QUOTIENT CURVES OF THE SUZUKI CURVE

MASSIMO GIULIETTI, GÁBOR KORCHMÁROS, AND FERNANDO TORRES

Abstract. A systematic study of the genera and plane models of quotient curves of the Suzuki curve $y^{2s+1} - y = x^{2s}(x^{2s+1} - x)$, $s \in \mathbb{N}$, is carried out.

1. Introduction

Throughout, let $K = \mathbb{F}_q$ be the finite field of order $q$ and $\bar{K}$ its algebraic closure. For a projective, geometrically irreducible, non-singular algebraic curve defined over $K$ (or simply, a curve over $K$) of genus $g > 0$, the inequality $|\#\mathcal{X}(K) - (q + 1)| \leq 2g\sqrt{q}$ is the Hasse-Weil bound on the number of its $K$-rational points. For possible applications to coding theory [13], [31], [9], correlations of shift register sequences [22], exponential sums [25], or finite geometry [19] one is often interested in those curves with “many rational points”. For $q$ a square, the Hermitian curve over $K : Y\sqrt{q}Z + YZ\sqrt{q} = X\sqrt{q} + 1$ attains the Hasse-Weil upper bound; that is to say, it is a maximal curve (see e.g. [31, VI.3.6]).

Let $N_q(g)$ denote the maximum number of $K$-rational points on a curve of genus $g$; see Section 7 for further information. A curve over $\bar{K}$ of genus $g$ whose number of rational points coincides with $N_q(g)$ is called optimal. There are three outstanding families of such curves, namely the curves (of positive genus) arising as Deligne-Lusztig varieties of dimension one (DLC); these families are characterized by the following data regarding their number of $K$-rational points, genus and automorphism group over $\bar{K}$ (which actually coincides with the automorphism group over $K$); see [5, Sect. 11], [14], [27], [15].

<table>
<thead>
<tr>
<th>Type</th>
<th>Number of rational points</th>
<th>Genus</th>
<th>Automorphism group</th>
</tr>
</thead>
<tbody>
<tr>
<td>I: $q$ square</td>
<td>$\sqrt{q}^s + 1$</td>
<td>$\sqrt{q}(\sqrt{q} - 1)/2$</td>
<td>$PGU(3, q)$</td>
</tr>
<tr>
<td>II: $q = 2q_0^2 &gt; 2$</td>
<td>$q^2 + 1$</td>
<td>$q_0(q - 1)$</td>
<td>$Sz(q)$</td>
</tr>
<tr>
<td>III: $q = 3q_0^2 &gt; 3$</td>
<td>$q^3 + 1$</td>
<td>$3q_0(q - 1)(q + q_0 + 1)/2$</td>
<td>$R(q)$</td>
</tr>
</tbody>
</table>

In addition, the enumerator $L(t)$ of their Zeta function is known (loc. cit.). In the table above $PGU(3, q), Sz(q)$ and $R(q)$ stand for the projective unitary group of degree three, the Suzuki group, and the Ree group over $K$ respectively. The genus, the number of rational points, and the automorphism group of a Hermitian curve coincide with those of a DLC of type I. It turns out that the number of rational points and the genus are the essential data to characterize both Hermitian curves and DLC of type II; see [28], [6, Sect. 3]. (A similar statement for the DLC of type III seems to be unknown.) Motivated by the optimality of a DLC $\mathcal{X}$ and Serre’s remark (cf. [21, Prop. 6], [1, Prop. 5]), see Section


Keywords: Finite field, Suzuki group, Quotient curve, Curves with many rational points.

here, one expects to obtain curves with many rational points from curves \( \tilde{X} \) that are \( K \)-covered by \( X \). Having in mind applications it is also important to have such curves in a form as explicit as possible. If \( X \) is the Hermitian curve over \( K \), then \( L(t) = (\sqrt{q^2t + 1})^{2g} \) with \( g = \sqrt{q^2} - 1 \); see e.g. [31, V.1.15]. Thus by the aforementioned Serre’s remark, the number of \( K \)-rational points of \( \tilde{X} \) also attains the Hasse-Weil upper bound.

In particular, by means of quotient curves of \( X \), the genus and plane models of a huge number of maximal curves were found; see e.g. [7], [3] and [4].

The aim of this paper is to investigate quotient curves of the DLC of type II; such a curve will be called the Suzuki curve (over \( K \)) and will be denoted by \( S \). The case of curves of Type III was investigated by Cakcak and Ozbudak [2].

From now on, \( q_0 := 2^s \) with \( s \geq 1 \), and \( q := 2q_0^2 \). The enumerator of the Zeta function of \( S \) is the polynomial \( L(t) = (qt^2 + 2q_0t + 1)^g \), with \( g = q_0(q - 1) \); see e.g. [14, Prop. 4.3]. Thus the number of \( K \)-rational points of a curve \( \tilde{S} \) of genus \( \tilde{g} \) which is \( K \)-covered by \( S \) is given by (cf. Section 3)

\[
\#\tilde{S}(K) = q + 2q_0\tilde{g} + 1.
\]

This value is in the interval from which the entries of the tables of curves with many rational points are taken for \( \tilde{g} \leq 50 \), \( q \leq 128 \) in van der Geer and van der Vlugt tables [8]. In Sections 4 and 5 we obtain an exhaustive list of tame quotient curves of \( S \), namely quotients arising from subgroups of Aut(\( S \)) of odd order: indeed, we compute the genus as well as exhibit a plane model for such curves. In Section 6 we consider non-tame quotient curves of \( S \), namely quotient arising from subgroups of Aut(\( S \)) of even order; here we cannot produce a complete list as in the odd case because the Suzuki group contains a huge number of pairwise non-isomorphic subgroups of even order. Our contribution consists in proving the existence of non-tame quotient curves of \( S \); for some of these curves we also provide a plane equation. A concrete application of our results provide new entries in the tables [8]: let \( q = 32 \) and \( r = 5 \); from Theorems 5.1(2) and 6.10(2) we have \( N_{32}(24) \geq 225 \) and \( N_{32}(10) \geq 113 \) respectively; cf. Section 7.

The approach employed in this paper is similar as in [3] and [4]: a concrete realization of \( S \) in \( \mathbb{P}^4 \) is stated via a very ample complete linear series obtained from the enumerator of its Zeta function (cf. Section 3); this embedding is such that \( S_\mathbb{Z}(q) \) acts linearly on \( S \) (cf. Section 2 and Theorem 3.2).

2. Preliminary results on the Suzuki group

In the course of the Introduction we have mentioned that the automorphism group Aut(\( S \)) of the Suzuki curve \( S \) is isomorphic to the Suzuki group \( S_\mathbb{Z}(q) \). We summarize those results on the structure of \( S_\mathbb{Z}(q) \) which play a role in the present work. For more details, the reader is referred to [20, Chap. XI.3], [33], [12, Chap. 17] and [23].

In Section 3 we will show that the curve \( S \) can be embedded in \( \mathbb{P}^4 \) (Theorem 3.1); this raises the problem of exhibit \( S_\mathbb{Z}(q) \) as a subgroup of automorphisms of \( \mathbb{P}^4 \). We start from a well-known concrete realization of \( S_\mathbb{Z}(q) \), namely as a subgroup of the automorphism group Aut(\( \mathbb{P}^3 \)) of \( \mathbb{P}^3 \) (loc. cit.). Let \( \tilde{T} := \{T_{a,c} : a, c \in K \} \) and \( \tilde{N} := \{N_d : d \in K^*\}, \)
where $T_{a,c}$ and $N_d$ are the elements of $\text{Aut}(\mathbb{P}^3)$ defined respectively by the matrices
\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
am & 1 & 0 & 0 \\
c & a^{2q_0 + 2} + ac + c^{2q_0} & a^{2q_0 + 1} + c & a & 1
\end{pmatrix},
\quad \text{and} \quad
\begin{pmatrix}
d^{-q_1 - 1} & 0 & 0 & 0 \\
0 & d^{-q_1} & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & d^{q_1 + 1}
\end{pmatrix}.
\]
In addition, let $W \in \text{Aut}(\mathbb{P}^3)$ be defined by the matrix
\[
\begin{pmatrix}
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0
\end{pmatrix}.
\]
Then the Suzuki group $Sz(q)$ can be assumed as the subgroup of $\text{Aut}(\mathbb{P}^3)$ generated by $\widetilde{T}, \widetilde{N}$ and $W$. Next consider the homomorphism of groups
\[
L : Sz(q) \to \text{Aut}(\mathbb{P}^4)
\]
defined on the generators of $Sz(q)$ by $T_{a,c} \mapsto T_{a,c}, N_d \mapsto N_d, W \mapsto W$, where the images are defined respectively by the matrices:
\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
am & 1 & 0 & 0 \\
c & a^{q_1 + 1} + c^{q_1} & a^{q_1} & 1 & 0 \\
(a^{q_1} + 1 + c^{q_1}) & c & a^{2q_1} & 0 & 1 & 0 \\
(a^{2q_1 + 2} + ac + c^{2q_1}) & a^{2q_1 + 1} + c & 0 & a & 1
\end{pmatrix},
\quad \text{and} \quad
\begin{pmatrix}
d^{-q_1 - 1} & 0 & 0 & 0 & 0 \\
0 & d^{-q_1} & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 0 & d^{q_1} & 0 & 0 \\
0 & 0 & 0 & d^{q_1 + 1} & 0
\end{pmatrix}.
\]
Let $\widetilde{T} := L(\widetilde{T}), \widetilde{N} := L(\widetilde{N})$ and $W := L(W)$. Then, as $Sz(q)$ is simple (loc. cit.), we can assume that $Sz(q)$ is the subgroup of $\text{Aut}(\mathbb{P}^4)$ generated by $\widetilde{T}, \widetilde{N}$ and $W$. Some other basic properties of the Suzuki group that we shall need are the following (loc. cit.):

(2.1) A cyclic subgroup of $Sz(q)$ of order $r > 1$, $r$ a divisor of $q - 1$, is conjugate in $Sz(q)$ to the subgroup $\{N_d \in \tilde{N} : d \in K, d^r = 1\};$

(2.2) Up to conjugacy there exist two cyclic subgroups of $Sz(q)$, $S_1$ and $S_{-1}$, of order $q + 2q_0 + 1$ and $q - 2q_0 + 1$ respectively. Such subgroups are called the Singer subgroups of $Sz(q)$. Also, their action on the $K$-rational points of $\pi(S)$, where $\pi$ is the morphism defined in (3.6), is semiregular;

(2.3) The subgroup $\widetilde{T}$ has exponent 4; that is to say, the maximum order of its elements is 4. Its center is an elementary abelian group of order $q$, say $\widetilde{T}_2$, whose elements are those of order $2$ of $T$. Furthermore, the normaliser of $\widetilde{T}$ in $Sz(q)$ acts transitively on $\widetilde{T}_2$;

(2.4) The cyclic subgroups of $Sz(q)$ of order 4 are pairwise conjugate in $Sz(q)$;
(2.5) A subgroup of $S_z(q)$ of order $2^v$, $r, v > 1$, $r$ a divisor of $q - 1$, is conjugate in $S_z(q)$ to a subgroup of $\tilde{T}\tilde{N}$. The order of a non-trivial element in $\tilde{T}\tilde{N}$ is either a 2-power or a divisor of $q - 1$ according as it belongs to $\tilde{T}$ or not;

(2.6) A subgroup of $S_z(q)$ of order $2r$, $r > 1$ a divisor of $q - 1$, is conjugate in $S_z(q)$ to a subgroup of $N_{S_z(q)}(\tilde{N})$, the normalizer of $\tilde{N}$ in $S_z(q)$. The subgroup $N_{S_z(q)}(\tilde{N})$ is dihedral with $2(q - 1)$ elements.

(2.7) A subgroup of $S_z(q)$ of order $2r$, $r > 1$ a divisor of $q \pm 2q_0 + 1$, is conjugate in $S_z(q)$ to a subgroup of the (unique) dihedral group of $S_z(q)$ which comprises $S_{\pm 1}$.

