).$$

From [44, Equation (A4)] $w_2(P) \neq 0$ since the zeros of $w_2^q - w_2 = y^{3q_0}(x^q - x)$, and hence of w_2, are all $\mathbb{F}_q$-rational. Hence P needs to be a zero of $yx^{q_0} - z$. Combining this with $z^q - z = x^{q_0}(y^q - y)$ we get that

$$x^{q_0}(y^q - y)(P) = z(P)^q - z(P) = y^q x^{q_0 q}(P) - y x^{q_0}(P),$$

hence $x^{q_0} y^q(P) = x^{q_0 q} y^q(P)$ and $y^q(x^q - x)^{q_0}(P) = 0$. This implies that P is $\mathbb{F}_q$-rational, a contradiction. □

We now follow exactly the same approach as in the previous section and start with the Ree-variant of Proposition 2.1. It refines Lemma 4.2 from [45].

Proposition 3.3. *Every automorphism of $\mathcal{R}_q$ can be lifted to an automorphism of $\tilde{\mathcal{R}}_q$ defined over $\mathbb{F}_q$ in a unique way. The resulting collection of automorphisms forms a group isomorphic to* $\mathrm{Ree}(q)$.

Proof. The automorphism group $\mathrm{Aut}(\mathcal{R}_q)$ is generated by an involution ϕ and automorphisms ψ_{abcd} defined by $\psi_{abcd}(x) = ax + b$, $\psi_{abcd}(y) = a^{q_0+1}y + ab^{q_0}x + c$, and $\psi_{abcd}(z) = a^{2q_0+1}z - a^{q_0+1}b^{q_0}y + ab^{2q_0}x + d$, with $a \in \mathbb{F}_q^*$ and $b, c, d \in \mathbb{F}_q$. As explained in [45], ψ_{abcd} can be lifted to an automorphism ψ of $\tilde{\mathcal{R}}_q$ by setting $\psi(t) = \alpha t$, where $\alpha^m = a$. Since $\gcd(q-1, m) = 1$, there exists exactly one choice for $\alpha \in \mathbb{F}_q^*$ such that $\alpha^m = a$. The involution ϕ, satisfies $\phi(x) = w_6/w_8$, $\phi(y) = w_{10}/w_8$, and $\phi(z) = w_9/w_8$. As observed in [45], it can be lifted to an automorphism of $\tilde{\mathcal{R}}_q$ by defining $\phi(t) = t/w_8$. The remainder of the proof is now similar as the proof of Proposition 2.1. □

As for the Suzuki case, we will call the lift of $\sigma \in \mathrm{Aut}(\mathcal{R}_q)$ described in Proposition 3.3 the $\mathbb{F}_q$-rational lift of σ and denote this lift again by σ. Also the fact already proved in [30] that $\mathrm{Aut}(\tilde{\mathcal{R}}_q) = \mathrm{Ree}(q) \times C_m$ is again an easy consequence of the existence of $\mathbb{F}_q$-rational lifts. Continuing the same strategy as in the previous section, we now collect various facts on subgroups of $\mathrm{Ree}(q)$. See [38], Section 2 for details.

Theorem 3.4. *Up to conjugation, the Ree group* $\mathrm{Ree}(q)$ *has the following maximal subgroups.*

1. *The Frobenius group F of order $q^3(q-1)$.*
2. *The centralizer C of an involution, of order $q(q-1)(q+1)$.*
3. *The normalizer N_- of a cyclic Singer group Σ_- with $|\Sigma_-| = q - 3q_0 + 1$ and $|N_-| = 6 \cdot |\Sigma_-|$.*
4. *The normalizer N_+ of a cyclic Singer group Σ_+ with $|\Sigma_+| = q + 3q_0 + 1$ and $|N_+| = 6 \cdot |\Sigma_+|$.*
5. *The normalizer N of a cyclic group A with $|A| = (q+1)/4$ and $|N| = 6(q+1)$.*
6. *The Ree groups* $\mathrm{Ree}(\hat{q})$ *for $q = \hat{q}^h$, with h a prime number.*

Let N_2 be the normalizer of a Sylow 2-subgroup of $\mathrm{Ree}(q)$. *Then, for any subgroup K of* $\mathrm{Ree}(q)$, *one of the following three possibilities occurs: K is isomorphic to* $\mathrm{Ree}(\hat{q})$ *where $q = \hat{q}^k$ and $1 \le k \le 2s+1$, or K is isomorphic to* $\mathrm{PSL}(2, 8)$, *or K is conjugated to a*

subgroup of one of F, C, N_-, N_+, N, or N_2. Finally, the subgroup N_2 has order 168, $\mathrm{PSL}(2,8)$ *has order* 504 *and both have conjugates contained in* $\mathrm{Ree}(3)$.

Lemma 2.2 and Theorem 3.4 allow us to describe all maximal subgroups of $\mathrm{Aut}(\tilde{\mathcal{S}}_q) = \mathrm{Ree}(q) \times C_m$. We obtain the following analogue of Corollary 2.4:

Corollary 3.5. *Any subgroup $H \subset \mathrm{Ree}(q) \times C_m$ is either of the form $\mathrm{Ree}(q) \times C_n$, with $n|m$ and $C_n \subseteq C_m$ the unique subgroup of order n, or contained in $M \times C_m$ with M a maximal subgroup of $\mathrm{Ree}(q)$.*

Proof. The proof is similar to that of Corollary 2.4. The main ingredient is that Theorem 3.4 implies that a subgroup of $\mathrm{Ree}(q)$ of index at most m, is equal to $\mathrm{Ree}(q)$ itself. □

In [30], the genus of the quotient curve $\tilde{\mathcal{R}}_q/H$ is computed when H is one of following subgroups of $\mathrm{Aut}(\tilde{\mathcal{R}}_q)$:

- $F \times C_m$ or one of its subgroups;
- $C \times C_m$ or one of its subgroups;
- $N_+ \times C_m$ or one of its subgroups;
- $N_- \times C_m$ or one of its subgroups of the form $K \times C_n$ with K a subgroup of N_- and n dividing m;
- $N \times C_m$ or one of its subgroups;
- $\mathrm{Ree}(\hat{q}) \times C_n$ for suitable $\hat{q}$ and for n dividing m.

