ACTA ARITHMETICA
122.3 (2006)

Quotient curves of the Suzuki curve

by

Massimo Giulietti (Perugia), Gábor Korchmáros (Potenza)
and Fernando Torres (Campinas)

1. Introduction. Throughout, let $K = \mathbb{F}_q$ be the finite field of order q and $\overline{K}$ 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 $|\#\mathcal{X}(K) - (q+1)| \le 2g\sqrt{q}$ is the *Hasse–Weil bound* on the number of its K-rational points. For possible applications to coding theory [12], [31], [8], 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 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 $\overline{K}$ (which actually coincides with the automorphism group over K); see [5, Sect. 11], [14], [27], [15].

Type	Number of rational points	Genus	Automorphism group
I: q square	$\sqrt{q}^3 + 1$	$\sqrt{q}(\sqrt{q}-1)/2$	$PGU(3,q)$
II: $q = 2q_0^2 > 2$	$q^2 + 1$	$q_0(q-1)$	$\mathcal{S}z(q)$
III: $q = 3q_0^2 > 3$	$q^3 + 1$	$3q_0(q-1)(q+q_0+1)/2$	$R(q)$

2000 *Mathematics Subject Classification*: Primary 11G20; Secondary 14G05, 20C33.
Key words and phrases: finite field, Suzuki group, quotient curve, curves with many rational points.

In addition, the enumerator $L(t)$ of their Zeta function is known (loc. cit.). In the table above $PGU(3,q)$, $\mathcal{S}z(q)$ 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 3 here, one expects to obtain curves with many rational points from curves $\widetilde{\mathcal{X}}$ that are K-covered by $\mathcal{X}$. Having in mind applications it is also important to have such curves in a form as explicit as possible. If $\mathcal{X}$ is the Hermitian curve over K, then $L(t) = (\sqrt{q}\,t+1)^{2g}$ with $g = \sqrt{q}(\sqrt{q}-1)/2$; see e.g. [31, V.1.15]. Thus by the aforementioned Serre's remark, the number of K-rational points of $\widetilde{\mathcal{X}}$ also attains the Hasse–Weil upper bound. In particular, by means of quotient curves of $\mathcal{X}$, 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 $\mathcal{S}$. The case of curves of type III was investigated by Çakçak and Özbudak [2].

From now on, $q_0 := 2^s$ with $s \geq 1$, and $q := 2q_0^2$. The enumerator of the Zeta function of $\mathcal{S}$ 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 $\widetilde{\mathcal{S}}$ of genus $\widetilde{g}$ which is K-covered by $\mathcal{S}$ is given by (cf. Section 3)

$$\#\widetilde{\mathcal{S}}(K) = q + 2q_0\widetilde{g} + 1.$$

This value is in the interval from which the entries of the tables of curves with many rational points are taken for $\widetilde{g} \leq 50$, $q \leq 128$ in van der Geer and van der Vlugt tables [9]. In Sections 4 and 5 we obtain an exhaustive list of *tame* quotient curves of $\mathcal{S}$, namely quotients arising from subgroups of $\mathrm{Aut}(\mathcal{S})$ 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 $\mathcal{S}$, namely quotient arising from subgroups of $\mathrm{Aut}(\mathcal{S})$ 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 $\mathcal{S}$; for some of these curves we also provide a plane equation. A concrete application of our results provides new

entries in the tables [9]: 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 to that in [3] and [4]: a concrete realization of $\mathcal{S}$ 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 $\mathcal{S}z(q)$ acts linearly on $\mathcal{S}$ (cf. Section 2 and Theorem 3.2).

2. Preliminary results on the Suzuki group. In the introduction we have mentioned that the automorphism group $\mathrm{Aut}(\mathcal{S})$ of the Suzuki curve $\mathcal{S}$ is isomorphic to the Suzuki group $\mathcal{S}z(q)$. We summarize those results on the structure of $\mathcal{S}z(q)$ which play a role in the present work. For more details, the reader is referred to [20, Chap. XI.3], [33], [13, Chap. 17] and [23].

In Section 3 we will show that the curve $\mathcal{S}$ can be embedded in $\mathbb{P}^4$ (Theorem 3.1); this raises the problem of exhibiting $\mathcal{S}z(q)$ as a subgroup of automorphisms of $\mathbb{P}^4$. We start from a well known concrete realization of $\mathcal{S}z(q)$, namely as a subgroup of the automorphism group $\mathrm{Aut}(\mathbb{P}^3)$ of $\mathbb{P}^3$ (loc. cit.). Let $\widetilde{T} := \{T_{a,c} : a, c \in K\}$ and $\widetilde{N} := \{N_d : d \in K^*\}$, where $T_{a,c}$ and N_d are the elements of $\mathrm{Aut}(\mathbb{P}^3)$ defined respectively by the matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ c & a^{2q_0} & 1 & 0 \\ a^{2q_0+2} + ac + c^{2q_0} & a^{2q_0+1} + c & a & 1 \end{pmatrix}, \quad \begin{pmatrix} d^{-q_0-1} & 0 & 0 & 0 \\ 0 & d^{-q_0} & 0 & 0 \\ 0 & 0 & d^{q_0} & 0 \\ 0 & 0 & 0 & d^{q_0+1} \end{pmatrix}.$$

In addition, let $W \in \mathrm{Aut}(\mathbb{P}^3)$ 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 $\mathcal{S}z(q)$ can be assumed to be the subgroup of $\mathrm{Aut}(\mathbb{P}^3)$ generated by $\widetilde{T}, \widetilde{N}$ and W. Next consider the homomorphism of groups

$$\mathbf{L} : \mathcal{S}z(q) \to \mathrm{Aut}(\mathbb{P}^4)$$

defined on the generators of $\mathcal{S}z(q)$ by $T_{a,c} \mapsto \mathbf{T}_{a,c}$, $N_d \mapsto \mathbf{N}_d$, $W \mapsto \mathbf{W}$, where the images are defined respectively by the matrices:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ a & 1 & 0 & 0 & 0 \\ a^{q_0+1}+c^{q_0} & a^{q_0} & 1 & 0 & 0 \\ c & a^{2q_0} & 0 & 1 & 0 \\ a^{2q_0+2}+ac+c^{2q_0} & a^{2q_0+1}+c & 0 & a & 1 \end{pmatrix},$$

$$\begin{pmatrix} d^{-q_0-1} & 0 & 0 & 0 & 0 \\ 0 & d^{-q_0} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & d^{q_0} & 0 \\ 0 & 0 & 0 & 0 & d^{q_0+1} \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let $\widetilde{\mathbf{T}} := \mathbf{L}(\widetilde{T})$, $\widetilde{\mathbf{N}} := \mathbf{L}(\widetilde{N})$ and $\mathbf{W} := \mathbf{L}(W)$. Then, as $\mathcal{S}z(q)$ is simple (loc. cit.), we can assume that $\mathcal{S}z(q)$ is the subgroup of $\mathrm{Aut}(\mathbb{P}^4)$ generated by $\widetilde{\mathbf{T}}$, $\widetilde{\mathbf{N}}$ and $\mathbf{W}$. Some other basic properties of the Suzuki group that we shall need are the following (loc. cit.):

(2.1) A cyclic subgroup of $\mathcal{S}z(q)$ of order $r > 1$, r a divisor of $q-1$, is conjugate in $\mathcal{S}z(q)$ to the subgroup $\{\mathbf{N}_d \in \widetilde{\mathbf{N}} : d \in K,\ d^r = 1\}$.

(2.2) Up to conjugacy there exist two cyclic subgroups of $\mathcal{S}z(q)$, $\mathcal{S}_1$ and $\mathcal{S}_{-1}$, of order $q+2q_0+1$ and $q-2q_0+1$ respectively. Such subgroups are called the *Singer subgroups* of $\mathcal{S}z(q)$. Also, their action on the K-rational points of $\pi(\mathcal{S})$, where π is the morphism defined in (3.6), is semiregular.