(2.8) A subgroup of $S_z(q)$ of order $4r$, $r > 1$ a divisor of $q \pm 2q_0 + 1$, is conjugate in $S_z(q)$ to a subgroup of $N_{S_z(q)}(S_{\pm 1})$, the normalizer of $S_{\pm 1}$ in $S_z(q)$. The subgroup $N_{S_z(q)}(S_{\pm 1})$ has $4(q \pm 2q_0 + 1)$ elements.

(2.9) Set $\tilde{q} := 2^{2q+1}$. A necessary and sufficient condition for $S_z(q)$ to contain a subgroup isomorphic to $S_z(\tilde{q})$ is that $\tilde{q}$ be a divisor of $q$ such that $2\tilde{s} + 1$ divides $2s + 1$. For every such divisor, $S_z(q)$ has exactly one conjugacy class of subgroups isomorphic to $S_z(\tilde{q})$.

(2.10) Any non-trivial subgroup of $S_z(q)$ is conjugate in $S_z(q)$ to one of the above subgroups.

3. Preliminary results on the Suzuki curve

Let $S$ be the Suzuki curve over $K$ ($q = 2q_0^2 > 2$) and $\pi : S \to \mathcal{S}$ a $K$-covering of curves over $K$. Let $L(t)$ and $L_{\mathcal{S}}(t)$ be the enumerator of the $Z$-function (over $K$) of $S$ and $\mathcal{S}$ respectively. An observation due to Serre states that $L_{\mathcal{S}}(t)$ divides $L(t)$ (see [21, Prop. 6], [1, Prop. 5]). As $L(t) = (qt^2 + 2q_0t + 1)^{g}$, where $g$ is the genus of $S$ (see [14, Prop. 4.3], [27]), we have $L_{\mathcal{S}}(t) = (qt^2 + 2q_0t + 1)^{\tilde{g}}$, $\tilde{g}$ being the genus of $\mathcal{S}$. In particular, the number of $\mathbb{F}_{q^r}$-rational points of $\mathcal{S}$, $r \in \mathbb{N}$, can be computed as follows (see e.g. [31, V.1.15])

\[(3.1) \quad \#\mathcal{S}(\mathbb{F}_{q^r}) = q^r + 1 - [(1 + i)^r + (1 - i)^r](-q_0)^r \tilde{g},\]

where $i = \sqrt{-1}$. Notice that $\mathcal{S}$ is maximal over $\mathbb{F}_{q^4}$. Next we describe a plane model of $S$ which will be the starting point towards the proof of our results. Hansen and Stichtenoth [16] noticed that the number of $K$-rational points and the genus of the non-singular model over $K$ of the plane curve

\[(3.2) \quad y^q + y = x^{q_0}(x^q + x) \quad (q = 2q_0^2 > 2)\]

are $q^2 + 1$ and $q_0(q - 1)$ respectively. Therefore by [6, Sect. 3], we may assume that $S$ is the non-singular model of (3.2). We recall that Henn [18] exhibited this curve as an example of a curve whose number of automorphisms exceeds the Hurwitz upper bound $84(q - 1)$ valid in zero characteristic.

Now we introduce a geometric invariant (over $K$) on the curve $S$. Among other properties, this invariant will allow us to consider $S$ as an embedded curve in $\mathbb{P}^4$ in such a way that $S_z(q)$ will act linearly on $S$; see Theorem 3.2. Let $h(t) := t^{2q}L(t^{-1})$ with $L(t)$ as above. This polynomial is the characteristic polynomial of the Frobenius morphism $\Phi$ over $K$ on the Jacobian $J$ of $S$; this morphism is induced by the Frobenius morphism $\Phi$ over $K$ on $S$. It turns out that $\Phi$ is semi-simple (see e.g. [26, p. 251]) and thus
We can state this property by using divisors on $S$; to do that
we use the fact that $f \circ \Phi = \Phi \circ f$, where $f : S \to J$, $P \mapsto [P - P_0]$, is the natural
morphism that maps $P_0 \in S(K)$ to $0 \in J$. Therefore, for $P \in S$ and $P_0 \in S(K)$ the
following linear equivalence on $S$ holds true:

$$qP + 2q_0 \Phi(P) + \Phi^2(P) \sim (q + 2q_0 + 1)P_0.$$  

This motivates the definition of the following complete linear series on $S$:

$$D = D_S := |(q + 2q_0 + 1)P_0|.$$  

The equivalence (3.3) shows that the definition of $D$ is independent of the $K$-rational point
$P_0$, and that $q + 2q_0 + 1$ belongs to the Weierstrass semigroup $H(P)$ at any $K$-rational
point $P \in S$. We subsume two important properties of $D$:

**Theorem 3.1.**  
(1) ([16, Prop. 1.5]) The dimension of $D$ is four;  
(2) The linear series $D$ is very ample.

**Proof.** (1) Let $P \in S(K)$, and $i \in \mathbb{N}$ such that $n_i = q + 2q_0 + 1 \in H(P)$; by (3.3) we have
to show that $i = 4$. Let $x, y : S \to \mathbb{P}^1$ be the $K$-rational functions on $S$ which define its
plane model (3.2). We have that $x$ is unramified in $\mathbb{P}^1$ but at $\infty$. Over $x = \infty$ there is
just one point, say $P_0 \in S$, which is, in particular, $K$-rational. It turns out that

$$\text{div}_\infty(x) = qP_0, \quad \text{and} \quad \text{div}_\infty(y) = (q + q_0)P_0.$$  

Let us put

$$z := x^{2q_0 + 1} + y^{2q_0}.$$  

By (3.2) the functions $x$ and $z$ satisfy

$$z^q + z = x^{2q_0}(x^q + x);$$

therefore, $\text{div}_\infty(z) = (q + 2q_0)P_0$ and so $H(P_0)$ contains the semigroup $H$ generated by
$q, q + q_0, q + 2q_0$ and $q + 2q_0 + 1$. After some computations, one shows that $\#(\mathbb{N} \setminus H) = q_0(q - 1)$ (see e.g. [16, Appendix]); thus $H(P_0) = H$ and so $i = 4$.

(2) Let $\pi : S \to \mathbb{P}^4$ be the morphism defined by $D$. We show that $\pi$ separates points
and separates tangent vectors; cf. [17, p. 308]. To see the former condition, it is enough to
show that $\pi$ is injective. Assume $\pi(P) = \pi(Q)$. Then the linear equivalence (3.3) implies
$\{P, \Phi(P), \Phi^2(P)\} = \{Q, \Phi(Q), \Phi^2(Q)\}$. We find that $\Phi^3(P) = P$ and $\Phi^3(Q) = Q$; thus
$P = Q$ since $S(F_{q^3}) = S(K)$ by (3.1). To prove the latter condition we use some facts
concerning Weierstrass point theory; our reference is Stöhr-Voloch paper [32]. We have
to show that the first positive element $j_1 = j_1(P)$ of the $(D, P)$-order sequence equals 1,
or equivalently that there exists $D' \in D$ such that $v_P(D') = 1$. If $P \notin S(K)$, $j_1 = 1$ by
(3.1) and (3.3); otherwise, let $n_1 < n_2 < n_3 < n_4 = q + 2q_0 + 1$ be the first four positive
elements of $H(P)$. Then $j_1 = n_4 - n_3$. and it is enough to show that $n_3 = q + 2q_0$ ($\ast$).
(Observe that ($\ast$) already holds true for the point $P_0$ over $x = \infty$.) As a matter of fact,
property ($\ast$) was proved in [6, p. 43] and the proof of the theorem is complete. \hfill $\square$

In order to study the concrete realization of $S$ in $\mathbb{P}^4$ we use the $K$-rational morphism

$$\pi := (1 : x : y : z : w),$$
where \( x, y, z \) are as above and \( w \) is a \( K \)-rational function such that \( \text{div}_\infty(w) = (q + 2q_0 + 1)P_0 \). We may assume
\[
(3.7) \quad w := xy^{2q_0} + z^{2q_0}.
\]
In fact, Eqs. (3.2) and (3.5) imply the following relation among the functions \( x, y \) and \( w \):
\[
w^q + w = y^{2q_0}(x^q + x),
\]
whence \( \text{div}_\infty(w) = (q + 2q_0 + 1)P_0 \). Next we shall point out some relations describing \( y, w \) as functions depending on \( x \) and \( z \) only. By raising (3.4) to the power \( q_0 \) and using Eq. (3.2) we obtain:
\[
(3.8) \quad y = x^{q_0 + 1} + z^{q_0};
\]
from (3.7), (3.8) and Eq. (3.5):
\[
(3.9) \quad w = x^{2q_0 + 2} + xz + z^{2q_0}.
\]
Therefore \( S \) can be assumed to be the locus in \( \mathbb{P}^4 \) defined by the set of points
\[
(3.10) \quad P_{(a,c)} := (1 : a : b : c : d), \quad \text{and} \quad A_4 := \pi(P_0) = (0 : 0 : 0 : 0 : 1),
\]
with \( x = a \in \bar{K}, \ z = c \in \bar{K} \) satisfying Eq. (3.5), and \( y = b \) and \( w = d \) defined by (3.8) and (3.9) respectively. Now we show that the concrete realization of the Suzuki group \( Sz(q) \) established in Section 2 coincides with \( \text{Aut}(S) \).

**Theorem 3.2.** The isomorphic image of \( Sz(q) \) in \( \text{Aut}(\mathbb{P}^4) \) stated in Section 2 acts linearly on \( S \).

**Proof.** By (3.10) and the definition of \( \bar{T}, \bar{N} \) and \( W \) (cf. Section 2) it follows that each element of the isomorphic image of \( Sz(q) \) in \( \text{Aut}(\mathbb{P}^4) \) acts linearly on \( S \). \( \square \)

**Remark 3.3.** If in (3.10) we only consider the points corresponding to \( a, c \in K \) together with the point \( A_4 \), we obtain the so-called Suzuki-Tits ovoid (cf. [33]); this was already noticed by Cossidente [6, Appendix].

4. **Quotient curves arising from subgroups of a cyclic subgroup of \( \text{Aut}(S) \) of order \( q - 1 \)**

For a divisor \( r > 1 \) of \( q - 1 \), let \( U \) be a cyclic subgroup of \( \text{Aut}(S) \) of order \( r \). As mentioned in (2.1), \( U \) is unique up to conjugacy, and we may assume \( U = \{ N_d \in \bar{N} : d \in K, d^r = 1 \} \). Let \( \bar{S} = S/U \) denote the quotient curve of \( S \) by \( U \), and \( \bar{g} \) its genus. The objective of this section is to prove the following theorem. Let \( s \in \mathbb{N} \) such that \( q_0 = 2^s \), and set
\[
(4.1) \quad f(t) := 1 + \sum_{i=0}^{s-1} t^{2^i(q_0+1)-(q_0+1)}(1 + t)^{2^i}.
\]

**Theorem 4.1.** With the notation above,

1. \( \bar{g} = \frac{1}{2}q_0(q-1) \);
2. The following curve is a plane model over \( K \) of \( \bar{S} \):
\[
V^{\frac{1}{2}(q-1)} f(U) = (1 + U^{q_0})(U^{q-1} + V^{\frac{1}{2}(q-1)}).
\]
We need some preliminary results. Consider the morphism
\[ \phi := (x : y : z) : S \to C := \phi(S) \subseteq \mathbb{P}^2. \]

The results in Claims 4.2, 4.3, 4.4 and Lemma 4.5 below will show that \( C \) is a plane model over \( K \) of \( S \).

**Claim 4.2.**
1. The divisor defined by \( \phi \) is given by \( E = -A_0 + (q + 2q_0)A_4 \);
2. The morphism \( \phi \) is birational so that \( C \) is a curve of degree \( q + 2q_0 - 1 \).

**Proof.**
1. By Eqs. (3.2), (3.5) and the fact that \( x : S \to \mathbb{P}^1 \) is unramified but at \( \infty \), where it is totally ramified,
\[
\text{div}(x) = A_0 + D_1 - qA_4, \\
\text{div}(y) = (q_0 + 1)A_0 + D_2 - (q + q_0)A_4, \quad \text{and} \\
\text{div}(z) = (2q_0 + 1)A_0 + D_3 - (q + 2q_0)A_4.
\]
with \( D_1 = \sum P_{(0,y^{q_0})}, y^{q-1} = 1; D_2 = \sum P_{(x,x^{2q_0+1})}, x^{q-1} = 1 \) and \( D_3 = \sum P_{(x,0)}, x^{q-1} = 1. \)

We have then \( E = -A_0 + (q + 2q_0)A_4 \).