Corollary 3.5 implies that the only cases where the genus of $\tilde{\mathcal{R}}_q/H$ has not been computed yet are if H is one of the missing subgroups of $N_- \times C_m$ or H is one of the missing subgroups of $\mathrm{Ree}(3) \times C_m$. For a generic subgroup H of $\mathrm{Aut}(\tilde{\mathcal{R}}_q)$, let g_H be the genus of the quotient curve $\tilde{\mathcal{R}}_q/H$. Again, we can use the theory of ramification groups and Hilbert's different formula to compute g_H. For each $\omega \in \mathrm{Aut}(\tilde{\mathcal{R}}_q)$, the quantity $\iota(\omega)$ was computed in [30], Theorem 48; however, as in the Suzuki case one mistake was made. Hereby we give the correct formulation and include a proof for the corrected case.

Theorem 3.6. *Let $\sigma \in \mathrm{Ree}(q) \times \{\mathrm{id}_{C_m}\}$, $\sigma \neq \mathrm{id}$ and $\{\mathrm{id}_{\mathrm{Ree}(q)}\} \times C_m = \langle \tau \rangle$. Then $\iota(\tau^k) = q^3 + 1$ for all $k = 1, \ldots, m-1$ and one of the following cases occurs.*

1. $\mathrm{ord}(\sigma) = 3$, *σ is in the center of a Sylow 3-subgroup, $\iota(\sigma) = m(q + 3q_0 + 1) + 1$, and $\iota(\sigma\tau^k) = 1$ for all $k = 1, \ldots, m-1$;*
2. $\mathrm{ord}(\sigma) = 3$, *σ is not in the center of any Sylow 3-subgroup $\iota(\sigma) = m(3q_0 + 1) + 1$, and $\iota(\sigma\tau^k) = 1$ for all $k = 1, \ldots, m-1$;*
3. $\mathrm{ord}(\sigma) = 9$, *$\iota(\sigma) = m + 1$, and $\iota(\sigma\tau^k) = 1$ for all $k = 1, \ldots, m-1$;*
4. $\mathrm{ord}(\sigma) = 2$, *$\iota(\sigma\tau^k) = q + 1$ for all $k = 0, \ldots, m-1$;*

5. $\mathrm{ord}(\sigma) = 6$, $\iota(\sigma\tau^k) = 1$ *for all* $k = 0, \ldots, m-1$;
6. $\mathrm{ord}(\sigma) \mid (q-1)$, $\mathrm{ord}(\sigma) \neq 2$, $\iota(\sigma\tau^k) = 2$ *for all* $k = 0, \ldots, m-1$;
7. $\mathrm{ord}(\sigma) \mid (q+1)$, $\mathrm{ord}(\sigma) \neq 2$, $\iota(\sigma\tau^k) = 0$ *for all* $k = 0, \ldots, m-1$;
8. $\mathrm{ord}(\sigma) \mid (q+3q_0+1)$, $\iota(\sigma\tau^k) = 0$ *for all* $k = 0, \ldots, m-1$;
9. $\mathrm{ord}(\sigma) \mid (q-3q_0+1)$, $\iota(\sigma) = 0$, $\iota(\sigma\tau^j) = m$ *for exactly six distinct* $j \in \{1, \ldots, m-1\}$ *and* $\iota(\sigma\tau^j) = 0$ *for all other* j *between* 1 *and* $m-1$.

Proof. Only the statements about $\iota(\sigma\tau^j)$ for $j = 1, \ldots, m-1$ in the ninth item need a proof, the rest of the theorem being identical to [30], Theorem 48.

Let $\sigma \in \Sigma_- \setminus \{\mathrm{id}\}$. Then σ fixes an $\mathbb{F}_{q^6}$-rational, not $\mathbb{F}_q$-rational, point P of the Ree curve $\mathcal{R}_q$ with certain affine coordinates $(x(P), y(P), z(P)) = (a, b, c)$. Further, σ maps P_∞, the unique pole of x, to an $\mathbb{F}_q$ rational point, say $P_{(\alpha_1,\beta_1,\gamma_1)}$, having affine coordinates $(\alpha_1, \beta_1, \gamma_1)$. By Proposition 3.3, we know that $\sigma \in \mathrm{Ree}(q)$ can be lifted uniquely to an element in $\mathrm{Aut}(\tilde{\mathcal{R}}_q)$ defined over $\mathbb{F}_q$, which we denote by σ again for convenience. First of all, using Lemma 3.1, one shows similarly as in the proof of Theorem 2.5 that

$$\left(\frac{\sigma(x^q + x)}{x^q + x}\right)_{\mathcal{R}_q} = (q^3+1)(P_\infty - P_{(\alpha_1,\beta_1,\gamma_1)}) = \left(\tilde{w}^{-m}\right)_{\mathcal{R}_q},$$

where $\tilde{w} := \omega(w_8)$ and $\omega \in \mathrm{Aut}(\mathcal{R}_q)$ is an element such that $\omega(P_\infty) = P_\infty$ and $\omega(P_{(0,0,0)}) = P_{(\alpha_1,\beta_1,\gamma_1)}$. Note that ω exists, since $\mathrm{Ree}(q)$ acts 2-transitive on the set of $\mathbb{F}_q$-rational points of $\mathcal{R}_q$. We may conclude that $\sigma(t) = \gamma t/\tilde{w}$, for some $\gamma \in \mathbb{F}_{q^6}^*$ and that for all $k = 0, \ldots, m-1$,

$$\sigma\tau^k(x) = \sigma(x),\ \sigma\tau^k(y) = \sigma(y),\ \sigma\tau^k(t) = \gamma\lambda^k \frac{t}{\tilde{w}},$$

where $\lambda \in \mathbb{F}_{q^6}^*$ is an element of multiplicative order m.