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

(2.4) The cyclic subgroups of $\mathcal{S}z(q)$ of order 4 are pairwise conjugate in $\mathcal{S}z(q)$.

(2.5) A subgroup of $\mathcal{S}z(q)$ of order $2^v r$, $r, v > 1$, r a divisor of $q-1$, is conjugate in $\mathcal{S}z(q)$ to a subgroup of $\widetilde{\mathbf{T}}\widetilde{\mathbf{N}}$. The order of a non-trivial element in $\widetilde{\mathbf{T}}\widetilde{\mathbf{N}}$ is either a 2-power or a divisor of $q-1$ according as it belongs to $\widetilde{\mathbf{T}}$ or not.

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

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

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

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

(2.10) Any non-trivial subgroup of $\mathcal{S}z(q)$ is conjugate in $\mathcal{S}z(q)$ to one of the above subgroups.

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

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

where $i = \sqrt{-1}$. Notice that $\widetilde{\mathcal{S}}$ is maximal over $\mathbb{F}_{q^4}$. Next we describe a plane model of $\mathcal{S}$ 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

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

are q^2+1 and $q_0(q-1)$ respectively. Therefore by [6, Sect. 3], we may assume that $\mathcal{S}$ 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 $84(g-1)$ valid in zero characteristic.

Now we introduce a geometric invariant (over K) on the curve $\mathcal{S}$. Among other properties, this invariant will allow us to consider $\mathcal{S}$ as an embedded curve in $\mathbb{P}^4$ in such a way that $\mathcal{S}z(q)$ will act linearly on $\mathcal{S}$; see Theorem 3.2. Let $h(t) := t^{2g}L(t^{-1})$ with $L(t)$ as above. This polynomial is the characteristic polynomial of the Frobenius morphism $\widetilde{\mathbf{\Phi}}$ over K on the Jacobian $\mathcal{J}$ of $\mathcal{S}$; this morphism is induced by the Frobenius morphism $\mathbf{\Phi}$ over K on $\mathcal{S}$. It turns out that $\widetilde{\mathbf{\Phi}}$ is semisimple (see e.g. [26, p. 251]) and thus $qI + 2q_0\widetilde{\mathbf{\Phi}} + \widetilde{\mathbf{\Phi}}^2 = 0$ on $\mathcal{J}$. We can state this property by using divisors on $\mathcal{S}$; to do that we use the fact that $f \circ \mathbf{\Phi} = \widetilde{\mathbf{\Phi}} \circ f$, where $f : \mathcal{S} \to \mathcal{J}$, $P \mapsto [P - P_0]$, is the natural morphism that maps $P_0 \in \mathcal{S}(K)$ to $0 \in \mathcal{J}$. Therefore, for $P \in \mathcal{S}$ and $P_0 \in \mathcal{S}(K)$ the following linear equivalence on $\mathcal{S}$

holds true:

$$qP + 2q_0\mathbf{\Phi}(P) + \mathbf{\Phi}^2(P) \sim (q + 2q_0 + 1)P_0. \tag{3.3}$$

This motivates the definition of the following complete linear series on $\mathcal{S}$:

$$\mathcal{D} = \mathcal{D}_{\mathcal{S}} := |(q + 2q_0 + 1)P_0|.$$

The equivalence (3.3) shows that the definition of $\mathcal{D}$ 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 $P \in \mathcal{S}$. We subsume two important properties of $\mathcal{D}$:

THEOREM 3.1.

(1) ([16, Prop. 1.5]) *The dimension of $\mathcal{D}$ is four.*
(2) *The linear series $\mathcal{D}$ is very ample.*

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

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

Put

$$z := x^{2q_0+1} + y^{2q_0}. \tag{3.4}$$

By (3.2) the functions x and z satisfy

$$z^q + z = x^{2q_0}(x^q + x); \tag{3.5}$$

therefore, $\mathrm{div}_\infty(z) = (q + 2q_0)P_0$ 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 $\pi : \mathcal{S} \to \mathbb{P}^4$ be the morphism defined by $\mathcal{D}$. We show that π separates points and separates tangent vectors; cf. [17, p. 308]. To see the former condition, it is enough to show that π is injective. Assume $\pi(P) = \pi(Q)$. Then the linear equivalence (3.3) implies

$$\{P, \mathbf{\Phi}(P), \mathbf{\Phi}^2(P)\} = \{Q, \mathbf{\Phi}(Q), \mathbf{\Phi}^2(Q)\}.$$

We find that $\mathbf{\Phi}^3(P) = P$ and $\mathbf{\Phi}^3(Q) = Q$; thus $P = Q$ since $\mathcal{S}(\mathbb{F}_{q^3}) = \mathcal{S}(K)$ by (3.1). To prove the latter condition we use some facts concerning Weierstrass point theory; our reference is Stöhr–Voloch's paper [32]. We have to show that the first positive element $j_1 = j_1(P)$ of the $(\mathcal{D}, P)$-order sequence equals 1, or equivalently that there exists $D' \in \mathcal{D}$ such that $v_P(D') = 1$. If $P \notin \mathcal{S}(K)$, then $j_1 = 1$ 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 $n_3 = q + 2q_0$ $(*)$. (Observe that $(*)$ already holds true for the point P_0 over $x = \infty$.) As a matter of fact, property $(*)$ was proved in [6, p. 43] and the proof of the theorem is complete. ∎

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

$$\pi := (1 : x : y : z : w), \tag{3.6}$$

where x, y, z are as above and w is a K-rational function such that $\mathrm{div}_\infty(w) = (q + 2q_0 + 1)P_0$. We may assume

$$w := xy^{2q_0} + z^{2q_0}. \tag{3.7}$$

In fact, (3.2) and (3.5) imply the following relation among x, y and w:

$$w^q + w = y^{2q_0}(x^q + x),$$

whence $\mathrm{div}_\infty(w) = (q + 2q_0 + 1)P_0$. Next we 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 (3.2) we obtain

$$y = x^{q_0+1} + z^{q_0}; \tag{3.8}$$

from (3.7), (3.8) and (3.5) we get

$$w = x^{2q_0+2} + xz + z^{2q_0}. \tag{3.9}$$

Therefore $\mathcal{S}$ can be assumed to be the locus in $\mathbb{P}^4$ defined by the set of points

$$P_{(a,c)} := (1 : a : b : c : d), \quad \text{and} \quad A_4 := \pi(P_0) = (0 : 0 : 0 : 0 : 1), \tag{3.10}$$

with $x = a \in \overline{K}$, $z = c \in \overline{K}$ satisfying (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 $\mathcal{S}z(q)$ established in Section 2 coincides with $\mathrm{Aut}(\mathcal{S})$.

THEOREM 3.2. *The isomorphic image of* $\mathcal{S}z(q)$ *in* $\mathrm{Aut}(\mathbb{P}^4)$ *stated in Section* 2 *acts linearly on* $\mathcal{S}$.