2. For a generic point \( P_{(a,c)} \in S \) we show \#\( \phi^{-1}(\phi(P_{(a,c)})) = 1 \). Let \( (x/y, z/y) = (a/b, c/b) \). By (3.8),
\[ a^{q_0+1}y^{q_0} + bc^{q_0}y^{q_0-1} + b^{q_0+1} = 0, \]
and after some computations one realizes that \( y = b \) is the only solution of this equation such that \( P_{(x,z)} \in S \). \( \square \)

Let \( (X : Y : Z) \) be projective coordinates for \( \mathbb{P}^2 \) and assume that \( Y = 0 \) is the line at infinity. We look for the equation \( f_1(X, Z) = 0 \) that defines the plane curve \( C \) above. The intersection divisor of \( Y \) and \( C \) is codified by the divisor \( \phi^*(Y) := \text{div}(y) + E = q_0A_0 + D_2 + q_0A_4 \); cf. Claim 4.2 and (4.2). This means that the line \( Y \) intersects \( C \) at \( q + 1 \) points, \( q_0 \) being the order of contact at both \( \phi(A_0) \) and \( \phi(A_4) \). Thus the term of degree \( q + 2q_0 - 1 \) of \( f_1(X, Z) \) can be assumed to be \( (XZ)^{q_0}(X^{q-1} + Z^{q-1}) \) and hence the defining equation of \( C \) will be of type
\[ f_1(X, Z) = f_2(X, Z) + (f_3(X, Z) + (XZ)^{q_0})(X^{q-1} + Z^{q-1}), \]
with \( \deg(f_2(X, Z)) < q + 2q_0 - 1 \), and \( \deg(f_3(X, Z)) < 2q_0 \). Now each \( N_d \in \hat{N} \) induces an automorphism on \( C \) by means of \( (X : Y : Z) \mapsto (dX : d^{q_0+1}Y : d^{2q_0+1}Z) \). Thus there exists \( e \in \hat{K}^* \) such that \( f_1(X, Z) = ef_1(d^{-q_0}X, d^{q_0}Z) \); we have then \( e = 1 \) by looking at the higher degree term of \( f_1(X, Z) \). Furthermore, \( f_2(X, Z) = \sum_{i,j} a_{i,j}X^iZ^j, a_{i,j} = a_{i,j}d^{j-i} \).
Suppose that \( a_{i,j} \neq 0 \), so that \( d^{j-i} = 1 \). Therefore \( (q - 1) \) divides \( (j - i) \) whenever \( d \) is a primitive element of \( K^* \); thus either \( j = i, j = i + q - 1 \), or \( i = j + q - 1 \). Write
\[
f_1(X, Z) = f_2(X, Z) + X^{q-1} \sum_{i,j; i \neq j} a_{i,j}X^jZ^j + Z^{q-1} \sum_{i,j; i \neq j} a_{i,j}XZ^i.
\]
On the other hand, the automorphism \( W \) of \( S \) (cf. Section 2) induces an automorphism on \( C \) via \( (X : Y : Z) \mapsto (Z : Y : X) \). Thus \( a_{i,j} = a_{j,i} \) and so
\[
f_1(X, Z) = \tilde{f}_2(XZ) + (\tilde{f}_3(XZ) + (XZ)^{q_0})(X^{q-1} + Z^{q-1}),
\]
where \( \tilde{f}_2(t) \) and \( \tilde{f}_3(t) \) are polynomials of degree at most \( q + q_0 - 1 \) and \( q_0 - 1 \) respectively.
Claim 4.3. $\deg(\tilde{f}_2(t)) = (q - 2)/2$.

Proof. For the line $L : X + Z = 0$, we compute $\phi^*(L)$ which is equal to $\text{div}_0(x + z) - A_0$ by Claim 4.2(1). Let $P := P_{a,a}$ be a zero of $x + z$ so that 

$$(x + z)^q + (x + z) = (x + a)^{q+2q_0} + (a^{2q_0} + 1)(x + a)^q + (x + a)^{2q_0 + 1} + (a^q + a)(x + a)^{2q_0} + (a^{2q_0} + 1)(x + a).$$

Since $x + a$ is a local parameter at $P$, the valuation of $x + z$ at $P$ is equal to either $2q_0 + 1$ or $1$ according to $a = 1$, or $a \in K \setminus \{1\}$ respectively. Thus 

$$\phi^*(L) = (2q_0 + 1)P_{(1,1)} + \sum_{x \not\in K \setminus \{0,1\}} P_{(x,x)}$$

and hence $\deg(\tilde{f}_2(t^2)) = q - 2$ as $\phi(P_{(1,1)})$ belongs to the line at infinity. \hfill \Box

Next we determine the explicit expression for $\tilde{f}_2(t)$ and $\tilde{f}_3(t)$, namely we show that $\tilde{f}_2(t) = f(t)$ and $\tilde{f}_3(t) = 1$.

Claim 4.4. (1) There exists $e \in K^*$ such that $ef(t) = \tilde{f}_2(t)$, where $f(t)$ is the polynomial defined in (4.1);

(2) $\tilde{f}_3(t) = 1$, and $e = 1$.

Proof. (1) We shall show that $f(t)$ and $\tilde{f}_2(t)$ have $(q - 2)/2$ common roots in $K$. Let $a \in K$; after some computations we have

$$(a^{2q_0 - 1})^{q_0} f(a^{2q_0 - 1}) = \text{Tr}_{K|\mathbb{F}_2}(a).$$

Since the map $a \mapsto a^{2q_0 - 1}$ is a bijection on $K$, the set of roots of $f(t)$ consists precisely of the $(q - 2)/2$ elements of the set

$$\{a^{2q_0 - 1} : \text{Tr}_{K|\mathbb{F}_2}(a) = 0, a \neq 0\}.$$ 

Now by (*) this set is invariant by the quadratic map $a \mapsto a^2$, and hence their elements are precisely the roots of $\tilde{f}_2(t)$.

(2) By (1), we have 

$$ef(\xi, \zeta) = (\tilde{f}_3(\xi, \zeta) + (\xi, \zeta)^{q_0})(\xi^{q_0} + \zeta^{q_0}),$$

where $\xi := x/y$ and $\zeta := z/y$. We use local power series computations at the point $A_0$, where $x$ is a local parameter; by dots we mean terms of higher degree. From Eqs. (3.2) and (3.5) $\xi = x^{-q_0} + x^{q-q_0+1} + \ldots$ and $\zeta = x^{q_0} + x^{q'} + \ldots$, where $q' > q + q_0 - 1$; thus $\xi \zeta = 1 + x^{q-1} + \ldots$. By the definition of $f(t)$, $f = 1 + x^{q-1} + \ldots$. Write $\tilde{f}_3(t) = a_0 + a_k x^m + a_{m+1} x^{m+1} + \ldots$, and suppose that $m = 2^nk \geq 1$ and $a_m \neq 0$. Then $\tilde{f}_3 = a_0 + a_m(1 + x^{q-1} + \ldots)^{2n} + \ldots$, and by comparing powers of $x$ (via (**)) we must have $(q - 1)2^n - q_0(q - 1) = 0$ which is a contradiction as $2^n < q_0$. Thus (**)) becomes

$$e(1 + x^{q-1} + \ldots) = ef(\xi, \zeta) = (a_0 + 1 + x^{(q-1)q_0} + \ldots)(x^{-(q-1)q_0} + \ldots)$$

and so $a_0 = 1$, and $e = 1$. \hfill \Box

We summarize the results above in the following.
Lemma 4.5. The Suzuki curve $S$ admits a plane model over $K$ defined by
$$f_1(X, Z) := f(XZ) + (1 + (XZ)^q)(X^{q-1} + Z^{q-1}),$$
where $f(t)$ is the polynomial given in (4.1).

Proof of Theorem 4.1. The genus $\tilde{g}$: It is straightforward to check that $U$ has exactly two fixed points on $S$, namely $A_0 := (1:0:0:0:0)$ and $A_4 = (0:0:0:0:1)$. Since $\tilde{S}$ is a tame quotient curve, the Riemann-Hurwitz genus formula gives $2q_0(q - 1) - 2 = r(2\tilde{g} - 2) + 2(r - 1)$, whence the result follows.

The plane equation: Let $\tilde{C}$ be the absolutely irreducible plane curve over $K$ whose function field is $K(XZ, Z^r)$. By the definition of $N_d$, $K(XZ, Z^r) \subseteq K(X, Z)^U$ ($\ast$). On the other hand, from the definition of $f_1(X, Z)$ in Lemma 4.5, $[K(X, Z) : K(XZ, Z^r)] = [K(XZ, Z) : K(XZ, Z^r)] = r$ and thus equality holds in ($\ast$). Taking $U := XZ$ and $V := Z^r$ we obtain the required equation for $\tilde{C}$, which is clearly a plane model of $\tilde{S}$. □

Remark 4.6. The geometric meaning of the proof of Lemma 4.5 emerges from the fact that the automorphisms $N_d$ and $W$ of $S$ preserve the line $L$ in $\mathbb{P}^4$ that joins the points $A_0$ and $A_4$. Indeed, the morphism $\phi$ above have been chosen to be the morphism associated to the 2-dimensional linear series cut out on $S$ by hyperplanes through $L$.

Remark 4.7. The curve $\tilde{S}$ in Theorem 4.1 is a covering of the hyperelliptic curve $vf(u) = (1 + u^{q_0})(u^{q-1} + v^2)$ of genus $\tilde{g}_0$; by replacing $v$ by $(1 + u^{q_0})v/\tilde{f}(u)$, such a hyperelliptic curve can be defined by
$$v^2 + v = \frac{(u + 1)^{q_0}u^{q/2}}{\tilde{f}(u)}.$$

5. Quotient curves arising from the subgroups of the Singer subgroups of $\text{Aut}(S)$

Let $S_1$ and $S_{-1}$ denote the Singer subgroups of $\text{Aut}(S)$ whose orders are $q + 2q_0 + 1$ and $q - 2q_0 + 1$ respectively; cf. (2.2). For a subgroup $\mathcal{U}$ of either $S_1$ or $S_{-1}$, denote by $\tilde{S} = S/\mathcal{U}$ the quotient curve of $S$ by $\mathcal{U}$, and $\tilde{g}$ its genus. The aim of this section is to prove the following theorem. Let $s \in \mathbb{N}$ such that $q_0 = 2^s$, and set

$$(5.1) \quad \tilde{f}(t) := 1 + \sum_{i=0}^{s-1} t^{2q_0}(1 + t)^{2i(q_0+1) - q_0} + t^{q/2}.$$

Theorem 5.1. With the notation above,

1. If $\mathcal{U}$ is a subgroup of $S_1$ of order $r > 1$, then $\tilde{g} = \frac{1}{r}(q + 2q_0 + 1)(q_0 - 1) + 1$ and a plane model over $\mathbb{F}_{q^4}$ of $\tilde{S}$ is given by
$$V^\frac{1}{r}(q + 2q_0 + 1) \tilde{f}(U) = U^{q + 2q_0 + 1} + V^\frac{1}{r}(q + 2q_0 + 1);$$

2. If $\mathcal{U}$ is a subgroup of $S_{-1}$ of order $r > 1$, then $\tilde{g} = \frac{1}{r}(q - 2q_0 + 1)(q_0 + 1) - 1$ and a plane model over $\mathbb{F}_{q^4}$ of $\tilde{S}$ is given by
$$bV^\frac{1}{r}(q - 2q_0 + 1) \tilde{f}(U) = (U^{q_0 - 1} + U^{2q_0 - 1})(U^{q - 2q_0 + 1} + V^\frac{1}{r}(q - 2q_0 + 1)),$$

where $\tilde{f}(t), f(t)$ are the polynomials defined in (5.1) and (4.1) respectively, and $b := \lambda^{q_0} + \lambda^{q_0 - 1} + \lambda^{-q_0} + \lambda^{-(q_0 - 1)}$ with $\lambda \in \mathbb{F}_{q^4}$ of order $q - 2q_0 + 1$. 