Now denote for $i = 0, 1, \ldots, 5$ by P_i the point of $\mathcal{R}_q$ with affine coordinates $(a^{q^i}, b^{q^i}, c^{q^i})$ and let O_i be the set of points lying above P_i in the cover $\tilde{\mathcal{R}}_q \to \mathcal{R}_q$. Note $P_0 = P$. Similarly as in the Suzuki case, if $\tilde{P} \in O_0$ is a point lying above P then there exists a unique k between 1 and $m-1$ such that $\sigma \circ \tau^k$ fixes $\tilde{P}$ implying that $\gamma\lambda^k = \tilde{w}(a, b, c)$ and hence that $\sigma\tau^k$ fixes the orbit O_0 point-wise. To show that none of the points in the remaining orbits O_i are fixed by $\sigma\tau^k$ is equivalent to showing that $\tilde{w}(a, b, c) \notin \mathbb{F}_{q^i}$. Since for $i = 1, \ldots, 5$, one has $\gcd(q^i - 1, m) = 1$, we see that $\tilde{w}(a, b, c) \in \mathbb{F}_{q^i}$ implies that $\tilde{w}(a, b, c) \in \mathbb{F}_q$. However, by Lemma 3.2 this cannot occur. We may conclude that $\iota(\sigma\tau^k) = m$. Starting with a point in one of the other orbits O_i, one can similarly find a unique k, a different one for each orbit, such that $\iota(\sigma\tau^k) = m$. □

As in the Suzuki case, we can supplement this with the following result:

Proposition 3.7. *Let* σ *be the* $\mathbb{F}_q$*-rational lift of an element of* $\mathrm{Aut}(\mathcal{R}_q)$ *of order* $q-3q_0+1$. *Then there exists a choice of the generator* τ *of* C_m *such that the six values of* j *for which* $\iota(\sigma\tau^j) = m$ *are* $q^d \bmod m$ *for* $d = 0, 1, 2, 3, 4, 5$.

Proof. The proof is completely similar to that of Proposition 2.6. □

Remark 3.8. As in Remark 2.7, one can show that the formulation of [30], Theorem 48 does not affect the genus computations carried out in [30]. In particular, Propositions 65, 66, 67, 68, and 72 from [30] are correct.

We now consider the two cases not fully treated in [30] in the following two subsections, namely all subgroups of $N_- \times C_m$ and all subgroups of $\mathrm{Ree}(3) \times C_m$.

3.1. Subgroups of $N_- \times C_m$

The normalizer N_- of a Singer cycle Σ_- has order $6m$ and is isomorphic to $C_m \rtimes C_6$, where the semidirect product is defined by the homomorphism $\varphi : C_6 \to \mathrm{Aut}(C_m)$ mapping ζ, a fixed generator of C_6, to the automorphism $\omega \mapsto \zeta\omega\zeta^{-1} = \omega^q$. See [35], Theorem 13.2, Chapter XI and [7], Proposition 4.13 for details. The group $N_- \times C_m$ is therefore isomorphic to $(C_m \rtimes C_6) \times C_m$ and can be presented as

$$\langle \zeta, \sigma, \tau \mid \mathrm{ord}(\zeta) = 6, \mathrm{ord}(\sigma) = \mathrm{ord}(\tau) = m, \zeta\sigma\zeta^{-1} = \sigma^q, \zeta\tau = \tau\zeta, \sigma\tau = \tau\sigma \rangle.$$

It is easy to see that all elements of order two in $N_- \times C_m$ are those of the form $\sigma^i\zeta^3$, while the elements of order three are those of the form $\sigma^i\zeta^2$ or $\sigma^i\zeta^4$. Finally the elements of order six are those of the form $\sigma^i\zeta$ or $\sigma^i\zeta^5$.

To find out which subgroups of $N_- \times C_m$ have not been treated in [30] yet, we give the following analogue of Proposition 2.10.

Proposition 3.9. *Let H be a subgroup of $N_- \times C_m$. Then there exist divisors n_1 and n_2 of m such that one of the following holds:*

1. $H \subseteq \Sigma_- \times C_m$,
2. *H is conjugated to* $\langle \sigma^{m/n_1}, \tau^{m/n_2}, \zeta^3 \rangle \cong (C_{n_1} \rtimes C_2) \times C_{n_2}$,
3. *H is conjugated to* $\langle \sigma^{m/n_1}, \tau^{m/n_2}, \zeta^2 \rangle \cong (C_{n_1} \rtimes C_3) \times C_{n_2}$, *or*
4. *H is conjugated to* $\langle \sigma^{m/n_1}, \tau^{m/n_2}, \zeta \rangle \cong (C_{n_1} \rtimes C_6) \times C_{n_2}$.

Proof. Let H be a subgroup of $N_- \times C_m$. Just as in the proof of Proposition 2.10, the Schur–Zassenhaus theorem implies that $H \cap (\Sigma_- \times C_m)$ has a complement K in H, which is isomorphic to $H/(H \cap (\Sigma_- \times C_m))$. Then four cases can be distinguished and dealt with similarly as in Proposition 2.10.

Case 1, $[H : (H \cap (\Sigma_- \times C_m))] = 1$. In this case $H = H \cap (\Sigma_- \times C_m)$ and hence $H \subseteq \Sigma_- \times C_m$.

Case 2, $[H : (H \cap (\Sigma_- \times C_m))] = 2$. In this case the complement K contains an element $\sigma^i\zeta^3$ of order two and since $\sigma^{-j}(\sigma^i\zeta^3)\sigma^j = \sigma^{i+j(q^3-1)}\zeta^3$. Since $\gcd(q^3 - 1, m) = 1$, we can choose j such that $\sigma^{-j}(\sigma^i\zeta^3)\sigma^j = \zeta^3$. Hence replacing H by a suitable conjugate, we may assume that ζ^3 is an element of H. If $\sigma^i\tau^j \in H$, then

$$H \ni \zeta^3(\sigma^i\tau^j)\zeta^3(\sigma^i\tau^j)^{-1} = \zeta^3\sigma^i\zeta^3\sigma^{-i} = \sigma^{i(q^3-1)}.$$

Since $\gcd(q^3-1, m) = 1$ and $\mathrm{ord}(\sigma) = m$, this implies that $\sigma^i \in H$. Hence whenever $\sigma^i\tau^j\zeta^e \in H$, with $e = 0, 3$, then $\sigma^i \in H$ and hence $\tau^j \in H$. This shows that H is of the form as in case two of the proposition.

Case 3, $[H : (H \cap (\Sigma_- \times C_m))] = 3$. Can be handled in a similar way.