Proof. By (3.10) and the definition of $\widetilde{\mathbf{T}}, \widetilde{\mathbf{N}}$ and $\mathbf{W}$ (cf. Section 2) it follows that each element of the isomorphic image of $\mathcal{S}z(q)$ in $\mathrm{Aut}(\mathbb{P}^4)$ acts linearly on $\mathcal{S}$. ∎

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 $\mathrm{Aut}(\mathcal{S})$ **of order** $q - 1$**.** For a divisor $r > 1$ of $q - 1$, let $\mathcal{U}$ be a cyclic subgroup of $\mathrm{Aut}(\mathcal{S})$ of order r. As mentioned in (2.1), $\mathcal{U}$ is unique up to conjugacy, and we may assume $\mathcal{U} = \{\mathbf{N}_d \in \widetilde{\mathbf{N}} : d \in K,\ d^r = 1\}$. Let $\widetilde{\mathcal{S}} = \mathcal{S}/\mathcal{U}$

denote the quotient curve of $\mathcal{S}$ by $\mathcal{U}$, and $\widetilde{g}$ its genus. The objective of this section is to prove the following theorem. Let $s \in \mathbb{N}$ be such that $q_0 = 2^s$, and set

$$f(t) := 1 + \sum_{i=0}^{s-1} t^{2^i(2q_0+1)-(q_0+1)}(1+t)^{2^i}. \tag{4.1}$$

THEOREM 4.1. *With the notation above*:

(1) $\widetilde{g} = \frac{1}{r}q_0(q-1)$.
(2) *The following curve is a plane model over K of $\widetilde{\mathcal{S}}$*:

$$V^{\frac{1}{r}(q-1)}f(U) = (1+U^{q_0})(U^{q-1} + V^{\frac{2}{r}(q-1)}).$$

We need some preliminary results. Consider the morphism

$$\phi := (x : y : z) : \mathcal{S} \to \mathcal{C} := \phi(\mathcal{S}) \subseteq \mathbb{P}^2.$$

The results in Claims 4.2–4.4 and Lemma 4.5 below will show that $\mathcal{C}$ is a plane model over K of $\mathcal{S}$.

CLAIM 4.2.

(1) *The divisor defined by ϕ is given by $E = -A_0 + (q+2q_0)A_4$.*
(2) *The morphism ϕ is birational so that $\mathcal{C}$ is a curve of degree $q+2q_0-1$.*

Proof. (1) By (3.2), (3.5) and the fact that $x : \mathcal{S} \to \mathbb{P}^1$ is unramified but at ∞, where it is totally ramified,

$$\begin{aligned} \operatorname{div}(x) &= A_0 + D_1 - qA_4, \\ \operatorname{div}(y) &= (q_0+1)A_0 + D_2 - (q+q_0)A_4, \\ \operatorname{div}(z) &= (2q_0+1)A_0 + D_3 - (q+2q_0)A_4, \end{aligned} \tag{4.2}$$

with $D_1 = \sum P_{(0,y^{2q_0})}$, $y^{q-1} = 1$; $D_2 = \sum P_{(x,x^{2q_0+1})}$, $x^{q-1} = 1$; and $D_3 = \sum P_{(x,0)}$, $x^{q-1} = 1$. Therefore $E = -A_0 + (q+2q_0)A_4$.

(2) For a generic point $P_{(a,c)} \in \mathcal{S}$ 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 $P_{(x,z)} \in \mathcal{S}$. ∎

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 $\mathcal{C}$ above. The intersection divisor of Y and $\mathcal{C}$ is codified by the divisor $\phi^*(Y) := \operatorname{div}(y) + E = q_0A_0 + D_2 + q_0A_4$; cf. Claim 4.2 and (4.2). This means that the line Y intersects $\mathcal{C}$ 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 $\mathcal{C}$ 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 $\mathbf{N}_d \in \widetilde{\mathbf{N}}$ induces an automorphism on $\mathcal{C}$ by means of $(X:Y:Z) \mapsto (dX : d^{q_0+1}Y : d^{2q_0+1}Z)$. Thus there exists $e \in \overline{K}^*$ such that $f_1(X,Z) = ef_1(d^{-q_0}X, d^{q_0}Z)$; we then have $e=1$ 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

$$f_1(X,Z) = f_2(X,Z) + X^{q-1}\sum_{i,j;\,i\neq j} a_{i,j}(XZ)^j + Z^{q-1}\sum_{i,j;\,i\neq j} a_{i,j}(XZ)^i.$$

On the other hand, the automorphism $\mathbf{W}$ of $\mathcal{S}$ (cf. Section 2) induces an automorphism on $\mathcal{C}$ via $(X:Y:Z) \mapsto (Z:Y:X)$. Thus $a_{i,j} = a_{j,i}$ and so

$$f_1(X,Z) = \widetilde{f}_2(XZ) + (\widetilde{f}_3(XZ) + (XZ)^{q_0})(X^{q-1} + Z^{q-1}),$$

where $\widetilde{f}_2(t)$ and $\widetilde{f}_3(t)$ are polynomials of degree at most $q/2+q_0-1$ and q_0-1 respectively.

Claim 4.3. $\deg(\widetilde{f}_2(t)) = (q-2)/2$.

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

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

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 as $a=1$ or $a \in K\setminus\{1\}$. Thus

$$\phi^*(L) = (2q_0+1)P_{(1,1)} + \sum_{x\notin K\setminus\{0,1\}} P_{(x,x)}$$

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

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

Claim 4.4.

(1) *There exists $e \in K^*$ such that $ef(t) = \widetilde{f}_2(t)$, where $f(t)$ is the polynomial defined in* (4.1).
(2) $\widetilde{f}_3(t) = 1$ *and* $e=1$.

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

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

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

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

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

(2) By (1), we have

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

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 (3.2) and (3.5), $\xi = x^{-q_0} + x^{q-q_0+1} + \cdots$ and $\zeta = x^{q_0} + x^{q'} + \cdots$, where $q' > q + q_0 - 1$; thus $\xi\zeta = 1 + x^{q-1} + \cdots$. By the definition of $f(t)$, $f = 1 + x^{q-1} + \cdots$. Write $\widetilde{f}_3(t) = a_0 + a_m t^m + a_{m+1} t^{m+1} + \cdots$, and suppose that $m = 2^n k \geq 1$ and $a_m \neq 0$. Then $\widetilde{f}_3 = a_0 + a_m(1 + x^{q-1} + \cdots)^{2n} + \cdots$, 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

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

and so $a_0 = 1$ and $e = 1$. ∎

We summarize the results above in the following.

LEMMA 4.5. *The Suzuki curve $\mathcal{S}$ admits a plane model over K defined by*

$$f_1(X, Z) := f(XZ) + (1 + (XZ)^{q_0})(X^{q-1} + Z^{q-1}),$$

where $f(t)$ is the polynomial given in (4.1).

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

The plane equation: Let $\widetilde{\mathcal{C}}$ be the absolutely irreducible plane curve over K whose function field is $K(XZ, Z^r)$. By the definition of $\mathbf{N}_d$, we have the inclusion $K(XZ, Z^r) \subseteq K(X, Z)^{\mathcal{U}}$. 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 the above inclusion is an equality. Taking $U := XZ$ and $V := Z^r$ we obtain the required equation for $\widetilde{\mathcal{C}}$, which is clearly a plane model of $\widetilde{\mathcal{S}}$. ∎

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

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

$$v^2 + v = \frac{(u+1)^{2q_0}u^{q-1}}{f(u)^2}.$$

5. Quotient curves arising from the subgroups of the Singer subgroups of $\mathrm{Aut}(\mathcal{S})$**.** Let $\mathcal{S}_1$ and $\mathcal{S}_{-1}$ denote the Singer subgroups of $\mathrm{Aut}(\mathcal{S})$ whose orders are $q+2q_0+1$ and $q-2q_0+1$ respectively; cf. (2.2). For a subgroup $\mathcal{U}$ of either $\mathcal{S}_1$ or $\mathcal{S}_{-1}$, denote by $\widetilde{\mathcal{S}} = \mathcal{S}/\mathcal{U}$ the quotient curve of $\mathcal{S}$ by $\mathcal{U}$, and $\widetilde{g}$ its genus. The aim of this section is to prove the following theorem. Let $s \in \mathbb{N}$ be such that $q_0 = 2^s$, and set

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

THEOREM 5.1. *With the notation above*:

(1) *If* $\mathcal{U}$ *is a subgroup of* $\mathcal{S}_1$ *of order* $r > 1$*, then*

$$\widetilde{g} = \frac{1}{r}(q+2q_0+1)(q_0-1)+1$$

and a plane model over $\mathbb{F}_{q^4}$ *of* $\widetilde{\mathcal{S}}$ *is given by*

$$V^{\frac{1}{r}(q+2q_0+1)}\widetilde{f}(U) = U^{q+2q_0+1} + V^{\frac{2}{r}(q+2q_0+1)}.$$

(2) *If* $\mathcal{U}$ *is a subgroup of* $\mathcal{S}_{-1}$ *of order* $r > 1$*, then*

$$\widetilde{g} = \frac{1}{r}(q-2q_0+1)(q_0+1)-1$$

and a plane model over $\mathbb{F}_{q^4}$ *of* $\widetilde{\mathcal{S}}$ *is given by*

$$bV^{\frac{1}{r}(q-2q_0+1)}f(U) = (U^{q_0-1}+U^{2q_0-1})(U^{q-2q_0+1}+V^{\frac{2}{r}(q-2q_0+1)}),$$

where $\widetilde{f}(t)$ *and* $f(t)$ *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 $\widetilde{\mathcal{S}}$, 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 5.2–5.4 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 $P = P_{(a,c)} \in \mathcal{S}$. Then $a = \mu$ 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 ϕ is birational; cf. (5.5) below. Let E be the divisor defined by ϕ. Then $v_{A_4}(E) = q + 2q_0 + 1$, and the base points of the linear series associated to ϕ are the common zeroes of h_0, h_1 and h_2.

Claim 5.2. *We have*

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

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 $c \in \overline{K}$ defined via (3.5). If $\widetilde{c} := c/b$, then $b(\widetilde{c}^q + \widetilde{c}) = \mu^{2q_0}(\mu^q + \mu)$; now taking into consideration (3.8) and the definition of h_0, we conclude that $\widetilde{c}$ is a solution of the system

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

From the definition of b it follows that $\widetilde{c}$ 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. ∎

Assume that λ 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 $\mathcal{C}$. The intersection divisor of X and $\mathcal{C}$ is codified by $\phi^*(X) = \mathrm{div}(h_0) + E = \mathrm{div}_0(h_0) + A_4$ by the previous claim. Let $\mathbf{B} := \mathbf{T}_{0,b} \circ \mathbf{W} \in \mathrm{Aut}(\mathcal{S})$. Thus $\mathbf{B}$ is defined by the matrix (cf. Section 2)

$$B = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & b^{q_0} \\ 0 & 1 & 0 & 0 & b \\ 1 & 0 & 0 & b & b^{2q_0} \end{pmatrix}.$$

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 $\deg(h_0) = q + 2q_0$); thus

$$\phi^*(X) = \sum_{i=1}^{q+2q_0+1} \mathbf{B}^i(A_0). \tag{5.3}$$

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

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

A straightforward computation shows that

$$MBM^{-1} = \Lambda, \tag{5.4}$$

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 M defines h_0, and we now define h_1 and h_2 by using the second and fourth row respectively; that is to say,

$$h_1 := \mu + x + \lambda z + \lambda\mu w, \qquad h_2 := \mu + x + \lambda^{-1} z + \lambda^{-1}\mu w. \tag{5.5}$$

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

$$\mathbf{B}^i(A_0) = \mathbf{M}^{-1}(0 : \lambda^i\mu : \lambda^{iq}\mu^q : \lambda^{-i}\mu : \lambda^{-iq}\mu^q)$$

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

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

$f_2(Y, Z)$ being a polynomial of degree at most $q + 2q_0$. To normalize $f_2(Y, Z)$ we use the fact that the automorphism $\mathbf{B}$ above induces an automorphism on $\mathcal{C}$ 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

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

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

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

Proof. Consider the line $L : Y + \lambda^2 Z = 0$; since $\lambda^2 h_2 + h_1 = (\lambda^2 + 1)(x + \mu)$,

$$\phi^*(L) = \mathrm{div}(x + \mu) + E = \mathrm{div}_0(x + \mu) + (2q_0 + 1)A_4$$

(cf. (4.2) and Claim 5.2). Thus $\deg(\widetilde{f}_2(t^2)) = q$ as $\phi(A_4) \in X$. ∎

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

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

$$(1 + a^{2q_0-1})^{q_0}\widetilde{f}(a^{2q_0-1}) = 1 + \mathrm{Tr}_{K|\mathbb{F}_2}(a);$$

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

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

Now we compute the roots of $\widetilde{f}_2(t)$. By the proof of Claim 5.3, such roots arise from the points $(1:Y:Z)\in\mathcal{C}$ 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

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

with z such that $b(z^q+z)=\mu^{2q_0}(\mu^q+\mu)$ $(*)$. Therefore $a\in\overline{K}$ is a root of $\widetilde{f}_2(t)$ if and only if $a=B(z)^{4q_0-2}$, 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 $\widetilde{f}(t)$ is invariant under the map $b\mapsto b^2$, we conclude that there exists $e\in\overline{K}$ such that $\widetilde{f}(t)=e\widetilde{f}_2(t)$. Now $\phi(P_{(\mu^{-1},\lambda\mu^{-1})})=(1:0:\lambda^{-1})$ and we have $e=1$. ∎

We have thus proved the following lemma.

LEMMA 5.5. *The Suzuki curve $\mathcal{S}$ admits a plane model over $\mathbb{F}_{q^4}$ defined by*

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

where $\widetilde{f}(t)$ 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 $\mathcal{C}$. By (4.2) and Claim 5.2,

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

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 $\mathbf{B}^i(A_0)$ $(i=2,\dots,q-2q_0+1)$ are zeroes of h_0; thus, up to multiplicity, there are $4q_0$ zeroes of h_0 missing. By the definition of h_0 and equations (3.2) and (3.5) we have

$$\begin{aligned}h_0^q+h_0&=(x^q+x)(b^{q_0-1}+x^{q_0}+b^{q_0-1}x^{2q_0})\\&=[(x+a)^q+(x+a)+a^q+a][(x-a)^{q_0}+b^{q_0-1}(x+a)^{2q_0}\\&\quad+b^{q_0}+a^{q_0}+b^{q_0-1}a^{2q_0}],\end{aligned}$$

$P_{(a,c)}$ being a zero of h_0. Since $\mu\notin K$, it follows that $v_{P_1}(h_0)=v_{P_2}(h_0)=q_0$. Now by using the system (5.2) with μ^{-1} instead of μ we find the remaining two zeroes of h_0, namely

$$P_3:=P_{(\mu^{-1},\lambda^q\mu^{-1})},\qquad P_4:=P_{(\mu^{-1},\lambda^q\mu^{-1}+b)};$$

moreover, $v_{P_3}(h_0)=v_{P_4}(h_0)=q_0$ and hence

$$\phi^*(X)=(q_0-1)P_1+(q_0-1)P_2+q_0P_3+q_0P_4+\sum_{i=1}^{q-2q_0+1}\mathbf{B}^i(A_0). \tag{5.6}$$

Next we compute the intersection divisor of X and $\mathcal{C}$: we have

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

where $Q_1 := \phi(P_1) = \phi(P_4) = (0 : 1 : 0)$ and $Q_2 := \phi(P_2) = \phi(P_3) = (0 : 0 : 1)$ (from (4.2) and the fact that $h_1 = \lambda^2 h_2 + (\lambda^2 + 1)(x + \mu)$). 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 $\mathcal{C}$ induced by $\mathbf{B}$ and $\mathbf{W} \circ \mathbf{B} \in \mathrm{Aut}(\mathcal{S})$ via $(X : Y : Y) \mapsto (X : \lambda Y : \lambda^{-1} Z)$ and $(X : Y : Z) \mapsto (X : Z : Y)$ respectively, we can further assume that $f_2(Y, Z) = \widetilde{f}_2(YZ)$ and $f_3(Y, Z) = \widetilde{f}_3(YZ)$ with $\widetilde{f}_2(t), \widetilde{f}_3(t) \in \mathbb{F}_{q^4}[t]$.