To work out a plane model for $\mathcal{S}$, we use the same approach as in Section 4. In particular, we write out appropriate plane models of $\mathcal{S}$; see Lemmas 5.5 and 5.7 below. We obtain these results through Claims 5.2, 5.3, 5.4 and Claim 5.6 respectively.

To begin with we look for a suitable birational morphism

$$\phi = (h_0 : h_1 : h_2) : \mathcal{S} \to \mathcal{C} := \phi(\mathcal{S}) \subseteq \mathbb{P}^2$$

of degree $q+2q_0+1$, or $q+2q_0-1$ with $h_0, h_1, h_2 \in \mathcal{L}((q+2q_0+1)P_0) = \langle 1, x, y, z, w \rangle$, where $x, y, z$ and $w$ are the rational functions on $\mathcal{S}$ defined in (3.2), (3.4) and (3.7) respectively. Let $\lambda \in \mathbb{F}_{q^4}$ be an element of order $q \pm 2q_0 + 1$ and set

$$b := \begin{cases} 
\lambda^{q_0} + \lambda^{q_0+1} + \lambda^{-q_0} + \lambda^{-(q_0+1)} & \text{if } \lambda \text{ has order } q + 2q_0 + 1; \\
\lambda^{q_0} + \lambda^{q_0-1} + \lambda^{-q_0} + \lambda^{-(q_0-1)} & \text{if } \lambda \text{ has order } q - 2q_0 + 1.
\end{cases}$$

Notice that $b^q - 1 = 1$. Let

$$\mu := \frac{\lambda + \lambda^{-1}}{b},$$

so that $\mu^{q^2-1} = 1$. Choose $h_1$ and $h_2$ with the following properties:

- $v_{A_4}(h_1) = v_{A_4}(h_2) = -(q + 2q_0 + 1)$;
- Let $P = P_{(a,c)} \in \mathcal{S}$. We have $a = \mu$ whenever $h_1(P) = h_2(P) = 0$.

Set

$$h_0 := b^{q_0-1}x + y + b^{q_0-1}$$

in such a way that $\phi$ is birational, cf. (5.5) below. Let $E$ be the divisor defined by $\phi$. Then $v_{A_4}(E) = q + 2q_0 + 1$, and the base points of the linear series associated to $\phi$ are the common zeroes of $h_0$, $h_1$ and $h_2$.

Claim 5.2. We have

$$E = \begin{cases} 
(q + 2q_0 + 1)A_4 & \text{if } \lambda^{q+2q_0+1} = 1, \\
-P_{(\mu,\mu^{q}c)} - P_{(\mu,\mu^{q}+b)} + (q + 2q_0 + 1)A_4 & \text{if } \lambda^{q-2q_0+1} = 1.
\end{cases}$$

In particular, the plane curve $\mathcal{C}$ above has degree $q + 2q_0 + 1$, or $q + 2q_0 - 1$.

Proof. Let $P_{(a,c)} \in \mathcal{S}$ be a common zero of $h_0$, $h_1$ and $h_2$ with $a = \mu$ and $c \in \bar{K}$ defined via Eq. (3.5). If $\bar{c} := c/b$, then $b(\bar{c}^q + \bar{c}) = \mu^{2q}(\mu^q + \mu)$; now taking into consideration (3.8) and the definition of $h_0$, we conclude that $\bar{c}$ is a solution of the system

$$(5.2) \quad b^{q_0}T^{q_0} + b^{q_0-1}T = b^{q_0-1}\mu + \mu^{q_0+1}, \quad b(T^q + T) = \mu^{2q}(\mu^q + \mu).$$

From the definition of $b$ it follows that $\bar{c}$ must be a root of the quadratic equation

$$T^2 + T = (\mu/b)^2.$$ 

It turns out that the solutions of this equation are $t := \mu\lambda^q/b$, and $t + 1$ since

$$\lambda^{2q} + b^2 \frac{\lambda^q}{\lambda + \lambda^{-1}} + 1 = 0.$$ 

It is straightforward to check that $t$ and $t + 1$ satisfy (5.2) if and only if $\lambda^{q-2q_0+1} = 1$, and the proof is complete. \qed
Assume that \( \lambda \) has order \( q + 2q_0 + 1 \). Let \((X : Y : Z)\) be projective coordinates of \( \mathbb{P}^2 \) and assume that \( X = 0 \) is the line at infinity. We look for an equation \( f_1(Y, Z) = 0 \) for the plane curve \( C \). The intersection divisor of \( X \) and \( C \) is codified by \( \phi^*(X) = \text{div}(h_0) + E = \text{div}_0(h_0) + A_4 \) by the previous claim. Let \( \mathbf{B} := \mathbf{T}_{0, b} \circ \mathbf{W} \in \text{Aut}(\mathcal{S}) \). Thus \( \mathbf{B} \) is defined by the matrix (cf. Section 2)

\[
\begin{pmatrix}
0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & b^{q_0} \\
0 & 1 & 0 & 0 & b \\
1 & 0 & 0 & b & b^{2q_0}
\end{pmatrix}
\]

We shall prove that the points \( \mathbf{B}^i(A_0) (i = 2, \ldots, q + 2q_0 + 1) \) are zeroes of \( h_0 \). To see this, we apply induction on \( i \); indeed, it is enough to show that \( h_0(\mathbf{B}^2(A_0)) = 0 \), which is a straightforward computation. On the other hand, \( \mathbf{B}(A_0) = A_4 \) and so the aforementioned points are precisely the zeroes of \( h_0 \) (recall that \( \deg(h_0) = q + 2q_0 + 1 \)); thus

\[
\phi^*(X) = \sum_{i=1}^{q+2q_0+1} \mathbf{B}^i(A_0).
\]

To see the significance of this computations on \( \mathcal{C} \) we have to compute \( \phi(\mathbf{B}^i(A_0)) \), \( i = 1, \ldots, q + 2q_0 + 1 \). At this point we choose concrete rational functions \( h_1 \) and \( h_2 \) on \( \mathcal{S} \). Let \( \lambda \in \mathbb{F}_{q^4} \) be of order \( q + 2q_0 + 1 \) and \( \mathbf{M} \) the automorphism of \( \mathbb{P}^4 \) defined by the matrix:

\[
\mathbf{M} := \begin{pmatrix}
0 & b^{q_0-1} & 1 & b^{q_0-1} & 0 \\
\mu & 1 & 0 & \lambda & \lambda \mu \\
\mu^q & 1 & 0 & \lambda^q & \lambda^q \mu^q \\
\mu & 1 & 0 & \lambda^{-1} & \lambda^{-1} \mu \\
\mu^q & 1 & 0 & \lambda^{-q} & \lambda^{-q} \mu^q
\end{pmatrix}.
\]

A straightforward computation shows that

\[
\mathbf{M} \mathbf{B} \mathbf{M}^{-1} = \Lambda,
\]

where

\[
\Lambda := \begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & \lambda & 0 & 0 & 0 \\
0 & 0 & \lambda^q & 0 & 0 \\
0 & 0 & 0 & \lambda^{-1} & 0 \\
0 & 0 & 0 & 0 & \lambda^{-q}
\end{pmatrix}.
\]

We observe that the first row of \( \mathbf{M} \) defines \( h_0 \), and we define now \( h_1 \) and \( h_2 \) by using the second and fourth row respectively; that is to say,

\[
h_1 := \mu + x + \lambda z + \lambda \mu w, \quad \text{and} \quad h_2 := \mu + x + \lambda^{-1} z + \lambda^{-1} \mu w.
\]

In particular, the Suzuki curve is birationality equivalent over \( \mathbb{F}_{q^4} \) to \( \mathcal{C} = \phi(\mathcal{S}) \) since \( \mathbf{M} \in \text{Aut}(\mathbb{P}^4) \) is defined over \( \mathbb{F}_{q^4} \). From (5.4),

\[
\mathbf{B}^i(A_0) = \mathbf{M}^{-1}(0 : \lambda^i \mu : \lambda^q \mu^q : \lambda^{-i} \mu : \lambda^{-iq} \mu^q)
\]
and hence $\phi(B^i(A_0)) = (0 : \lambda^i : \lambda^{-i})$, $i = 1, \ldots, q + 2q_0 + 1$. Thus we may assume that $C$ is defined by

$$f_1(Y, Z) = f_2(Y, Z) + (Y^{q+2q_0+1} + Z^{q+2q_0+1}),$$

being $f_2(Y, Z)$ a polynomial of degree at most $q + 2q_0$. To normalize $f_2(Y, Z)$ we use the fact that the automorphism $B$ above induces an automorphism on $C$ via $(X : Y : Z) \mapsto (X : \lambda^{-1}Y : \lambda Z)$; then we proceed as in the proof of Lemma 4.5 to conclude that

$$f_2(Y, Z) = \tilde{f}_2(Y Z),$$

where $\tilde{f}_2(t)$ is a polynomial of degree less than $(q + 2q_0 + 1)/2$.

Claim 5.3. $\deg(\tilde{f}_2(t)) = q/2$.

Proof. Consider the line $L : Y + \lambda^2 Z = 0$; since $\lambda^2 h_2 + h_1 = (\lambda^2 + 1)(x + \mu)$, $\phi^*(L) = \text{div}(x + \mu) + E = \text{div}_0(x + \mu) + (2q_0 + 1)A_4$ (cf. (4.2) and Claim 5.2). Thus $\deg(\tilde{f}_2(t^2)) = q$ as $\phi(A_4) \in X$.

Claim 5.4. The polynomial $\tilde{f}(t)$ in (5.1) coincides with $\tilde{f}_2(t)$.

Proof. We show that both polynomials $\tilde{f}(t)$ and $\tilde{f}_2(t)$ have $q/2$ different common roots. After some computations, for $a \in K$

$$(1 + a^{2q_0-1})^{q_0}\tilde{f}(a^{2q_0-1}) = 1 + \text{Tr}_{K/F_2}(a);$$

thus the set of roots of $\tilde{f}(t)$ is given by

$$\{a^{2q_0-1} : a \in K, \; \text{Tr}_{K/F_2}(a) = 1\}.$$

Now we compute the roots of $\tilde{f}_2(t)$. By the proof of Claim 5.3, such roots arise from the points $(1 : Y : Z) \in C$ with $Y = \lambda^2 Z$. We have

$$(1 : Y : Z) = (1 : \lambda B(z)^{2q_0-1} : \lambda^{-1}B(z)^{2q_0-1}),$$

where

$$B(z) := z^{q_0} + z + \frac{\mu}{b} + \frac{\mu^{2q_0+1}}{b^{q_0}}$$

with $z$ such that $b(z^q + z) = \mu^{2q_0}(\mu^q + \mu)$. Therefore $a \in K$ is a root of $\tilde{f}_2(t)$ if and only if $a = B(z)^{2q_0-2}$, $z$ being as in (*). Now $B(z) \in K$, and by using the fact that the map $a \mapsto a^{2q_0-1}$ is a bijection on $K$, and that the set of roots of $\tilde{f}(t)$ is invariant under the map $b \mapsto b^2$, we conclude that there exists $e \in \tilde{K}$ such that $\tilde{f}(t) = e\tilde{f}_2(t)$. Now $\phi(P_{(\mu-1,\lambda^{-1})}) = (1 : 0 : \lambda^{-1})$ and we have $e = 1$.

We have then proved the following lemma.