Case 4, $[H : (H \cap (\Sigma_- \times C_m))] = 6$. Can be handled in a similar way. □

This proposition shows that the only subgroups of $N_- \times C_m$ not considered in [30], are contained in $\Sigma_- \times C_m$. In the following, we determine the genus of $\tilde{R}_q/H$ for all possible subgroups of $\Sigma_- \times C_m$.

Theorem 3.10. *Let H be a subgroup of $\Sigma_- \times C_m = \langle \sigma, \tau \rangle$ with standard exponents (n_1, n_2, a). Suppose that $m = p_1^{e_1} \cdots p_r^{e_r}$, with $p_1, \ldots, p_r$ mutually distinct prime numbers and $e_1, \ldots, e_r$ positive integers. For $d \in \{0, 1, 2, 3, 4, 5\}$, write $\nu_{d,\ell} = \min\{v_{p_\ell}(n_1 q^d - a), v_{p_\ell}(n_2)\}$. The genus of the quotient curve $\tilde{R}_q/H$ is*

$$g_H = \frac{(q^3+1)(q-2) - \Delta_H}{2|H|} + 1,$$

with $|H| = m^2/(n_1 n_2)$ and

$$\Delta_H = \left(\frac{m}{n_2} - 1\right) \cdot (q^3+1) + \sum_{d=0}^{5} \left(\frac{m \prod_{\ell=1}^{r} p_\ell^{\nu_{d,\ell}}}{n_1 n_2} - 1 \right) \cdot m.$$

Proof. The proof is very similar to the proof of Theorem 2.11 and is therefore omitted. □

The following genus, obtained using Theorem 3.10 for $s = 1$, is new up to our knowledge.

3.2. Subgroups of $\mathrm{Ree}(3) \times C_m$

Up to conjugation, $\mathrm{Ree}(3)$ has four maximal subgroups: $\mathrm{PSL}(2, 8)$, of order 504, the normalizer N_2 of a Sylow 2-subgroup, with $|N_2| = 168$, the Frobenius group $\hat{F}$ of order 54 and the subgroup $\hat{N}_+$ of order 42 normalizing a cyclic Singer group of order 7. In the following, we compute the genera of quotient curves $\tilde{R}_q/H$ when H is a subgroup of $\mathrm{Ree}(3) \times C_m$. Some special cases have been already covered in [30], precisely the cases of subgroups H of $\mathrm{Ree}(3) \times C_m$ of the form $H = K \times C_n$, with $K = \mathrm{Ree}(3)$, K subgroup of $\hat{F}$ or K subgroup of $\hat{N}_+$ and C_n subgroup of C_m.

We first complete the study of subgroups of $\mathrm{Ree}(3) \times C_m$ of the form $H = K \times C_n$, with K a subgroup of $\mathrm{Ree}(3)$ and C_n subgroup of C_m; we call these subgroups *non-skew* subgroups of $\mathrm{Ree}(3) \times C_m$. Then, we will consider subgroups of $\mathrm{Ree}(3) \times C_m$ that are not

direct product of a subgroup of Ree(3) and a subgroup of C_m; we call these subgroups *skew* subgroups of $\mathrm{Ree}(3) \times C_m$.

We start by computing the genus of the quotient curve $\tilde{\mathcal{R}}_q/H$ when H is a non-skew subgroup of $\mathrm{Ree}(3) \times C_m$ that has not been already considered in [30]. According to Theorem 3.4, it remains to study the case of $H = \mathrm{PSL}(2,8) \times C_n$ with n dividing m and the case of $H = K \times C_n$, with K subgroup of N_2 and n dividing m.

Theorem 3.11. *Let $H = \mathrm{PSL}(2,8) \times C_n$, with n dividing m. Then the genus of the quotient curve $\tilde{R}_q/H$ is*

$$g_H = \frac{(q^3+1)(q-2) - \Delta_H}{1008n} + 1,$$

with

$$\Delta_H = 63nq + 56m(q + 3q_0 + 4) + 287n + 216(\gcd(7,n) - 1)m + (n-1)(q^3+1).$$

Proof. Using GAP, one obtains that $\mathrm{PSL}(2,8)$ has one element of order 1, 63 elements of order 2, 56 elements of order 3, 216 elements of order 7 and 168 elements of order 9. Moreover, its elements of order 3 are cubes of elements of order 9, hence they lie in the center of a Sylow 3-subgroup (see the proof of Lemma 3 in [38]). From Theorem 3.6:

$$\begin{aligned}\Delta_H =& 1 \cdot (n-1)(q^3+1) + 63 \cdot n(q+1) + 56 \cdot (m(q+3q_0+1) + 1 + (n-1)) + \\ & 216 \cdot (\gcd(7,n) - 1)m + 168 \cdot ((m+1) + (n-1)).\end{aligned}$$

The conclusion follows from the Riemann–Hurwitz formula. □

The lattice of conjugacy classes of subgroups of N_2 is represented in Fig. 1; each conjugacy class $\mathcal{H}_i$ in the figure is a class of subgroups of N_2 of order i. In particular, $\mathcal{H}_{168}$ and $\mathcal{H}_1$ have size 1 and contain N_2 and $\{\mathrm{id}\}$ respectively. The figure was computed using GAP.

Subgroups in class $\mathcal{H}_{21}$ or in class $\mathcal{H}_6$ are also subgroups of $\hat{N}_+$. Thus, only the cases of K a subgroup of N_2 in class $\mathcal{H}_{168}$, $\mathcal{H}_{56}$, $\mathcal{H}_{24}$, $\mathcal{H}_{12}$, $\mathcal{H}_8$ or $\mathcal{H}_4$ are left.