Claim 5.6.

(1) *With $f(t)$ defined in* (4.1), *there exists $e \in \mathbb{F}_{q^4}^*$ such that $ef(t) = \widetilde{f}_2(t)$.*

(2) *There exists $e' \in \mathbb{F}_{q^4}$ such that $\widetilde{f}_3(t) + t^{2q_0-1} = e'(t^{q_0} + t^{2q_0-1})$.*

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 $\mathcal{S}$ defining the function field of $\mathcal{S}$. Thus

$$ef(\xi\zeta) = (\widetilde{f}_3(\xi\zeta) + (\xi\zeta)^{2q_0-1})(\xi^{q-2q_0+1} + \zeta^{q-2q_0+1}).$$

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 $\widetilde{f}_3(t)$ 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 $\widetilde{f}_3(t)$ follows. Now for $a \in \overline{K}$ a root of $\widetilde{f}_3(t) + t^{2q_0-1}$, 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 ℓ be a local parameter at $P = P_{(a,bc)}$; then

$$\begin{aligned}
h_0 &= (b^{q_0-1}(1 + a^{2q_0}) + a^{q_0})\ell + \cdots, \\
h_1 &= h_1(P_i) + (1 + \lambda(a^{2q_0} + \mu a^{2q_0+1} + \mu bc))\ell + \cdots, \\
h_2 &= h_2(P_i) + (1 + \lambda^{-1}(a^{2q_0} + \mu a^{2q_0+1} + \mu bc))\ell + \cdots,
\end{aligned}$$

and it follows that $v_P(\xi\zeta - P) > 0$ for some i and also that $a = 0$ or 1. Thus 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

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

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,

$$\begin{aligned} h_0 &= b^{q_0-1}x + x^{q_0+1} + \cdots, \\ h_1 &= \mu + x + \lambda x^{2q_0+1} + \cdots, \\ h_2 &= \mu + x + \lambda^{-1} x^{2q_0+1} + \cdots, \end{aligned} \tag{5.8}$$

whence

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

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

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

where $\varrho := b^{-q_0}\mu^{-1}$. The order at 0 of the former series is c/b^{2q_0-1}; for the latter, it is enough to compute the order at 0 of

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

By (5.8) and some computations,

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

thus we obtain

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

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

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

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

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 $\widetilde{g}$: By the proof of Claim 5.2 (see (5.3) and (5.6) above), the natural morphism $\mathcal{S} \to \widetilde{\mathcal{S}}$ is unramified or totally ramified precisely at four points according as $\mathcal{U} \subseteq \mathcal{S}_1$ or $\mathcal{U} \subseteq \mathcal{S}_{-1}$. Then the formula for $\widetilde{g}$ is computed by the Riemann–Hurwitz genus formula.

The plane equation: Let $\widetilde{\mathcal{C}}$ be the absolutely irreducible plane curve over K whose function field is $K(YZ, Z^r)$. By the definition of $\mathcal{S}_{\pm 1}$, we have the

inclusion $K(YZ, Z^r) \subseteq K(Y, Z)^{\mathcal{U}}$. On the other hand, from the definition of $f_1(X, Z)$ in Lemmas 5.5 and 5.7,

$$[K(Y, Z) : K(YZ, Z^r)] = [K(YZ, Z) : K(YZ, Z^r)] = r$$

and thus the inclusion is an equality. Taking $U := YZ$ and $V := Z^r$ we obtain the required equation for $\widetilde{\mathcal{C}}$, which is clearly a plane model of $\widetilde{\mathcal{S}}$. ∎

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 $\mathbf{B}$ defined above, and ϕ is the morphism defined by the linear series cut out on $\mathcal{S}$ by hyperplanes through L. By the proof of Claim 5.2, (5.3) and (5.6), the natural morphism $\mathcal{S} \to \widetilde{\mathcal{S}}$ is unramified or totally ramified at the aforementioned points according as $\mathcal{U} \subseteq \mathcal{S}_1$ or $\mathcal{U} \subseteq \mathcal{S}_{-1}$.

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

6. Non-tame quotient curves of the Suzuki curve. In this section we investigate quotient curves of the Suzuki curve $\mathcal{S}$ arising from the non-tame subgroups of $\mathrm{Aut}(\mathcal{S})$. 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 relevant natural morphism and thus the genus of such curves; in several cases we will also provide plane models.

From Section 2, the subgroups of $\mathcal{S}z(q)$ of even order are of the following types, up to conjugacy in $\mathcal{S}z(q)$:

I. Subgroups of $\widetilde{\mathbf{T}}$;
II. Subgroups of order $2^v r$ with $v > 1$ and $r > 1$ 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 divisor of $q \pm 2q_0 + 1$;
VI. Subgroups isomorphic to $\mathcal{S}z(\overline{q})$.

Type I. Let $\mathcal{U}$ be a subgroup of $\widetilde{\mathbf{T}}$. We shall compute the genus $\widetilde{g}$ of the quotient curve $\widetilde{\mathcal{S}} = \mathcal{S}/\mathcal{U}$, by considering the subgroup $\mathcal{U}_2$ of $\mathcal{U}$ 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 $2^u := \#\mathcal{U}_2$ and $2^v := \#\mathcal{U}$. Recall that $q = 2q_0^2$ and $q_0 = 2^s$, $s \in \mathbb{N}$.

THEOREM 6.1. *With the notation above*,

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

in particular, $u \le 2s+1$ *and* $v - u \le s$.

Proof. The Riemann–Hurwitz formula asserts that

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

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

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

We see that $\mathbf{T} \ne 1$ is an element of order 2 for $a = 0$, otherwise its order is 4. Thus the Riemann–Hurwitz formula above becomes

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

and we obtain the formula for $\widetilde{g}$. The numerical conditions follow from the fact that $\widetilde{g}$ 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 $\widetilde{\mathbf{T}}$ in terms of their elements of order 2. Such a general problem is computationally beyond our reach, because $\widetilde{\mathbf{T}}$ 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 $\mathcal{U}$ be a subgroup of $\widetilde{\mathbf{T}}$ and $\mathcal{U}_2$ the subgroup of its elements of even order. Let 2^v and 2^u be the orders of $\mathcal{U}$ and $\mathcal{U}_2$ respectively. Then*:

(1) $v \le 2u$.
(2) *For every integer u' with $u \le u' \le v$ there is a subgroup of $\mathcal{U}$ of order $2^{u'}$ containing $\mathcal{U}_2$. In particular, for each integer u' with $2s+1 \le u' \le 4s+2$, there is a subgroup of $\widetilde{\mathbf{T}}$ of order $2^{u'}$ containing all elements of $\widetilde{\mathbf{T}}$ of order 2.*

Proof. (1) We consider the homomorphism of groups

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

where K is equipped with its additive structure. We have $\mathrm{Ker}(\Phi) = \mathcal{U}_2$ and thus $\mathcal{U}/\mathcal{U}_2$ is isomorphic to $\Phi(\mathcal{U})$. As the map $K \to K$, $a \mapsto a^{2q_0+1}$, is injective, and as $\mathbf{T}_{a,c}^2 = \mathbf{T}_{0,a^{2q_0+1}}$, we have $\#\Phi(\mathcal{U}) \le \#\mathcal{U}_2$ and hence the assertion.

(2) Since the quotient $\mathcal{U}/\mathcal{U}_2$ is an elementary abelian group, the converse of the Lagrange theorem holds and the first statement follows; for the second statement take $\mathcal{U} = \widetilde{\mathbf{T}}$; cf. (2.3). ∎

Sufficient conditions for the existence of a subgroup $\mathcal{U}$ of $\widetilde{\mathbf{T}}$ with a given subgroup $\mathcal{U}_2$ is ensured by the following lemma. Let $\Phi_{\mathcal{U}}$ be the map defined in the proof of Lemma 6.2.