Lemma 5.5. The Suzuki curve $S$ admits a plane model over $F_{q^4}$ defined by

$$f_1(Y, Z) = \tilde{f}(Y Z) + (Y^{q+2q_0+1} + Z^{q+2q_0+1}),$$

where $\tilde{f}(t)$ is as in (5.1).
Now let $\lambda \in \mathbb{F}_{q^4}$ be of order $q-2q_0+1$. We compute the intersection divisor of $X$ and $C$. By (4.2) and Claim 5.2

$$\phi^*(X) = \text{div}(h_0) + E = \text{div}_0(h_0) - P_1 - P_2 + A_4,$$

where $P_1 := P_{(\mu, \lambda^q \mu)}$ and $P_2 := P_{(\mu, \lambda^q \mu + b)}$; by arguing as in the proof of the previous lemma, we check that the points $B^i(A_0)$ ($i = 2, \ldots, q - 2q_0 + 1$) are zeroes of $h_0$; thus, up to multiplicity, there are $4q_0$ zeroes of $h_0$ missing. By the definition of $h_0$, Eqs. (3.2) and (3.5) we have

$$h_0^3 + h_0 = (x^q + x)(b^{q_0-1} + x^{q_0} + b^{q_0-1}x^{2q_0})$$

$$= [(x + a)^q + (x + a) + a^q + a][(x - a)^{q_0} + b^{q_0-1}(x + a)^{2q_0} + b^{q_0} + a^{q_0} + b^{q_0-1}a^{2q_0}],$$

$P_{(a,c)}$ being a zero of $h_0$. Since $\mu \not\in K$, it follows that $v_{P_1}(h_0) = v_{P_2}(h_0) = q_0$. Now by using the system (5.2) with $\mu^{-1}$ instead of $\mu$ we find the remaining two zeros of $h_0$, namely $P_3 := P_{(\mu^{-1}, \lambda^q \mu^{-1})}$, and $P_4 := (\mu^{-1}, \lambda^q \mu^{-1} + b)$; moreover, $v_{P_3}(h_0) = v_{P_4}(h_0) = q_0$ and hence

$$\phi^*(X) = (q_0 - 1)P_1 + (q_0 - 1)P_2 + q_0P_3 + q_0P_4 + \sum_{i=1}^{q-2q_0+1} B^i(A_0).$$

Next we compute the intersection divisor of $X$ and $C$: we have

$$X \cdot C = \sum_{i=1}^{q-2q_0+1} (0 : \lambda^i : \lambda^{-i}) + (2q_0 - 1)Q_1 + (2q_0 - 1)Q_2,$$

where $Q_1 := \phi(P_1) = \phi(P_4) = (0 : 1 : 0)$ and $Q_2 := \phi(P_2) = \phi(P_3) = (0 : 0 : 1)$ (the last two computations follow from (4.2) and the fact that $h_1 = \lambda^2h_2 + (\lambda^2 + 1)(x + \mu)$). Then we may assume

$$f_1(Y, Z) = f_2(Y, Z) + (f_3(Y, Z) + (YZ)^{2q_0-1})(Y^{q-2q_0+1} + Z^{q-2q_0+1}),$$

where $\deg(f_2(Y, Z)) < q + 2q_0 - 1$ and $\deg(f_3(Y, Z)) < 4q_0 - 2$. Now by using the action of the automorphisms on $C$ induced by $B$ and $W \circ B \in \text{Aut}(S)$ via $(X : Y : Z) \mapsto (X : \lambda Y : \lambda^{-1}Z)$ and $(X : Y : Z) \mapsto (X : Z : Y)$ respectively, we can further assume that $f_2(Y, Z) = \tilde{f}_2(YZ)$ and $f_3(Y, Z) = \tilde{f}_3(YZ)$ with $\tilde{f}_2(t), \tilde{f}_3(t) \in \mathbb{F}_{q^4}[t]$.

**Claim 5.6.**

1. With $f(t)$ defined in (4.1), there exists $e \in \mathbb{F}_{q^4}$ such that $ef(t) = \tilde{f}_2(t)$;
2. There exists $e' \in \mathbb{F}_{q^4}$ such that $\tilde{f}_3(t) + t^{2q_0-1} = e'(t^{q_0} + t^{2q_0-1})$.

**Proof.**

1. The proof is similar to that of Claims 4.4 and 5.4.
2. Let $\xi := h_1/h_0$ and $\zeta := h_2/h_0$ be the rational functions on $S$ defining the function field of $S$. Thus

$$ef(\xi\zeta) = (\tilde{f}_3(\xi\zeta) + (\xi\zeta)^{2q_0-1})(\xi^{q-2q_0+1} + \zeta^{q-2q_0+1}).$$
Let $P_1, P_2, P_3$ and $P_4$ be the points in the support of $\phi^*(X)$ (see 5.6). Next we use computations by using the valuation at $P_1$ to show first that the order of $\tilde{f}_3(t)$ is $q_0 - 1$. By (4.2) we have

$$v_{P_1}(f_3(\xi \zeta) + (\xi \zeta)^{2q_0 - 1}) = (q_0 - 1)(q - 2q_0 + 1),$$

and $v_{P_1}(\xi \zeta) = q - 2q_0 + 1$; thus the assertion on the order of $\tilde{f}_3(t)$ follows. Now for $a \in \bar{K}$ a root of $f_3(t) + t^{2q_0 - 1}$, let $\mathcal{C}_a$ be the conic defined by the equation $YZ = a$. We have $\mathcal{C}_a \cap \mathcal{C} \subseteq X$; otherwise, $f(a) = 0$ by (1), so that $\mathcal{C}_a$ would be a component of $\mathcal{C}$, which is a contradiction. Let $\ell$ be a local parameter at $P = P_{(a, b_0)}$; then

$$h_0 = (b^{q_0 - 1}(1 + a^{2q_0}) + a^{q_0})\ell + \ldots$$

$$h_1 = h_1(P_t) + (1 + \lambda(a^{2q_0} + \mu a^{2q_0 + 1} + \mu bc))\ell + \ldots$$

$$h_2 = h_2(P_t) + (1 + \lambda^{-1}(a^{2q_0} + \mu a^{2q_0 + 1} + \mu bc))\ell + \ldots,$$

and it follows that $v_P(\xi \zeta - P) > 0$ for some $i$ and also that $a = 0$ or 1. Then the proof of Claim 5.6 is complete.

We have shown so far that $\mathcal{C}$ can be defined over $\mathbb{F}_{q^4}$ by a polynomial of type

$$(5.7) \quad f_1(Y, Z) = cf(YZ) + ((YZ)^{q_0 - 1} + (YZ)^{2q_0 - 1})(Y^{q_0 - 2q_0 + 1} + Z^{q - 2q_0 + 1}).$$

Finally, we prove that $c = b$; we use local computations at $P_{(0, 0)} \in \mathcal{S}$ via the rational functions $\xi = h_1/h_0$ and $\zeta = h_2/h_0$ (recall that $x$ is a local parameter at that point). By the definition of $h_0, h_1$ and $h_2$,

$$(5.8) \quad h_0 = b^{q_0 - 1}x + x^{2q_0 + 1} + \ldots, \quad h_1 = \mu + x + \lambda x^{2q_0 + 1} + \ldots, \quad h_2 = \mu + x + \lambda^{-1}x^{2q_0 + 1} + \ldots,$$

whence

$$\xi = (\mu/b^{q_0 - 1})x^{-1}(1 + \ldots), \quad \zeta = (\mu/b^{q_0 - 1})x^{-1}(1 + \ldots).$$

Now by means of Eq. (5.7) we compare the order at 0 of the local power series

$$c\rho^2\xi\zeta f(\rho^2\xi \zeta), \quad and \quad ((\rho^2\xi \zeta)^{q_0} + (\rho^2\xi \zeta)^{2q_0})(\xi^{q_0 - 2q_0 + 1} + \zeta^{q - 2q_0 + 1})\rho^{q_0 - 2q_0 + 1},$$

where $\rho := b^{-q_0}x^{-1}$. The order at 0 of the former series is $c/b^{2q_0 - 1}$; as far as the last series concerns, it is enough to compute the order at 0 of

$$(\rho^2\xi \zeta)^{q_0}(\xi^{q_0 - 2q_0 + 1} + \zeta^{q - 2q_0 + 1})\rho^{q_0 - 2q_0 + 1}.$$

By (5.8) and some computations

$$\frac{h_1^{q_0 - 2q_0 + 1} + h_2^{q_0 - 2q_0 + 1}}{h_0^{q_0 - 2q_0 + 1}} = \frac{1}{b^{6(q_0 - 1)}}x^{-q_0 + 4q_0 + \ldots};$$

thus we obtain

$$\frac{c}{b^{2q_0 - 1}} = \frac{1}{b^{4q_0 - 2}}b^{6(q_0 - 1)}$$

so that $c = b$. Thus the following holds.

**Lemma 5.7.** The Suzuki curve $\mathcal{S}$ admits a plane model over $\mathbb{F}_{q^4}$ defined by

$$f_1(Y, Z) = bf(YZ) + ((YZ)^{q_0 - 1} + (YZ)^{2q_0 - 1})(Y^{q_0 - 2q_0 + 1} + Z^{q - 2q_0 + 1}),$$

where $f(t)$, is as in (4.1), and $b = \lambda^{q_0} + \lambda^{q_0 - 1} + \lambda^{-q_0} + \lambda^{-(q_0 - 1)}$ with $\lambda \in \mathbb{F}_{q^4}$ of order $q - 2q_0 + 1$. 


Proof of Theorem 5.1. The genus $\tilde{g}$: By the proof of Claim 5.2, see (5.3) and (5.6) above, we have that the natural morphism $S \rightarrow \tilde{S}$ is either unramified, or totally ramified precisely at four points according as $U \subseteq S_1$, or $U \subseteq S_{-1}$. Then the formula for $\tilde{g}$ is computed by the Riemann-Hurwitz genus formula.

The plane equation: Let $\tilde{C}$ be the absolutely irreducible plane curve over $K$ whose function field is $K(YZ, Z^r)$. By the definition of $S_1$, $K(YZ, Z^r) \subseteq K(YZ)_{1}$ and thus equality holds in (5). Taking $U := YZ$ and $V := Z^r$ we obtain the required equation for $\tilde{C}$, which is clearly a plane model of $\tilde{S}$.

Remark 5.8. Let $P_1, P_2, P_3$ and $P_4$ be the points defined in (5.6), and $L$ the line through the points $P_1$ and $P_2$. This line is fixed by the automorphism $B$ defined above, and $\phi$ is the morphism defined by the linear series cut out on $S$ by hyperplanes through $L$. By the proof of Claim 5.2, (5.3) and (5.6), the natural morphism $S \rightarrow \tilde{S}$ is unramified, or totally ramified at the aforementioned points whenever $U \subseteq S_1$, or $U \subseteq S_{-1}$.

Remark 5.9. The curves in Theorem 5.1 covers a hyperelliptic curve of genus $q_0$ defined by $v^2 + v = u^{(q+2q_0+1)/2}/f(u)$ in Case (1) and by $v^2 + bv = (1 + u)^{q_0} u^{q/2}/f(u)$ in Case (2).

6. Non-tame quotient curves of the Suzuki curve

In this section we investigate quotient curves of the Suzuki curve $S$ arising from the non-tame subgroups of $\text{Aut}(S)$. Non-tame ramifications together with a huge number of pairwise non-conjugate subgroups of even order (especially 2-subgroups) do not allow us to obtain results as complete as those achieved in Sections 4 and 5. Nevertheless, we manage to compute the degree of the ramification divisor of the respective natural morphism and thus the genus of such curves; in several cases we also provide plane models.

From Section 2, the subgroups of $S_z(q)$ of even order are of the following types, up to conjugacy in $S_z(q)$:

I. Subgroups of $\widetilde{T}$;
II. Subgroups of order $2^r r > 1$, $r > 1$ with $r$ a divisor of $q - 1$;
III. Dihedral subgroups of order $2r$ with $r > 1$ a divisor of $q - 1$;
IV. Subgroups of order $2r$ with $r > 1$ a divisor of $q \pm 2q_0 + 1$;
V. Subgroups of order $4r$ with $r > 1$ a divisors of $q \pm 2q_0 + 1$;
VI. Subgroups isomorphic to $S_z(q)$.

Type I. Let $U$ be a subgroup of $\widetilde{T}$. We shall compute the genus $\tilde{g}$ of the quotient curve $\tilde{S} = S/U$, by considering the subgroup $U_2$ of $U$ consisting of the elements of even order together with the identity (a similar problem on the Hermitian curve was considered in [7]). Let $u$ and $v$ be the integers such that $2^u := \#U_2$ and $2^v := \#U$. Recall that $q = 2q_0^2$ and $q_0 = 2^s$, $s \in \mathbb{N}$.