Theorem 3.12. *Let $H = K \times C_n$, with K a subgroup of N_2 of order 168, 56, 24, 12, 8 or 4 and n dividing m. Then the genus of the quotient curve $\tilde{R}_q/H$ is*

$$g_H = \frac{(q^3+1)(q-2) - \Delta_H}{2n|K|} + 1,$$

with

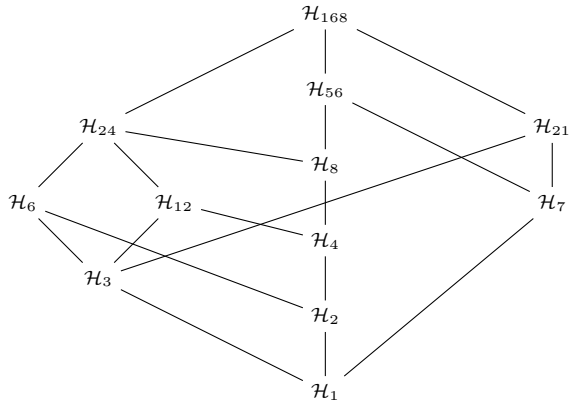

Fig. 1. Lattice of conjugacy classes of subgroups of N_2.

$$\Delta_H = \begin{cases} 7nq + 56m(3q_0+1) & \\ \quad + 119n + 48(\gcd(7,n)-1)m + (n-1)(q^3+1) & \text{if } |K| = 168, \\ 7n(q+1) + 48(\gcd(7,n)-1)m + (n-1)(q^3+1) & \text{if } |K| = 56, \\ 7nq + 8m(3q_0+1) + 23n + (n-1)(q^3+1) & \text{if } |K| = 24, \\ 3nq + 8m(3q_0+1) + 11n + (n-1)(q^3+1) & \text{if } |K| = 12, \\ 7n(q+1) + (n-1)(q^3+1) & \text{if } |K| = 8, \\ 3n(q+1) + (n-1)(q^3+1) & \text{if } |K| = 4. \end{cases}$$

Proof. Assume $|K| = 168$ first, so that $K = N_2$; using GAP, we computed that K has one element of order 1, 7 elements of order 2, 56 elements of order 3, 56 elements of order 6 and 48 elements of order 7. Moreover, its elements of order 3 do not lie in the center of a Sylow 3-subgroup. From Theorem 3.6:

$$\begin{aligned} \Delta_H =& 1 \cdot (n-1)(q^3+1) + 7 \cdot n(q+1) + 56 \cdot (m(3q_0+1) + 1 + (n-1)) + \\ & 56 \cdot n + 48 \cdot (\gcd(7,n)-1)m. \end{aligned}$$

The conclusion follows from the Riemann–Hurwitz formula. The argument for the cases of K having order 56, 24, 12, 8 or 4 is similar and is omitted. □

This completes the study of non-skew subgroups of $\mathrm{Ree}(3) \times C_m$. We now turn our attention to skew subgroups. If 7 does not divide m, then $\gcd(|\mathrm{Ree}(3)|, m) = 1$, since $\mathrm{Ree}(3)$ has order $1512 = 2^3 \cdot 3^3 \cdot 7$. Hence in this case no skew subgroups exist. It is easy to see that 7 divides m if and only if $s \equiv 2 \pmod 6$ or $s \equiv 3 \pmod 6$. In the remainder of this subsection, we will assume that m is divisible by 7. We start by narrowing down where skew subgroups of $\mathrm{Ree}(3) \times C_m$ can be located.

Lemma 3.13. *Let n be a divisor of m. Any maximal subgroup of* $\mathrm{Ree}(3) \times C_n$ *is non-skew. The same is true for the maximal subgroups of* $\mathrm{PSL}(2,8) \times C_n$.

Proof. Let $H \subseteq \mathrm{Ree}(3) \times C_n$ be a maximal subgroup. If $\gcd(n,7) = 1$, then Lemma 2.2 implies immediately that H is non-skew. If $\gcd(n,7) = 7$, the same lemma implies that if H is skew, the projection map $\pi_1 : H \to \mathrm{Ree}(3)$ is surjective. Hence for any $\sigma \in \mathrm{Ree}(3)$, there exists $\tau^k \in C_n$ such that $\sigma\tau^k \in H$. But then for any $\sigma \in \mathrm{Ree}(3)$, $\sigma^m = (\sigma\tau^k)^m \in H$. In particular, any 2-Sylow and 3-Sylow subgroup of $\mathrm{Ree}(3)$ is contained in H. Since $\mathrm{Ree}(3)$ does not contain a proper subgroup of cardinality a multiple of $2^3 \cdot 3^3$, its maximal groups having orders 504, 168, 54, and 42, we see that H contains $\mathrm{Ree}(3)$. This implies that H was non-skew after all.

A very similar argument works for maximal subgroups of $\mathrm{PSL}(2,8) \times C_n$. First one deduces that any skew subgroup contains any Sylow 2- and 3-group of $\mathrm{PSL}(2,8)$. However, the maximal subgroups of $\mathrm{PSL}(2,8)$ have order $2 \cdot 7$, $2 \cdot 3^2$ (coming from dihedral groups D_7, D_9) or $2^3 \cdot 7$ (coming from a point-stabilizer). Hence the only subgroup of $\mathrm{PSL}(2,8)$ whose order is a multiple of $2^3 \cdot 3^2$, is $\mathrm{PSL}(2,8)$ itself. Hence also in this case, H is non-skew. □

This lemma combined with Lemma 2.2 and the last part of Theorem 3.4 implies that a skew subgroup of $\mathrm{Ree}(3) \times C_m$ is a subgroup of $N_2 \times C_m$, $\hat{F} \times C_m$, or of $\hat{N}_+ \times C_m$. Since $\gcd(|\hat{F}|, m) = 1$ and skew subgroups of $\hat{N}_+ \times C_m$ are necessarily contained in $C_7 \times C_m$ (shown similarly as Proposition 3.9), it is enough to investigate skew subgroups of $N_2 \times C_m$. We start by considering maximal subgroups of this group. The subgroup lattice of N_2 depicted in Fig. 1 will be very convenient. For any i, we denote by H_i a representative subgroup from the conjugation class $\mathcal{H}_i$.

Lemma 3.14. *Let n be a divisor of m. Any skew subgroup of $N_2 \times C_n$ has a conjugate contained in $H_{56} \times C_n$.*

Proof. If $\gcd(n,7) = 1$, no skew subgroups of $N_2 \times C_n$ exist and there is nothing to prove. Assume therefore that $7|n$. Write $C_n = \langle \tilde{\tau} \rangle$ and $N_2 = \langle s_1, s_2, s_3, l, r \rangle$, with s_1, s_2, s_3 of order 2 generating a 2-Sylow subgroup, l of order 3, r of order 7, satisfying $lrl^{-1} = r^2$ and several other relations that we will not need.