LEMMA 6.3.

(1) *Let $\mathcal{V}$ be an elementary abelian group of $\widetilde{\mathbf{T}}$ of order 2^u. Then there exists a subgroup $\mathcal{U}$ of $\widetilde{\mathbf{T}}$ of order 2^{u+1} such that $\mathcal{U}_2$ coincides with $\mathcal{V}$.*

(2) *Let $v \ge u \ge 0$ be integers, and $\mathcal{B}$ an additive subgroup of K of order 2^u. If there exists an additive subgroup $\mathcal{A}$ of K of order 2^{v-u} such that $\mathcal{A}^{2q_0+1} \subseteq \mathcal{B}$, then there exists a subgroup $\mathcal{U}$ of $\widetilde{\mathbf{T}}$ of order 2^v such that $\Phi_{\mathcal{U}}(\mathcal{U}) = \mathcal{A}$ and $\mathrm{Ker}(\Phi_{\mathcal{U}}) = \{\mathbf{T}_{0,c} : c \in \mathcal{B}\}$ (in particular, $\mathrm{ord}(\mathcal{U}_2) = 2^u$).*

Proof. (1) Since the normalizer in $\mathrm{Aut}(\mathcal{S})$ of $\widetilde{\mathbf{T}}$ acts transitively on the set of elements of order 2 of $\widetilde{\mathbf{T}}$ (cf. (2.3)) we may assume $\mathbf{T}_{0,1} \notin \mathcal{V}$. Then the group $\mathcal{U}$ generated by $\mathcal{V}$ and $\mathbf{T}_{0,1}$ fulfills the required conditions.

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

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

center $Z(\widetilde{\mathbf{T}})$ (cf. (2.3)) we have

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

Finally, $\Phi_{\mathcal{U}}(\mathbf{T}\circ\mathbf{T}_0) = \Phi_{\mathcal{U}}(\mathbf{T}) + \Phi_{\mathcal{U}}(\mathbf{T}_0) = a + a_0$ implies $\Phi_{\mathcal{U}}(\mathcal{U}) = \mathcal{A}$ and $\mathrm{Ker}(\Phi_{\mathcal{U}}) \subseteq \mathrm{Ker}(\Phi_{\mathcal{U}_0})$, 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 $\mathcal{V} = \{\mathbf{T}_{0,0}, \mathbf{T}_{0,1}, \mathbf{T}_{0,e}, \mathbf{T}_{0,e+1}\}$ is an elementary abelian subgroup of $\widetilde{\mathbf{T}}$ of order 2^v with $v = 2$. Assume that there is a subgroup $\mathcal{U}$ of $\widetilde{\mathbf{T}}$ of order 2^4 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 $\mathbf{T}_{a_i,c_i}$ $(i = 1, 2, 3)$ together with $\mathbf{T}_{0,0}$ 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 $\mathbf{T}_{a_i,c_i}^2 = T_{0,a_i^{2q_0+1}}$. Then $(*)$ implies $a_3^{2q_0} + a_3 = 0$, a contradiction.

COROLLARY 6.5. *Let $v \ge u \ge 0$ be integers such that $v-u \le s$, $u \le 2s+1$ and $v \le 2u$. Then there exists a non-tame quotient curve of $\mathcal{S}$ whose genus is given by Theorem* 6.1 *provided that*

$$v - u \le \log_2(u+1) \quad \text{or} \quad (v-u) \,|\, (2s+1). \tag{6.1}$$

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

Now suppose that $(v - u) \,|\, (2s + 1)$ and $v \le 2u$. Then $\mathbb{F}_{2^{v-u}}$ is a subfield of K. Let $\mathcal{B}$ be any additive subgroup of order 2^u containing the additive group $\mathcal{A}$ of $\mathbb{F}_{2^{v-u}}$. Again Lemma 6.3(2) proves the assertion. ∎

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

THEOREM 6.6. *With the notation above*:

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

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

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

$$\sum_{i=0}^{2s} V^{2^i} = \sum_{i=0}^{2s} U^{2^i} + \sum_{i=0}^{s} \Big(\sum_{j=i}^{s} U^{2^j} \Big) U^{2^i} + \sum_{i=s+2}^{2s} \Big(\sum_{j=0}^{i-s-2} U^{2^j} \Big)^{2q_0} U^{2^i}.$$

Proof. (1) We have $\mathcal{U} = \mathcal{U}_2$ and the formula for the genus follows from Theorem 6.1. We now consider the morphism $\phi := (1 : x : z^{\widetilde{q}} + z) : \mathcal{S} \to \mathbb{P}^2$; then $\widetilde{\mathcal{S}}$ is the non-singular model over K of $\phi(\mathcal{S})$ since $\phi^{-1}(\phi(P_{(a,c)})) = \{P_{(a,c+e)} : e \in \mathbb{F}_{\widetilde{q}}\}$. To write a plane equation for $\phi(\mathcal{S})$ we use (3.5) with $U := x$ and $V := z^{\widetilde{q}} + z$ taking into account that $z^q + z = (z^{\widetilde{q}} + z) + (z^{\widetilde{q}} + z)^{\widetilde{q}} + \cdots + (z^{\widetilde{q}} + z)^{\widetilde{q}^{n-1}}$.

(2) Since the cyclic subgroups of $\mathrm{Aut}(\mathcal{S})$ of order 4 are pairwise conjugate in $\mathrm{Aut}(\mathcal{S})$ (cf. (2.4)), we may assume $\mathcal{U}$ to be generated by $\mathbf{T}_{1,0}$. Here $\mathcal{U}_2$ has two elements and the formula for $\widetilde{g}$ follows from Theorem 6.1. We now consider the morphism $\phi := (1 : x^2 + x : x^3 + x + z^2 + z) : \mathcal{S} \to \mathbb{P}^2$. Then $\widetilde{\mathcal{S}}$ is the non-singular model over K of $\phi(\mathcal{S})$ since $\phi^{-1}(\phi(P_{(a,c)})) = \{\mathbf{T}_{1,0}^i : i = 1, \ldots, 4\}$. To write a plane equation for $\phi(\mathcal{S})$ we notice that

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

therefore, with $U := x^2 + x$ and $V := x^3 + x + z^2 + z$, by the equalities (3.5), $x^q + x = \sum_{i=0}^{2s} (x^2 + x)^{2^i}$ and $x^3 + x = (x^2 + x) + (x^3 + x^2)$,

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

Now the claimed equation follows from the relations

$$x^{2^i} + x^{2q_0} = \begin{cases} \sum_{j=i}^{s} (x^2 + x)^{2^j} & \text{if } i < s+1, \\ 0 & \text{if } i = s+1, \\ (\sum_{j=0}^{i-s-2} (x^2 + x)^{2^j})^{2q_0} & \text{if } i > s+1. \end{cases}$$ ∎

Type II. The basic fact here is that, up to conjugacy in $\mathrm{Aut}(\mathcal{S})$, a subgroup $\mathcal{U}$ of $\mathrm{Aut}(\mathcal{S})$ of order $2^v r$ $(v, r > 1,\ r \mid (q-1))$ is contained in $\widetilde{\mathbf{T}}\widetilde{\mathbf{N}}$; moreover, the orders of its elements are known (cf. (2.5)).

THEOREM 6.7. *For a subgroup* $\mathcal{U}$ *of* $\widetilde{\mathbf{T}}\widetilde{\mathbf{N}}$ *of order* $2^v r$ *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*

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

in particular, $u \le 2s+1$, $v - u \le s$ *and* r *divides* $q/2^u - 1$.