Theorem 6.1. With the notation above,

$$\tilde{g} = \frac{q_0}{2^{v-u}} \left( \frac{q}{2^u} - 1 \right);$$

in particular, $u \leq 2s + 1$ and $v - u \leq s$. 
Proof. The Riemann-Hurwitz formula asserts that

$$2q_0(q - 1) - 2 = 2^v(2\bar{g} - 2) + \deg(R),$$

where $R$ is the associated ramification divisor of the natural morphism $\mathcal{S} \to \mathcal{S}$. Let $\ell$ be a local parameter at $P \in \mathcal{S}$; we have $v_P(R) = \sum_T i_{T,P}$, where the summation is extended over all $T \in U$ such that $T(P) = P$, and where $i_{T,P} = v_P(T^*(\ell) - \ell)$ (see e.g. [31, III.8.8]). By the definition of $T = T_{a,c}$ (cf. Section 2), $v_P(R) = 0$ for $P \neq A_4$. On the other hand, at the point $A_4$ the rational function $z/w$ is a local parameter by (4.2); therefore

$$i_{T,A_4} = \begin{cases} 2q_0 + 2, & \text{for } a = 0, \\ 2, & \text{for } a \neq 0. \end{cases}$$

We have that $T \neq 1$ is an element of order 2 for $a = 0$, otherwise its order is 4. Thus the Riemann-Hurwitz above becomes

$$2q_0(q - 1) - 2 = 2^v(2\bar{g} - 2) + (2q_0 + 2)(2^u - 1) + 2(2^u - 2^u),$$

and we obtain the formula for $\bar{g}$. The numerical conditions follow from the fact that $\bar{g}$ must be a non-negative integer.

In Corollary 6.5 we are going to point out sufficient conditions for the existence of non-tame quotient curves of $\mathcal{S}$ whose genus can be computed via Theorem 6.1. For some cases regarding $v = u$ and $(v, u) = (2, 1)$, we can exhibit a plane model; see Theorem 6.6.

Theorem 6.1 raises the problem of classifying the subgroups of $\tilde{T}$ in terms of their elements of order $2$. Such a general problem is computationally beyond our possibility, because $\tilde{T}$ contains a huge number of pairwise non-conjugate subgroups. The following lemma states some (necessary) numerical conditions on $u$ and $v$.

**Lemma 6.2.** Let $U$ be a subgroup of $\tilde{T}$ and $U_2$ the subgroup of its elements of even order. Let $2^v$ and $2^u$ be the orders of $U$ and $U_2$ respectively. Then the following statements hold true:

1. $v \leq 2u$;
2. For every integer $u'$ with $u \leq u' \leq v$ there is a subgroup of $U$ of order $2^{u'}$ containing $U_2$. In particular, for each integer $u'$ with $2s + 1 \leq u' \leq 4s + 2$, there is a subgroup of $\tilde{T}$ of order $2^{u'}$ containing all elements of $\tilde{T}$ of order $2$.

**Proof.** (1) We consider the homomorphism of groups

$$\Phi = \Phi_U : U \to K, \quad T_{a,c} \mapsto a,$$

where $K$ is equipped with its additive structure. We have $\ker(\Phi) = U_2$ and thus $U/U_2$ is isomorphic to $\Phi(U)$. As the map $K \to K : a \mapsto a^{2^{q_0+1}}$ is injective, and as $T_{a,c}^2 = T_{0,a2^{q_0+1}}$, we have that $\# \Phi(U) \leq \#U_2$ and hence the assertion.

(2) Since the quotient group $U/U_2$ is an elementary abelian group, the converse of the Lagrange theorem holds and the first statement follows; for the second statement take $U = \tilde{T}$; cf. (2.3).

Sufficient conditions for the existence of a subgroup $U$ of $\tilde{T}$ with a given subgroup $U_2$ is ensured by the following lemma. Let $\Phi_U$ be the map defined in the proof of Lemma 6.2.
Lemma 6.3. Let \( \mathcal{V} \) be an elementary abelian group of \( \tilde{T} \) of order \( 2^u \). Then there exists a subgroup \( \mathcal{U} \) of \( \tilde{T} \) of order \( 2^{u+1} \) such that \( \mathcal{U}_2 \) coincides \( \mathcal{V} \);

(2) Let \( v \geq u \geq 0 \) be integers, and \( B \) an additive subgroup of \( K \) of order \( 2^u \). If there exists an additive subgroup \( A \) of \( K \) of order \( 2^{v-u} \) such that \( A^{2q_0+1} \subseteq B \), then there exists a subgroup \( \mathcal{U} \) of \( \tilde{T} \) of order \( 2^v \) such that \( \Phi_{\mathcal{U}}(\mathcal{U}) = A \) and \( \ker(\Phi_{\mathcal{U}}) = \{ T_{0,c} : c \in B \} \) (in particular, \( \ord(\mathcal{U}_2) = 2^v \)).

Proof. (1) Since the normaliser in \( \text{Aut}(S) \) of \( \tilde{T} \) acts transitively on the set of elements of order 2 of \( \tilde{T} \), cf. (2.3), we may assume \( T_{0,1} \not\in \mathcal{V} \). Then the group \( \mathcal{U} \) generated by \( \mathcal{V} \) and \( T_{0,1} \) fulfills the required conditions.

(2) The proof of this assertion is by induction on \( v \geq u \). If \( v = u \), then \( A = \{ 0 \} \) and \( \mathcal{U} := \{ T_{0,c} : c \in B \} \) have the required properties. Suppose now that \( v > u \). As \( A \) is an elementary abelian group, it contains a subgroup \( A_0 \) of index 2, that is of order \( 2^{(v-1)-u} \). Since \( A_0^{2q_0+1} \subseteq A^{2q_0+1} \), there is by induction a subgroup \( \mathcal{U}_0 \) in \( \tilde{T} \) of order \( 2^{v-1} \) with \( \Phi_{\mathcal{U}_0}(\mathcal{U}_0) = A_0 \) and \( \ker(\Phi_{\mathcal{U}_0}) = \{ T_{0,c} : c \in B \} \). Fix \( T := T_{a,c} \in \tilde{T} \) with \( a \in A \setminus A_0 \) which does not belong to \( \mathcal{U}_0 \) by (*). Let \( \mathcal{U} \) be the subgroup of \( \tilde{T} \) generated by \( \mathcal{U}_0 \) together with \( T \).

To prove that the order of \( \mathcal{U} \) is \( 2^v \) we show that \( \mathcal{T}\mathcal{U}_0 = \mathcal{U}_0 \mathcal{T} \). Let \( \mathcal{T} := T_{a_0,c_0} \) be any element of \( \mathcal{U}_0 \). Note that \((\mathcal{T} \circ \mathcal{T}_0)^2 = T_{0,(a+a_0)^2q_0+1} \in \mathcal{U}_0 \). In fact, \((a+a_0)^2q_0+1 \in B \) since \( a+a_0 \in A \), and the claim follows by (**). Now, as \( \tilde{T} \) has exponent 4 and as every element of order two in \( \tilde{T} \) is in the center \( Z(\tilde{T}) \), cf. (2.3), we have

\[
\mathcal{T} \circ \mathcal{T}_0 = \mathcal{T} \circ \mathcal{T}_0(\mathcal{T} \circ \mathcal{T}_0^4 \circ \mathcal{T}^3) = (\mathcal{T} \circ \mathcal{T}_0)^2 \mathcal{T}_0^3 \circ \mathcal{T}^3 = (\mathcal{T} \circ \mathcal{T}_0)^4 \circ \mathcal{T}_0 \circ \mathcal{T} \in \mathcal{U}_0 \mathcal{T}.
\]

Finally, \( \Phi_{\mathcal{U}}(\mathcal{T} \circ \mathcal{T}_0) = \Phi_{\mathcal{U}}(\mathcal{T}) + \Phi_{\mathcal{U}}(\mathcal{T}_0) = a + a_0 \) implies \( \Phi_{\mathcal{U}}(\mathcal{U}) = A \) and \( \ker(\Phi_{\mathcal{U}}) \subseteq \ker(\Phi_{\mathcal{U}_0}) \), and the result follows.

Remark 6.4. Lemma 6.3(1) does not hold true for subgroups \( \mathcal{U} \) of order \( 2^{u+\ell} \) with \( \ell > 1 \), as the following example shows. Fix an element \( e \in K \setminus \mathbb{F}_2 \). The set \( \mathcal{V} = \{ T_{0,0}, T_{0,1}, T_{0,e}, T_{0,e+1} \} \) is an elementary abelian subgroup of \( \tilde{T} \) of order \( 2^u \) with \( v = 2 \). Assume that there is a subgroup \( \mathcal{U} \) of \( \tilde{T} \) of order \( 2^d \) such that \( \mathcal{U}_2 = \mathcal{V} \). Then there are three pairwise distinct non-zero elements \( a_1, a_2, a_3 \in K \) and three elements \( c_1, c_2, c_3 \in K \) such that \( T_{a_i,c_i} (i = 1, 2, 3) \) together with \( T_{0,0} \) form a complete set of representatives of the cosets of \( \mathcal{U}/\mathcal{V} \). Furthermore, \( \Phi_{\mathcal{U}}(\mathcal{U}) = \{ 0, a_1, a_2, a_3 \} \) and \( a_3 = a_1 + a_2 \). On the other hand, we can assume \( a_1 = 1, a_2^{2q_0+1} = e, a_3^{2q_0+1} = e + 1 \) since \( T_{a_i,c_i}^2 = T_{0,a_i^{2q_0+1}} \). Then (*) implies \( a_3^{2q_0} + a_3 = 0 \), a contradiction.

Corollary 6.5. Let \( v \geq u \geq 0 \) integers such that \( v - u \leq s, u \leq 2s + 1 \) and \( v \leq 2u \). Then there exists a non-tame quotient curve of \( S \) whose genus is given by Theorem 6.1 provided that

\[
(6.1) \quad v - u \leq \log_2 (u + 1), \quad \text{or} \quad (v - u)(2s + 1).
\]

Proof. Suppose at first that both \( v - u \leq 2s + 1 \) and \( v - u \leq \log_2 (u + 1) \) hold. For any additive subgroup \( A \) of \( K \) of order \( 2^{v-u} \), the additive subgroup \( B' \) of \( K \) generated by all elements in \( A^{2q_0+1} \) has order at most \( 2^{2v-u} - 1 \). In fact, \( K \) can be viewed as a vector space over its subfield \( \mathbb{F}_2 \), and the subspace generated by \( A^{2q_0+1} \) has dimension at most \( 2^{v-u} - 1 \).
Then there exists an additive subgroup $\mathcal{B}$ of $K$ of order $2^n$ containing $\mathcal{B}'$, and the claim follows from Lemma 6.3(2).

Now suppose that $(v - u) \mid (2s + 1)$ and $v \leq 2u$. Then $\mathbb{F}_{2^u}$ is a subfield of $K$. Let $\mathcal{B}$ be any additive subgroup of order $2^n$ containing the additive group $\mathcal{A}$ of $\mathbb{F}_{2^u}$.

In some cases we are also able to provide a plane model for $\tilde{S} = S/\mathcal{U}$.

**Theorem 6.6.** With the notation above, the following hold true:

1. Let $q = \bar{q}^n$ and $\mathcal{U}$ be the elementary abelian subgroup of $\tilde{T}$ consisting of all automorphisms $T_{0,c}$ with $c \in \mathbb{F}_{\bar{q}}$. Then the curve $\tilde{S}$ has genus $\tilde{g} = q_0(\frac{2}{q} - 1)$, and a plane model over $K$ of $\tilde{S}$ is given by

   $$\sum_{i=0}^{n-1} V^q_i = U^{2q_0}(U^q + U);$$

2. For a cyclic subgroup $\mathcal{U}$ of $\text{Aut}(S)$ of order 4, the curve $\tilde{S}$ has genus $\tilde{g} = \frac{1}{4}q_0(q - 2)$, and a plane model over $K$ of $\tilde{S}$ is given by

   $$\sum_{i=0}^{2s} V^{2i} = \sum_{i=0}^{2s} U^{2i} + \sum_{i=0}^{s} \left( \sum_{j=i}^{s} U^{2j} \right) U^{2i} + \sum_{i=s+2}^{2s} \left( \sum_{j=0}^{i-s-2} U^{2j} \right) U^{2i}.\tag{2}$$

**Proof.** (1) We have $\mathcal{U} = U_2$ and the formula for the genus follows from Theorem 6.1. We consider now the morphism $\phi := (1 : x : z^q + z) : S \to \mathbb{P}^2$; then $\tilde{S}$ is the non-singular model over $K$ of $\phi(S)$ since $\phi^{-1}(\phi(P_{(a,c)})) = \{ P_{(a,c+e)} : e \in \mathbb{F}_{\bar{q}} \}$. To write a plane equation for $\phi(S)$ we use Eq. (3.5) with $U := x$ and $V := z^q + z$ taking into account that $z^q + z = (z^q + z) + (z^q + z)^q + \ldots + (z^q + z)^{q-1}$.