Then we can choose $H_{56} := \langle s_1, s_2, s_3, r \rangle$, $H_{24} := \langle s_1, s_2, s_3, l \rangle$ and $H_{21} := \langle l, r \rangle$. Now first suppose that H be a maximal subgroup of $N_2 \times C_n$ that is skew. Then, reasoning as in the proof of Lemma 3.13, we can conclude that after a suitable conjugation H_{24} is contained in H and that for any $\sigma \in N_2$, there exists k such that $\sigma\tilde{\tau}^k \in H$. In particular $r\tilde{\tau}^a \in H$ for some integer a. It follows that $H \ni (lr\tilde{\tau}^a l^{-1})(r\tilde{\tau}^a)^{-1} = r$. But then $N_2 \subseteq H$, so H is not skew after all. We may conclude that any maximal subgroup of $N_2 \times C_n$ is non-skew and therefore up to conjugation is of the form $H_{21} \times C_n$, $H_{24} \times C_n$, $H_{56} \times C_n$, $N_2 \times C_{n/7}$, or $N_2 \times C_{n/p}$, for some prime number p distinct from 7, dividing n.

Using Lemma 2.2, we see that any skew subgroup of $N_2 \times C_n$ has a conjugate contained in $H_{21} \times C_n$, $H_{56} \times C_n$, or $N_2 \times C_{n/p}$. In the latter case, the above argument can be

iterated leading to the conclusion that a skew subgroup of $N_2 \times C_{n/p}$ has a conjugate contained in $H_{21} \times C_n$ or $H_{56} \times C_n$. Now, with a similar reasoning as before, one can show that up to conjugation all maximal subgroups of $H_{21} \times C_n$ are $\langle l \rangle \times C_n$, $\langle r \rangle \times C_n$, $H_{21} \times C_{n/7}$, and $H_{21} \times C_{n/p}$, for some prime number p distinct from 7, dividing n. Hence any skew subgroup of $H_{21} \times C_n$ has a conjugate contained in $\langle r \rangle \times C_n \subset H_{56} \times C_n$. The lemma now follows. □

It remains to analyze the skew subgroups of $H_{56} \times C_m$, where $H_{56} = \langle s_1, s_2, s_3, r \rangle$ is the unique subgroup of N_2 in the conjugation class $\mathcal{H}_{56}$.

Theorem 3.15. *Assume $7 \mid m$. All skew subgroups of $H_{56} \times C_m$ are either of the form $H_{i,w} := \langle s_1, s_2, s_3, r\tau^{iw} \rangle$ or of the form $H'_{i,w} := \langle r\tau^{iw} \rangle$, for $1 \leq i \leq 6$ and $7w \mid m$. Define $n := \frac{m}{7w}$. The genus of the quotient curve $\tilde{R}_q/H_{i,w}$ is*

$$g_{H_{i,w}} = \frac{(q^3+1)(q-n-1) - 7n(q+1) - \delta}{16m} \cdot w + 1,$$

where $\delta = 0$ if $7 \mid n$ and $\delta = 48m$ if $7 \nmid n$. The genus of the quotient curve $\tilde{R}_q/H'_{i,w}$ is

$$g_{H'_{i,w}} = \frac{(q^3+1)(q-n-1) - \delta'}{2m} \cdot w + 1,$$

where $\delta' = 0$ if $7 \mid n$ and $\delta' = 6m$ if $7 \nmid n$.

Proof. Observe that H_{56} can be presented as $H_{56} := \langle s_1, s_2, s_3, r \rangle$ as in the proof of Lemma 3.14 with $s_1^2 = s_2^2 = s_3^2 = \mathrm{id} = r^7$, $rs_1 = s_2 r$, $rs_2 = s_3 r$, and $rs_3 = s_2 s_1 r$. The s_i commute with each other, meaning that the group $\langle s_1, s_2, s_3 \rangle$ is an elementary abelian 2-group of order eight. The group H_{56} has exactly one subgroup of index 7, namely $\langle s_1, s_2, s_3 \rangle$, the Sylow 2-subgroup of N_2 of order 8. By definition N_2 is the normalizer of a 2-Sylow subgroup of Ree(3). Since the 2-Sylow subgroup of N_2 is contained in H_{56}, it is also normal in H_{56}. Hence H_{56} has one element of order 1 and seven elements of order 2. One can check that the remaining 48 elements have order seven. This means that any cyclic subgroup of H_{56} of order 7 is conjugated with $\langle r \rangle$. In particular, such subgroups are not normal. From Fig. 1 we conclude that a nontrivial normal subgroup of H_{56}, necessarily is contained in the 2-Sylow subgroup $\langle s_1, s_2, s_3 \rangle$. In particular $[H_{56}, H_{56}] \subset \langle s_1, s_2, s_3 \rangle$, where $[H_{56}, H_{56}]$ denotes the commutator subgroup of H_{56}. Also, Sylow's theorem implies that the normalizer of $\langle r \rangle$ in H_{56} is $\langle r \rangle$ itself, since it needs to have index eight in H_{56}. As a consequence, the only elements in H_{56} that commute with r are powers of r.

Now let $H \subset H_{56} \times C_m$ be a skew subgroup and denote by $\pi_1 : H \to H_{56}$ the projection on the first coordinate. If $s \in \pi_1(H)$ has order two, then $s \in H$, since for any $\tau^a \in C_m$, $s = (s\tau^a)^m \in H$. Since H is skew, this implies that there exists an element $\tilde{r} \in H_{56}$ of order seven and $\tau^a \in C_m$ such that $\tilde{r}\tau^a \in H$. Since all subgroups of order seven in H_{56}

are conjugated, this means that a conjugate of H contains an element of the form $r^i\tau^a$ for some $i \in \{1,\dots,6\}$. Redefining H to be that conjugate, we conclude that $r\tau^b \in H$ for some positive integer b, by taking a suitable power of the element $r^i\tau^a$. Now let n_2 the smallest positive integer such that $\tau^{n_2} \in H$ and $0 \le a < n_2$ be the smallest nonnegative integer such that $r\tau^a \in H$.