Proof. The Riemann–Hurwitz genus formula states

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

where R is the ramification divisor of the natural morphism $\mathcal{S} \to \widetilde{\mathcal{S}}$. We have to look at the points $P \in \mathcal{S}$ for which there exists $\mathbf{T} \in \mathcal{U}$ with $\mathbf{T}(P) = P$, and compute $i_{\mathbf{T},P} = v_P(\mathbf{T}^*(\ell) - \ell)$, ℓ 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,

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

where the summation is extended over all the automorphisms $\mathbf{T} \in \mathcal{U} \setminus \widetilde{\mathbf{T}}$ such that $\mathbf{T}(A_4) = A_4$; from (4.2) we obtain $i_{\mathbf{T},A_4} = 2$ and the formula for $\widetilde{g}$ follows. The numerical conditions follow from the fact that $\widetilde{g}$ 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 is a divisor of $q - 1$ and $q/2^u - 1$. 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. This follows from 6.3(2) and the structure of $\widetilde{\mathbf{T}}\widetilde{\mathbf{N}}$. ∎

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

THEOREM 6.9. *Let $\mathcal{U}$ be a subgroup of $\mathrm{Aut}(\mathcal{S})$ of order $2r$ with $r > 1$ a divisor of $q - 1$. Then the quotient curve $\widetilde{\mathcal{S}} = \mathcal{S}/\mathcal{U}$ has genus*

$$\widetilde{g} = \frac{q_0}{2}\left(\frac{q-1}{r} - 1\right),$$

and a plane model over K of $\widetilde{\mathcal{S}}$ is given by

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

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 $N_{\mathrm{Aut}(\mathcal{S})}(\widetilde{\mathbf{N}})$ is a dihedral group of order $2(q-1)$ which comprises $\widetilde{\mathbf{N}}$ 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 $\mathcal{S} \to \widetilde{\mathcal{S}}$ is $(2q_0+2)r + 2(r-1)$ and the result follows from the Riemann–Hurwitz genus formula.

A plane model: Let $\psi := \widetilde{\phi} \circ \phi : \mathcal{S} \to \mathbb{P}^2$, where ϕ is the morphism defined in Section 4 and $\widetilde{\phi}$ is the morphism on $\phi(\mathcal{S})$ defined by $(X : 1 : Z) \mapsto (1 : XZ : X^r + Z^r)$. We claim that $\widetilde{\mathcal{S}}$ is the non-singular model over K of $\psi(\mathcal{S})$. Since ϕ is birational (see Lemma 4.5), to prove this claim it is enough to check that $\#\widetilde{\phi}^{-1}(\widetilde{\phi}(P)) = 2r$ for a (generic) point $P = (a : 1 : c) \in \phi(\mathcal{C})$. We have $(a\tau^{-i} : 1 : c\tau^i), (c\tau^i : 1 : a\tau^{-i}) \in \widetilde{\phi}^{-1}(\widetilde{\phi}(P))$ $(i = 1, \dots, r)$, where τ is an element of order r in K^*. On the other hand, let $P' = (\widetilde{a} : 1 : \widetilde{c})$ be such that $\widetilde{\phi}(P') = \widetilde{\phi}(P)$. Then $\widetilde{a}^r$ and $\widetilde{c}^r$ are the roots of $W^2 + (a^r + c^r)W + a^r c^r = 0$ and hence the claim is proved.

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

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

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

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

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

Type IV. We use the fact that each subgroup of $\mathrm{Aut}(\mathcal{S})$ of order $2r$ with $r > 1$ and $r \mid (q \pm 2q_0 + 1)$ is conjugate under $\mathrm{Aut}(\mathcal{S})$ to a subgroup of the dihedral subgroup of $\mathrm{Aut}(\mathcal{S})$ which comprises the Singer subgroups $\mathcal{S}_{\pm 1}$ 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 $\mathrm{Aut}(\mathcal{S})$ of order $2r$.*

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

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

Furthermore, a plane model over $\mathbb{F}_{q^4}$ of $\widetilde{\mathcal{S}}$ is given by

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

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

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

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

Furthermore, a plane model over $\mathbb{F}_{q^4}$ of $\widetilde{\mathcal{S}}$ is given by

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

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

Proof. The genus: The subgroup $\mathcal{U}$ has $r-1$ non-trivial elements of odd order and r of even order; thus the degree of the ramification divisor is $(2q_0+2)r + \widetilde{R}$ (cf. proof of Theorem 6.1). By (4.2), in case (1) we obtain $\widetilde{R} = 0$ and in case (2), $\widetilde{R} = 4(r-1)$. 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 case (1), the corresponding morphism ϕ is taken to be the one defined in Section 5; we use the plane model of $\mathcal{S}$ in Lemma 5.5 written as

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

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

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

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

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

Proof. The subgroup $\mathcal{U}$ 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 $\mathcal{S} \to \widetilde{\mathcal{S}}$ is $(2q_0+2)r + (2r)2 + \widetilde{R}$, where $\widetilde{R} = 0$ if $r \mid (q+2q_0+1)$ and $\widetilde{R} = 4(r-1)$ if $r \mid (q-2q_0+1)$. Now the assertion follows by the Riemann–Hurwitz genus formula. ∎

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

THEOREM 6.12. *With the notation above, the genus of* $\widetilde{\mathcal{S}} = \mathcal{S}/\mathcal{U}$ *is given by*

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

where

$$\begin{aligned}\Delta := {} & (\widetilde{q}^2+1)[(2q_0+2)(\widetilde{q}-1) + 2\widetilde{q}(\widetilde{q}-1)] + \widetilde{q}^2(\widetilde{q}^2+1)(\widetilde{q}-2) \\ & + \widetilde{q}^2(\widetilde{q}+2\widetilde{q}_0+1)(\widetilde{q}-1)(\widetilde{q}-2\widetilde{q}_0).\end{aligned}$$

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

$$\begin{aligned}(\overline{q}^2+1)[(2q_0+2)(\overline{q}-1) + 2\overline{q}(\overline{q}-1)] + \overline{q}^2(\overline{q}^2+1)(\overline{q}-2) \\ + \overline{q}^2(\overline{q}+2\overline{q}_0+1)(\overline{q}-1)(\overline{q}-2\overline{q}_0),\end{aligned}$$

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 [8] and [9].

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 a 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,

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

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 of three numbers: Serre's bound, Ihara's bound (cf. [9, p. 1]), and 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 $q = 2q_0^2$, and the genus $g = \widetilde{g}$ of a quotient curve $\widetilde{\mathcal{S}}$ of the Suzuki curve $\mathcal{S}$. Note that by (3.1), $\#\widetilde{\mathcal{S}}(K) = q + 2q_0\widetilde{g} + 1 \ge \lfloor b/\sqrt{2} \rfloor$; thus we might expect

"many" K-rational points on the curve $\widetilde{\mathcal{S}}$ (this is the case when $q \leq 128$ and $\widetilde{g} \leq 50$ according to [9, Sect. 1]). We only consider the cases $q_0 = 2$, $q_0 = 4$, $q_0 = 8$, $\widetilde{g} \leq 50$ so 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 [9]; we remark that the tables are updated periodically.

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

Reference	Cor. 6.5	Thm. 4.1	Cor. 6.5	Cor. 6.5	Cor. 6.5
$\widetilde{g}$	1	2	3	6	14
$N_8(\widetilde{g})$	14	18	24	33–35	65
$\#\widetilde{\mathcal{S}}(K)$	13	17	21	**33**	**65**

The curve of genus 2 almost attains $N_8(2)$; it is given by

$$V^2 + V = \frac{(1+U)^4 U^7}{f(U)^2},$$

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 $N_8(2)$. However, this appears to be out of reach. The cases $\widetilde{g} = 6, 14$ were already noticed by Stichtenoth [30, p. 205].