(2) Since the cyclic subgroups of $\text{Aut}(S)$ of order 4 are pairwise conjugate in $\text{Aut}(S)$ (cf. (2.4)), we may assume $\mathcal{U}$ to be generated by $T_{1,0}$. Here $U_2$ has two elements and the formula for $\tilde{g}$ follows from Theorem 6.6. We consider now the morphism $\phi := (1 : x^2 + x : x^3 + x + z^q + z) : S \to \mathbb{P}^2$. We have that $\tilde{S}$ is the non-singular model over $K$ of $\phi(S)$ since $\phi^{-1}(\phi(P_{(a,c)})) = \{ T_{1,0}^i : i = 1, \ldots, 4 \}$. To write a plane equation for $\phi(S)$ we notice that

$$\sum_{i=0}^{2s} (x^3 + x + z^q + z)^{2i} = \sum_{i=0}^{2s} (x^3 + x)^{2i} + z^q + z;$$

therefore, with $U := x^2 + x$ and $V := x^3 + x + z^2 + z$, by Eq. (3.5),

$$x^q + x = \sum_{i=0}^{2s} (x^2 + x)^{2i},$$

and $x^3 + x = (x^2 + x) + (x^3 + x^2)$:

$$\sum_{i=0}^{2s} V^{2i} = \sum_{i=0}^{2s} U^{2i} + \sum_{i=0}^{2s} (x^2 + x + x^{2q_0}) U^{2i}.\tag{2}$$

Now the claimed equation follows from the relations

$$x^{2i} + x^{2q_0} = \begin{cases} 
\sum_{j=1}^{s} (x^2 + x)^{2j} & \text{if } i < s + 1, \\
0 & \text{if } i = s + 1, \\
(\sum_{j=0}^{s-i-2} (x^2 + x)^{2j})^{2q_0} & \text{if } i > s + 1.
\end{cases}$$
Type II. The basic fact here is that, up to conjugacy in $\text{Aut}(\mathcal{S})$, a subgroup $\mathcal{U}$ of $\text{Aut}(\mathcal{S})$ of order $2^vr$ ($v, r > 1$, $r \mid (q - 1)$) is contained in $\tilde{\text{T}}\tilde{\text{N}}$; moreover, the orders of its elements are known, cf. (2.5).

**Theorem 6.7.** For a subgroup $\mathcal{U}$ of $\tilde{\text{T}}\tilde{\text{N}}$ of order $2^vr$, with $v, r > 1$ and $r \mid (q - 1)$, let the subgroup $\mathcal{U}_2$ of $\mathcal{U}$ consist of all elements of order 2. If $\mathcal{U}_2$ has order $2^u$, then

$$\tilde{g} = \frac{q_0}{2v-u} \left( \frac{q}{2^u} - 1 \right);$$

in particular, $u \leq 2s + 1$, $v - u \leq s$ and $r$ divides $\frac{q}{2^u} - 1$.

**Proof.** The Riemann-Hurwitz genus formula states $2q_0(q - 1) - 2 = 2^vr(2\tilde{g} - 2) + \text{deg}(R)$, where $R$ is the ramification divisor of the natural morphism $\mathcal{S} \to \tilde{\mathcal{S}}$. We have to look at the points $P \in \mathcal{S}$ for which there exists $T \in \mathcal{U}$ with $T(P) = P$, and compute $i_{T,P} = v_P(T^*(\ell) - \ell)$, $\ell$ being a local parameter at $P$; by (4.2) the only possible fixed point of $\mathcal{U}$ is $A_4$. By the computation in the proof of Theorem 6.1,

$$\text{deg}(R) = (2q_0 + 2)(2^u - 1) + 2(2^v - 2^u) + \sum i_{T,A_4}$$

where the summation is extended over all the automorphisms $T \in \mathcal{U} \setminus \tilde{T}$ such that $T(A_4) = A_4$; from (4.2) we obtain $i_{T,A_4} = 2$ and the formula for $\tilde{g}$ follows. The numerical conditions follow from the fact that $\tilde{g}$ is a non-negative integer. □

**Corollary 6.8.** Let $u, v, r > 1$ be integers such that $v \geq u \geq 0$, $u \leq 2s + 1$, $v - u \leq s$ and $r$ a divisor of $(q - 1)$ and $\frac{q}{2^u} - 1$. Then there is a non-tame quotient curve of $\mathcal{S}$ whose genus is given by Theorem 6.7 provided that (6.1) holds true.

**Proof.** It follows from 6.3(2) and the structure of $\tilde{\text{T}}\tilde{\text{N}}$. □

Type III. The basic fact here is that each subgroup of $\text{Aut}(\mathcal{S})$ of order $2r$, $r > 1$ and $r \mid (q - 1)$, is conjugate to a subgroup of the dihedral subgroup $N_{\text{Aut}(\mathcal{S})}(\mathcal{N})$; cf. (2.6). We show the following.

**Theorem 6.9.** Let $\mathcal{U}$ be a subgroup of $\text{Aut}(\mathcal{S})$ of order $2r$ with $r > 1$ a divisor of $q - 1$. Then the quotient curve $\tilde{\mathcal{S}} = \mathcal{S}/\mathcal{U}$ has genus $\tilde{g} = \frac{q_0}{2} \left( \frac{q-1}{r} - 1 \right)$, and a plane model over $K$ of $\tilde{\mathcal{S}}$ is given by

$$f(V) = \sum (-1)^{i+j}(i+j-1)! \frac{i!j!}{U^iV^j(1 + V^{q_0})},$$

where the summation is extended over all pairs $(i,j)$ of non-negative integers with $i + 2j = (q - 1)/r$, and $f(t)$ is the polynomial defined in (4.1).

**Proof.** The genus: The subgroup $N_{\text{Aut}(\mathcal{S})}(\tilde{\mathcal{N}})$ is a dihedral group of order $2(q - 1)$ which comprises $\tilde{\mathcal{N}}$ together with a coset consisting entirely of elements of order 2. Hence $\mathcal{U}$ has $r - 1$ non-trivial elements of odd order and each of the remaining $r$ elements in $\mathcal{U}$ has order 2. Thus, by (4.2), the degree of the ramification divisor of the natural morphism $\mathcal{S} \to \tilde{\mathcal{S}}$ is $(2q_0 + 2)r + 2(r - 1)$ and the result follows from the Riemann-Hurwitz genus formula.
A plane model: Let $\psi := \tilde{\phi} \circ \phi : S \to \mathbb{P}^2$, where $\phi$ is the morphism defined in Section 4 and $\tilde{\phi}$ is the morphism on $\phi(S)$ defined by $(X : 1 : Z) \mapsto (1 : XZ : X^r + Z^r)$. We claim that $\tilde{S}$ is the non-singular model over $K$ of $\psi(S)$. Since $\phi$ is birational (see Lemma 4.5), to prove this claim it is enough to check that $\# \tilde{\phi}^{-1}(\tilde{\phi}(P)) = 2r$ for a (generic) point $P = (a : 1 : c) \in \phi(C)$. We have that $(a\tau^{-i} : 1 : c\tau^i), (c\tau^{-i} : 1 : a\tau^i) \in \tilde{\phi}^{-1}(\tilde{\phi}(P))$ ($i = 1, \ldots, r$), where $\tau$ is an element of order $r$ in $K^*$. On the other hand, let $P' = (\tilde{a} : 1 : \tilde{c})$ such that $\tilde{\phi}(P') = \tilde{\phi}(P)$. Then $\tilde{a}^r$ and $\tilde{c}^r$ are the roots of $W^2 + (a^r + c^r)W + a^r c^r = 0$ and whence the claim is proved.

To find an equation of $\psi(S)$ we start from the equation defining $\phi(S)$ in Lemma 4.5:

$$f(\tilde{X}\tilde{Y}) = (1 + (\tilde{X}\tilde{Y})^g_0)((\tilde{X}^{r^{(-1)/r}} + (\tilde{Y}^r)^{(q-1)/r})$$

Thus we need a formula relating the form $A^m + B^m$ with polynomials of type $A + B$ and $A^rB^r$. We can do that by means of Waring’s formula in two indeterminates over a finite field [22, Thm. 1.76], namely

$$(6.2) \quad A^m + B^m = \sum (-1)^{i+j} \frac{(i+j-1)!m}{i!j!} (A + B)^i(AB)^j,$$

where the summation is extended over all pairs $(i, j)$ of non-negative integers for which $i + 2j = m$ holds. Now the result follows by taking $m = \frac{q-1}{r} \equiv 1 \pmod{2}$, $U := \tilde{X}^r + \tilde{Y}^r$ and $V := \tilde{X}\tilde{Y}$.

**Type IV.** We use the fact that each subgroup of Aut($S$) of order $2r$, $r > 1$ and $r \mid (q \pm 2q_0 + 1)$, is conjugate under Aut($S$) to a subgroup of the dihedral subgroup of Aut($S$) which comprises the Singer subgroups $S_{\pm 1}$ together with a coset consisting entirely of non-trivial elements of order 2; cf. (2.7).

**Theorem 6.10.** Let $r > 1$ be an integer and $\mathcal{U}$ a subgroup of Aut($S$) of order $2r$.

1. If $r$ is a divisor of $q + 2q_0 + 1$, the quotient curve $\tilde{S} = S/\mathcal{U}$ has genus

$$\tilde{g} = \frac{q_0 - 1}{2} \left( \frac{q + 2q_0 + 1}{r} - 1 \right).$$

Furthermore, a plane model over $\mathbb{F}_{q^t}$ of $\tilde{S}$ is given by

$$\tilde{f}(V) = \sum (-1)^{i+j} \frac{(i+j-1)!}{i!j!} U^iV^{rj},$$

where the summation is extended over all pairs $(i, j)$ of non-negative integers with $i + 2j = (q + 2q_0 + 1)/r$, and $\tilde{f}(t)$ is the polynomial defined in (5.1);

2. If $r$ is a divisor of $q - 2q_0 + 1$, the quotient curve $\tilde{S} = S/\mathcal{U}$ has genus

$$\tilde{g} = \frac{q_0 + 1}{2} \left( \frac{q - 2q_0 + 1}{r} - 1 \right).$$

Furthermore, a plane model over $\mathbb{F}_{q^t}$ of $\tilde{S}$ is given by

$$bf(V) = \sum (-1)^{i+j} \frac{(i+j-1)!}{i!j!} U^iV^{rj}(V^{q_0-1} + V^{2q_0-1}),$$

where the summation is extended over all pairs $(i, j)$ of non-negative integers with $i + 2j = (q - 2q_0 + 1)/r$. 

- **Proof.**
where the summation is extended over all pairs $(i, j)$ of non-negative integers with $i + 2j = (q - 2q_0 + 1)/r$, $f(t)$ defined in (4.1), and $b$ as in Theorem 5.1(2).

Proof. The genus: The subgroup $U$ has $r - 1$ non-trivial elements of odd order and $r$ of even order; thus the degree of the ramification divisor is $(2q_0 + 2)r + \tilde{R}$ (cf. proof of Theorem 6.1). By (4.2), in case (1) we obtain $\tilde{R} = 0$ and in case (2), $\tilde{R} = 4(r - 1)$. Now the result follows from the Riemann-Hurwitz genus formula.

A plane model: To find the equations stated above we argue as in the proof of Theorem 6.9. For the case (1), the corresponding morphism $\phi$ is taken to be the one defined in Section 5; we use the plane model of $S$ in Lemma 5.5 written as

$$\tilde{f}(\tilde{X}\tilde{Y}) = (\tilde{X}^r)^{(q+2q_0+1)/r} + (\tilde{Y}^r)^{(q+2q_0+1)/r}.$$ 

Then we get the claimed equation from (6.2) with $m = \frac{q+2q_0+1}{r} \equiv 1 \pmod{2}$, $U := \tilde{X}^r + \tilde{Y}^r$ and $V := \tilde{X}\tilde{Y}$. For the case (2) we use the plane model of $S$ stated in Lemma 5.7. □

Type V. We use the fact that any any subgroup of $\text{Aut}(S)$ order $4r$ with $r > 1$ and $r \mid (q \pm 2q_0 + 1)$ is conjugate in $\text{Aut}(S)$ to a subgroup of $N_{\text{Aut}(S)}(S_{\pm 1})$ (which has order $4(q \pm 2q_0 + 1)$).