If $H = \langle r\tau^a, \tau^{n_2}\rangle$, then since H is skew, we have $a > 0$. Note that from Lemma 2.8, we may conclude that $n_2|7a$ and since $0 < a < n_2$ implies $n_2 \not| a$, we have $n_2/7|a$. In particular, $a = in_2/7$ for some $i = 1,\dots,6$, which implies that a suitable power of $r\tau^a$ is equal to τ^{n_2}. Here we used $\gcd(i,m) = 1$ for $i = 1,\dots,6$. We conclude that $H = \langle r\tau^a\rangle$. Defining $w = n_2/7$, we see that $H = H'_{i,w}$. Note that the genus of $\tilde{\mathcal{R}}_q/H'_{i,w}$ is the same as the one corresponding to the subgroup of $C_m \times C_m$ with standard exponents $(m/7, n_2, a)$. Therefore, that genus can be obtained directly from Theorem 3.10. Writing $p_1 = 7$, first of all note that if $p_\ell \neq 7$, then $\nu_{d,\ell} = v_{p_\ell}(n_2)$, since $n_1 = m/7$ and $n_2/7|a$. Also note that since q has multiplicative order six modulo m and we assume that 7 divides m, the element q is a primitive element modulo seven. Moreover, we have $\frac{m}{7}q^d - a = \frac{n_2}{7}\left(\frac{m}{n_2}q^d - i\right)$ for some $1 \le i \le 6$. Hence, we see that if $7|m/n_2$, then $\nu_{d,1} = v_7(n_2/7) = v_7(n_2) - 1$ for all d, while if $7 \not| m/n_2$, then there exists exactly one d such that $\nu_{d,1} = v_7(n_2)$, while $\nu_{d,1} = v_7(n_2) - 1$ for the remaining values of d. Combining the above, we see that

$$\Delta_{H'_{i,w}} = \left(\frac{m}{7w} - 1\right)\cdot(q^3+1) \quad \text{if 7 divides } \frac{m}{n_2}$$

and

$$\Delta_{H'_{i,w}} = \left(\frac{m}{7w} - 1\right)\cdot(q^3+1) + (7-1)\cdot m \quad \text{if 7 does not divide } \frac{m}{n_2}.$$

The stated genus formula for $g_{H'_{i,w}}$ now follows.

Now suppose that $\langle r\tau^a\rangle \subsetneq H$ and choose an element $g\tau^b \in H \setminus \langle r\tau^a\rangle$ for some $g \in H_{56}$. Then $H \ni r\tau^a g\tau^b\tau^{-a}r^{-1}\tau^{-b}g^{-1} = rgr^{-1}g^{-1}$ is an element of the commutator subgroup of H_{56} and hence in $\langle s_1, s_2, s_3\rangle$. We denote this element by s. If $s = rgr^{-1}g^{-1} = \mathrm{id}$, then g would have been a power of r, but then $g\tau^b \in \langle r\tau^a\rangle = \langle r\tau^a, \tau^{n_2}\rangle$ from the definition of a and n_2. Hence H contains the element $s \in \langle s_1, s_2, s_3\rangle \setminus \{\mathrm{id}\}$. Now conjugation by $r\tau^a$ permutes the elements of the set $\langle s_1, s_2, s_3\rangle \setminus \{\mathrm{id}\}$ with a permutation of order a divisor of seven. Since $rs_1r^{-1} = s_2$, the action is not trivial. Hence conjugation by $r\tau^a$ cyclically permutes the elements of the set $\langle s_1, s_2, s_3\rangle \setminus \{\mathrm{id}\}$. In particular, we may conclude that $\langle s_1, s_2, s_3\rangle \subset H$, implying that $H = \langle s_1, s_2, s_3, r\tau^a\rangle = H_{i,w}$. The genus computation is now very similar as before. The eight cyclic subgroups $\langle sr\tau^a\rangle$, with $s \in \langle s_1, s_2, s_3\rangle \setminus \{\mathrm{id}\}$, give rise to the contribution δ to $\Delta_{H_{i,w}}$, while the elements of the form $s\tau^{jn_2}$ give rise to the contribution $7m/n_2(q+1)$. The remaining elements of the form τ^{jn_2} give the contribution $(m/n_2 - 1)(q^3+1)$. □

The following genera, obtained using Theorems 3.11 and 3.12 for $s = 1$, are new up to our knowledge. Note that for $s = 1$ Theorem 3.15 cannot give new genera, because 7 does not divide m in this case.

Acknowledgments

The first and third author would like to acknowledge the support from The Danish Council for Independent Research (DFF-FNU) for the project *Correcting on a Curve*, Grant No. 8021-00030B.