Theorem 6.11. Let $U$ be a subgroup of $\text{Aut}(S)$ of order $4r$, with a divisor $r > 1$ of $q \pm 2q_0 + 1$. Then the genus $\tilde{g}$ of the quotient curve $\tilde{S} = S/U$ is given by

$$\tilde{g} = \begin{cases} 
\frac{q_0-1}{4} + \frac{q_0+2q_0+1}{r} - 1 & \text{for } r \mid (q + 2q_0 + 1), \\
\frac{q_0+1}{4} + \frac{q_0-2q_0+1}{r} - 1 & \text{for } r \mid (q - 2q_0 + 1).
\end{cases}$$

Proof. The subgroup $U$ comprises $r$ elements of odd order together with the same number of elements of order 2 and $2r$ elements of order 4. By (4.2) the degree of the ramification divisor of the natural map $S \to \tilde{S}$ is $(2q_0 + 2)r + (2r)2 + \tilde{R}$, where $\tilde{R} = 0$ if $r \mid (q + 2q_0 + 1)$ and $\tilde{R} = 4(r - 1)$ if $r \mid (q - 2q_0 + 1)$. Now the proof follows by the Riemann-Hurwitz genus formula. □

Type VI. Let $q_0 = 2^s$. Set $\tilde{q} := 2^{2s+1}$, with $s$ a divisor of $s$ such that $2s + 1$ divides $2s + 1$. This is an arithmetical (necessary) condition in order that $\text{Aut}(S)$ contains a subgroup $U$ isomorphic to $S_{\pm 1}(\tilde{q})$.

Theorem 6.12. With the notation above, the genus of $\tilde{S} = S/U$ is given by

$$\tilde{g} = \frac{q_0(q - 1) - 1 + (\tilde{q}^2 + 1)\tilde{q}^2(\tilde{q} - 1) + \Delta}{(\tilde{q}^2 + 1)\tilde{q}^2(\tilde{q} - 1)},$$

where

$$\Delta := (\tilde{q}^2 + 1)((2q_0 + 2)(\tilde{q} - 1) + 2\tilde{q}(\tilde{q} - 1)) + \tilde{q}^2(\tilde{q}^2 + 1)(\tilde{q} - 2) + \tilde{q}^2(\tilde{q} + 2q_0 + 1)(\tilde{q} - 1)(\tilde{q} - 2\tilde{q}_0).$$

Proof. It is straightforward to see that $U$ has $(\tilde{q}^2 + 1)(\tilde{q} - 1)$ elements of order 2, and $(\tilde{q}^2 + 1)(\tilde{q}^2 - \tilde{q})$ elements of order 4. Furthermore, $U$ has $\frac{1}{2}\tilde{q}^2(\tilde{q}^2 + 1)$ subgroups of order $\tilde{q} - 1$. Also, $U$ has $\frac{1}{4}\tilde{q}^2(\tilde{q} + 2\tilde{q}_0 + 1)(\tilde{q} - 1)$ subgroups of order $\tilde{q} - 2\tilde{q}_0 + 1$. Finally, $U$ has
$\frac{1}{4}q^2(q - 2q_0 + 1)(q - 1)$ subgroups of order $q + 2q_0 + 1$. Thus by (4.2) the degree of the ramification divisor of $S \to \bar{S}$ equals

$$(q^2 + 1)[(2q_0 + 2)(q - 1) + 2q(q - 1)] + q^2(q^2 + 1)(q - 2) + q^2(q + 2q_0 + 1)(q - 1)(q - 2q_0),$$

whence the assertion follows by the Riemann-Hurwitz genus formula.

7. On curves with many rational points

Let $N_q(g)$ be the maximum number of $K$-rational points that a curve over $K$ of genus $g > 0$ can have. Our references for this section are [9] and [8].

The study of the function $N_q(g)$ is strongly motivated by applications, as already mentioned in the Introduction; in particular, good Goppa geometric codes have been constructed from the Suzuki curve by Matthews [24]. In general, no closed formula for $N_q(g)$ is known. The study of $N_q(g)$ viewed as function of $g$ was initiated by Serre [29]. He was able to compute $N_q(1)$ and $N_q(2)$.

For any non-negative integer $g$,

$$(7.1) \quad a_q(g) \leq N_q(g) \leq b_q(g) \leq q + 2g\sqrt{q} + 1,$$

where $a_q(g)$ is the number of $K$-rational points of a specific curve over $K$ of genus $g$, and $b_q(g)$ is a theoretical upper bound. One often takes $b_q(g)$ as the smallest number among the Serre’s bound, Ihara’s bound (cf. [8, p. 1]), or the one obtained via Explicit Formulas (see e.g. [31, V.3.4]).

We shall investigate the left hand side inequality in (7.1) with $q = 2q_0$, and $g = \tilde{g}$ the genus of a quotient curve $\bar{S}$ of the Suzuki curve $S$. Note that by (3.1) $\#\bar{S}(K) = q + 2q_0\tilde{g} + 1 \geq \lceil b/\sqrt{2} \rceil$: thus we might expect “many” $K$-rational points from the curve $\bar{S}$ (this is the case when $q \leq 128$ and $\tilde{g} \leq 50$ according to [8, Sect. 1]). We only consider the cases $q_0 = 2$, $q_0 = 4$, $q_0 = 8$, $\tilde{g} \leq 50$ in such a way that we can compare the number of rational points of the curves studied in this paper with the entries of van der Geer and van der Vlugt tables [8]; we remark that such tables are updated periodically.

1. $q_0 = 2$. Here $\#\bar{S}(K) = 9 + 4\tilde{g}$. We have the following data:

<table>
<thead>
<tr>
<th>References</th>
<th>Cor. 6.5</th>
<th>Thm. 4.1</th>
<th>Cor. 6.5</th>
<th>Cor. 6.5</th>
<th>Cor. 6.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\tilde{g}$</td>
<td>14</td>
<td>18</td>
<td>24</td>
<td>33 - 35</td>
<td>65</td>
</tr>
<tr>
<td>$N_{\tilde{g}}(\tilde{g})$</td>
<td>13</td>
<td>17</td>
<td>21</td>
<td>33</td>
<td>65</td>
</tr>
<tr>
<td>$#\bar{S}(K)$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The curve of genus 2 almost attains $N_{\tilde{g}}(2)$; it is given by

$$V^2 + V = \frac{(1 + U)^2U^4}{f(U)},$$

where $f(U) = U^3 + U^2 + 1$ (Remark 4.7). It would be interesting to find an explicit equation of a plane model of a curve realizing $N_{\tilde{g}}(2)$. However, this appears to be out of reach. The cases $\tilde{g} = 6, 14$ were already noticed by Stichtenoth [30, p. 205].

2. $q_0 = 4$. Here $\#\bar{S}(K) = 33 + 8\tilde{g}$. We have the following data:
We have $113 \leq N_{32}(10) \leq 143$, where the upper bound is obtained from Serre’s bound.

The equation of $S$ is given by

$$bf(V) = (U^5 + U^3V^5 + UV^{10})(V^3 + V^7),$$

where $b = \lambda^4 + \lambda^3 + \lambda^{-4} + \lambda^{-3}$ with $\lambda \in F_{32^4}$ of order 25, and $f(V) = 1 + V^2(1 + V) + V^9(1 + V)^2$. The cases $\bar{g} = 12$, $\bar{g} = 28$ and $\bar{g} = 30$ were already noticed by van der Geer and van der Vlugt [11] via fiber product of certain Artin-Schreier curves. We do not know if such curves are isomorphic to the corresponding quotient curves $S$ here. The curve of genus $\bar{g} = 14$ almost attains $N_{32}(14)$. We have $225 \leq N_{32}(24) \leq 245$, where the upper bound is obtained from Ihara’s bound; a plane model of $S$ is given by

$$bV^5f(U) = (U^3 + U^7)(U^{25} + V^{10}),$$

where $b$ and $f(U)$ are as above.

3. $q_0 = 8$. Here $\#S(K) = 129 + 16\bar{g}$. We have the following data:

<table>
<thead>
<tr>
<th>Reference</th>
<th>$\bar{g}$</th>
<th>$N_{32}(\bar{g})$</th>
<th>$#S(K)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cor. 6.5</td>
<td>1</td>
<td>150</td>
<td>145</td>
</tr>
<tr>
<td>Cor. 6.5</td>
<td>2</td>
<td>172</td>
<td>161</td>
</tr>
<tr>
<td>Cor. 6.5</td>
<td>3</td>
<td>192</td>
<td>177</td>
</tr>
<tr>
<td>Cor. 6.5</td>
<td>4</td>
<td>215 - 217</td>
<td>193</td>
</tr>
<tr>
<td>Cor. 6.5</td>
<td>6</td>
<td>243 - 261</td>
<td>225</td>
</tr>
<tr>
<td>Thm. 6.11</td>
<td>7</td>
<td>258 - 283</td>
<td>241</td>
</tr>
<tr>
<td>Cor. 6.5</td>
<td>8</td>
<td>257 - 305</td>
<td>257</td>
</tr>
<tr>
<td>Cor. 6.5</td>
<td>12</td>
<td>321 - 393</td>
<td>321</td>
</tr>
<tr>
<td>Thm. 6.10(1)</td>
<td>14</td>
<td>353 - 437</td>
<td>353</td>
</tr>
<tr>
<td>Thm. 5.1(2)</td>
<td>24</td>
<td>513 - 657</td>
<td>513</td>
</tr>
<tr>
<td>Cor. 6.5</td>
<td>28</td>
<td>577 - 745</td>
<td>577</td>
</tr>
<tr>
<td>Cor. 6.5</td>
<td>30</td>
<td>609 - 789</td>
<td>609</td>
</tr>
<tr>
<td>Thm. 5.1(1)</td>
<td>36</td>
<td>...</td>
<td>705</td>
</tr>
<tr>
<td>Thm. 6.11</td>
<td>49</td>
<td>...</td>
<td>913</td>
</tr>
</tbody>
</table>
For \( \tilde{g} = 8 \), the existence of a curve with 257 \( K \)-rational points was pointed out by Wirtz [34]. We have that \( \tilde{S} \) is hyperelliptic and it is defined by (cf. Remark 4.7)

\[
V^2 + V = \frac{(1 + U)^8 U^{64}}{f(U)},
\]

where \( f(U) = 1 + U^8(1 + U) + U^{25}(1 + U)^2 + U^{59}(1 + U)^4 \). We do not know whether \( \tilde{S} \) is isomorphic to Wirtz’s curve. For \( \tilde{g} = 12, 14, 24, 28, 30 \), the existence problem was solved affirmatively by van der Geer and van der Vlugt [11], [10]. Again, it is still unknown to us whether such curves are isomorphic to the corresponding \( \tilde{S} \). Furthermore, \( 705 \leq N_{128}(36) \leq 921 \); here the upper bound follows from Serre’s bound. A plane equation for \( \tilde{S} \) is given by

\[
V^5 \tilde{f}(U) = U^{145} + V^{10},
\]

where \( \tilde{f}(U) = 1 + U^8(1 + U) + U^{16}(1 + U)^{10} + U^{32}(1 + U)^{28} + U^{64} \). Finally, \( 913 \leq N_{128}(49) \leq 1207 \) where, again, the upper bound follows from Serre’s bound. Unfortunately in this case we do not have an explicit plane model for \( \tilde{S} \).

Acknowledgement: M. Giulietti and G. Korchmáros were supported by the Italian Ministry MIUR, project Strutture Geometriche, Combinatoria e loro applicazioni, PRIN 2001-2002, and by GNSAGA. The work of F. Torres was supported by the “Secretaria de Estado de Educación y Universidades del Ministerio de Educación, Cultura y Deportes de España” (SB2000-0225), CNPq-Brazil (306676/03-6) and PRONEX (66.2408/96-9).

References