References

[1] M. Abdon, L. Quoos, On the genera of subfields of the Hermitian function field, Finite Fields Appl. 10 (2004) 271–284.
[2] N. Anbar, P. Beelen, A. Bassa, A complete characterization of Galois subfields of the generalized Giulietti–Korchmaros function field, Finite Fields Appl. 48 (2017) 318–330.
[3] A. Bassa, L. Ma, C. Xing, S.L. Yeo, Towards a characterization of subfields of the Deligne–Lusztig function fields, J. Comb. Theory, Ser. A 120 (7) (2013) 1351–1371.
[4] P. Beelen, L. Landi, M. Montanucci, Weierstrass semigroups on the Skabelund maximal curve, Finite Fields Appl. 72 (2021) 101811.
[5] P. Beelen, M. Montanucci, A new family of maximal curves, J. Lond. Math. Soc. 98 (3) (2018) 573–592.
[6] P. Beelen, M. Montanucci, On subfields of the second generalization of the GK maximal function field, Finite Fields Appl. 64 (2020) 101669.
[7] E. Çakçak, F. Özbudak, Subfields of the function field of the Deligne–Lusztig curve of Ree type, Acta Arith. 115 (2004) 133–180.
[8] E. Çakçak, F. Özbudak, Number of rational places of subfields of the function field of the Deligne–Lusztig curve of Ree type, Acta Arith. 120 (1) (2005) 79–106.
[9] A. Cossidente, G. Korchmáros, F. Torres, On curves covered by the Hermitian curve, J. Algebra 216 (1999) 56–76.
[10] A. Cossidente, G. Korchmáros, F. Torres, Curves of large genus covered by the Hermitian curve, Commun. Algebra 28 (10) (2000) 4707–4728.
[11] F. Dalla Volta, M. Montanucci, G. Zini, On the classification problem for the genera of quotients of the Hermitian curve, Commun. Algebra 47 (12) (2019) 4889–4909.
[12] Y. Danişman, M. Özdemir, On the genus spectrum of maximal curves over finite fields, J. Discrete Math. Sci. Cryptogr. 18 (5) (2015) 513–529.
[13] I. Duursma, A. Eid, Smooth embeddings for the Suzuki and Ree curves, in: Algorithmic Arithmetic, Geometry, and Coding Theory, vol. 637, 2015, pp. 251–291.
[14] S. Fanali, M. Giulietti, On some open problems on maximal curves, Des. Codes Cryptogr. 56 (2010) 131–139.
[15] S. Fanali, M. Giulietti, Quotient curves of the GK curve, Adv. Geom. 12 (2012) 239–268.
[16] R. Fuhrmann, A. Garcia, F. Torres, On maximal curves, J. Number Theory 67 (1) (1997) 29–51.
[17] R. Fuhrmann, F. Torres, The genus of curves over finite fields with many rational points, Manuscr. Math. 89 (1996) 103–106.
[18] A. Garcia, Curves over finite fields attaining the Hasse–Weil upper bound, in: European Congress of Mathematics, vol. II, Barcelona, 2000, in: Progr. Math., vol. 202, Birkhäuser, Basel, 2001, pp. 199–205.
[19] A. Garcia, On curves with many rational points over finite fields, in: Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer, Berlin, 2002, pp. 152–163.
[20] A. Garcia, C. Güneri, H. Stichtenoth, A generalization of the Giulietti–Korchmáros maximal curve, Adv. Geom. 10 (3) (2010) 427–434.
[21] A. Garcia, H. Stichtenoth, Topics in Geometry, Coding Theory and Cryptography, Algebra and Application, vol. 6, Springer, Dordrecht, 2007.
[22] A. Garcia, H. Stichtenoth, C. Xing, On subfields of the Hermitian function field, Compos. Math. 120 (2000) 137–170.

[23] G. van der Geer, Curves over finite fields and codes, in: European Congress of Mathematics, vol. II, Barcelona, 2000, in: Progr. Math., vol. 202, Birkhäuser, Basel, 2001, pp. 225–238.
[24] G. van der Geer, Coding theory and algebraic curves over finite fields: a survey and questions, in: Applications of Algebraic Geometry to Coding Theory, Physics and Computation, in: NATO Sci. Ser. II Math. Phys. Chem., vol. 36, Kluwer, Dordrecht, 2001, pp. 139–159.
[25] G. van der Geer, M. van der Vlugt, Generalized Reed–Muller codes and curves with many points, J. Number Theory 72 (1998) 257–268.
[26] G. van der Geer, M. van der Vlugt, How to construct curves over finite fields with many points, preprint arXiv:alg-geom/9511005v2.
[27] M. Giulietti, J.W.P. Hirschfeld, G. Korchmáros, F. Torres, A family of curves covered by the Hermitian curve, Semin. Congr. 21 (2009) 63–78.
[28] M. Giulietti, G. Korchmáros, A new family of maximal curves over a finite field, Math. Ann. 343 (2009) 229–245.
[29] M. Giulietti, G. Korchmáros, F. Torres, Quotient curves of the Suzuki curve, Acta Arith. 122 (3) (2006) 245–274.
[30] M. Giulietti, M. Montanucci, L. Quoos, G. Zini, On some Galois covers of the Suzuki and Ree curves, J. Number Theory 189 (2018) 220–254.
[31] M. Giulietti, L. Quoos, G. Zini, Maximal curves from subcovers of the GK-curve, J. Pure Appl. Algebra 220 (10) (2016) 3372–3383.
[32] C. Güneri, M. Özdemir, H. Stichtenoth, The automorphism group of the generalized Giulietti–Korchmaros function field, Adv. Geom. 13 (2013) 369–380.
[33] L. Héthelyi, E. Horváth, F. Petényi, The depth of subgroups of Suzuki groups, Commun. Algebra 43 (10) (2015) 4553–4569.
[34] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics, Princeton, 2008.
[35] B. Huppert, N. Blackburn, Finite Groups III, Springer-Verlag, Berlin Heidelberg, 1982.
[36] G. Lachaud, Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, C. R. Acad. Sci., Sér. 1 Math. 305 (16) (1987) 729–732.
[37] K. Lauter, Deligne–Lusztig curves as ray class fields, Manuscr. Math. 98 (1) (1999) 87–96.
[38] V.M. Levchuk, Ya.N. Nuzhin, Structure of Ree groups, Algebra Log. 24 (1) (1985) 16–26.
[39] H. Lüneburg, Die Suzukigruppen und ihre Geometrien, Lecture Notes in Mathematik, vol. 10, Springer-Verlag, Berlin, 1965.
[40] L. Ma, C. Xing, On subfields of the Hermitian function fields involving the involution automorphism, J. Number Theory 198 (2019) 293–317.
[41] M. Montanucci, G. Zini, On the spectrum of genera of quotients of the Hermitian curve, Commun. Algebra 46 (11) (2018) 4739–4776.
[42] M. Montanucci, G. Zini, Quotients of the Hermitian curve from subgroups of $\mathrm{PGU}(3, q)$ without fixed points or triangles, J. Algebraic Comb. 52 (3) (2019) 339–368.
[43] M. Montanucci, G. Zini, The complete list of genera of quotients of the $\mathbb{F}_{q^2}$-maximal Hermitian curve for $q \equiv 1 \pmod 4$, J. Algebra 550 (2020) 23–53.
[44] J.P. Pedersen, A function field related to the Ree group, Lect. Notes Math. 1518 (1992) 122–131.
[45] D.C. Skabelund, New maximal curves as ray class fields over Deligne–Lusztig curves, Proc. Am. Math. Soc. 146 (2) (2017) 525–540.
[46] H. Stichtenoth, Algebraic Function Fields and Codes, Graduate Texts in Mathematics, vol. 254, Springer, Berlin, 2009.