2. $q_0 = 4$. Here $\#\widetilde{\mathcal{S}}(K) = 33 + 8\widetilde{g}$. We have the following data:

Reference	$\widetilde{g}$	$N_{32}(\widetilde{g})$	$\#\widetilde{\mathcal{S}}(K)$
Cor. 6.5	1	44	41
Cor. 6.5	2	53	49
Cor. 6.5	3	64	57
Thm. 4.1	4	71–75	65
Thm. 6.11	5	83–86	73
Cor. 6.5	6	86–97	81
Thm. 6.10(2)	10	...	**113**
Cor. 6.5	12	129–163	**129**
Cor. 6.5	14	146–185	145
Thm. 5.1(2)	24	...	**225**
Cor. 6.5	28	257–298	**257**
Cor. 6.5	30	273–313	**273**

We have $113 \leq N_{32}(10) \leq 143$, where the upper bound is obtained from Serre's bound. The equation of $\widetilde{\mathcal{S}}$ 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 $\lambda \in \mathbb{F}_{32^4}$ of order 25, and $f(V) = 1 + V^2(1+V) + V^9(1+V)^2$. The cases $\widetilde{g} = 12$, $\widetilde{g} = 28$ and $\widetilde{g} = 30$ were already noticed by van der Geer and van der Vlugt [11] via fiber products of certain Artin–Schreier curves. We do not know if such curves are isomorphic to the corresponding quotient curves $\widetilde{\mathcal{S}}$ here. The curve of genus $\widetilde{g} = 14$ almost attains $N_{32}(14)$. We have $225 \le N_{32}(24) \le 245$, where the upper bound is obtained from Ihara's bound; a plane model of $\widetilde{\mathcal{S}}$ is given by

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

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

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

Reference	$\widetilde{g}$	$N_{128}(\widetilde{g})$	$\#\widetilde{\mathcal{S}}(K)$
Cor. 6.5	1	150	145
Cor. 6.5	2	172	161
Cor. 6.5	3	192	177
Cor. 6.5	4	215–217	193
Cor. 6.5	6	243–261	225
Thm. 6.11	7	258–283	241
Cor. 6.5	8	257–305	**257**
Cor. 6.5	12	321–393	**321**
Thm. 6.10(1)	14	353–437	**353**
Thm. 5.1(2)	24	513–657	**513**
Cor. 6.5	28	577–745	**577**
Cor. 6.5	30	609–789	**609**
Thm. 5.1(1)	36	...	**705**
Thm. 6.11	49	...	**913**

For $\widetilde{g} = 8$, the existence of a curve with 257 K-rational points was pointed out by Wirtz [34]. We find that $\widetilde{\mathcal{S}}$ is hyperelliptic and it is defined by (cf. Remark 4.7)

$$V^2 + V = \frac{(1+U)^{16}U^{127}}{f(U)^2},$$

where $f(U) = 1 + U^8(1+U) + U^{25}(1+U)^2 + U^{59}(1+U)^4$. We do not know whether $\widetilde{\mathcal{S}}$ is isomorphic to Wirtz's curve. For $\widetilde{g} = 12, 14, 24, 28, 30$, 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 $\widetilde{\mathcal{S}}$. Furthermore, $705 \le N_{128}(36) \le 921$; here the upper bound follows from Serre's bound. A plane equation for $\widetilde{\mathcal{S}}$ is

given by

$$V^5\widetilde{f}(U) = U^{145} + V^{10},$$

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

Acknowledgements. 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

[1] Y. Aubry and M. Perret, *Divisibility of zeta functions of curves in a covering*, Arch. Math. (Basel) 82 (2004), 205–213.

[2] E. Çakçak and F. Özbudak, *Subfields of the function field of the Deligne–Lusztig curve of Ree type*, Acta Arith. 115 (2004), 133–180.

[3] A. Cossidente, G. Korchmáros and F. Torres, *On curves covered by the Hermitian curve*, J. Algebra 216 (1999), 56–76.

[4] —, —, —, *Curves of large genus covered by the Hermitian curve*, Comm. Algebra 28 (2000), 4707–4728.

[5] P. Deligne and G. Lusztig, *Representations of reductive groups over finite fields*, Ann. of Math. 103 (1976), 103–161.

[6] R. Fuhrmann and F. Torres, *On Weierstrass points and optimal curves*, Rend. Circ. Mat. Palermo. Suppl. 51 (1998), 25–46.

[7] A. Garcia, H. Stichtenoth and C. P. Xing, *On subfields of the Hermitian function field*, Compos. Math. 120 (2000), 137–170.

[8] G. van der Geer, *Error-correcting codes and curves over finite fields*, in: Mathematics Unlimited–2001 and Beyond, B. Engquist and W. Schmid (eds.), Springer, 2001, 1115–1138.

[9] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, February 29, 2004; http://www.wins.uva.nl/~geer.

[10] —, —, *Quadratic forms, generalized Hamming weights of codes and curves with many points*, J. Number Theory 59 (1996), 20–36.

[11] —, —, *Curves over finite fields of characteristic* 2 *with many rational points*, C. R. Acad. Sci. Paris Sér. I 317 (1993), 593–597.

[12] V. D. Goppa, *Geometry and Codes*, Math. Appl. 24, Kluwer, Dordrecht, 1988.

[13] D. Gorenstein, *Finite Groups*, Chelsea, New York, 1980.

[14] J. P. Hansen, *Deligne–Lusztig varieties and group codes*, in: Lecture Notes in Math. 1518, Springer, 1992, 63–81.

[15] J. P. Hansen and J. P. Pedersen, *Automorphism groups of Ree type, Deligne–Lusztig curves and function fields*, J. Reine Angew. Math. 440 (1993), 99–109.

[16] J. P. Hansen and H. Stichtenoth, *Group codes on certain algebraic curves with many rational points*, Appl. Algebra Engrg. Comm. Comput. 1 (1990), 67–77.

[17] R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math. 52, Springer, New York, 1977.
[18] H. W. Henn, *Funktionenkörper mit großer Automorphismengruppe*, J. Reine Angew. Math. 302 (1978), 96–115.
[19] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, 2nd ed., Oxford Univ. Press, Oxford, 1998.
[20] B. Huppert and N. Blackburn, *Finite Groups III*, Springer, 1982.
[21] G. Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C. R. Acad. Sci. Paris Sér. I 305 (1987), 729–732.
[22] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1987.
[23] H. Lüneburg, *Translation Planes*, Springer, 1980.
[24] G. L. Matthews, *Codes from the Suzuki function field*, IEEE Trans. Inform. Theory 50 (2004), 3298–3302.
[25] C. J. Moreno, *Algebraic Curves over Finite Fields*, Cambridge Tracts in Math. 97, Cambridge Univ. Press, 1991.
[26] D. Mumford, *Abelian Varieties*, Tata Inst. Fund. Res. Stud. Math. 5, Oxford Univ. Press, Bombay, 1994.
[27] J. P. Pedersen, *A function field related to the Ree group*, in: Lecture Notes in Math. 1518, Springer, 1992, 122–131.
[28] H. G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. 457 (1994), 185–188.
[29] J. P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér I 296 (1983), 397–402.
[30] H. Stichtenoth, *Algebraic-geometric codes associated to Artin–Schreier extensions of* $\mathbb{F}_q(z)$, in: Proc. 2nd Int. Workshop on Alg. and Comb. Coding Theory, Leningrad, 1990, 203–206.
[31] —, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.
[32] K. O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) 52 (1986), 1–19.
[33] J. Tits, *Ovoïdes et groupes de Suzuki*, Arch. Math. (Basel) 13 (1962), 187–198.
[34] M. Wirtz, *Konstruktion und Tabellen linearer Codes*, Westfälische Wilhelms-Univ. Münster, 1991.

Dipartimento di Matematica e Informatica
Università di Perugia
06123 Perugia, Italy
E-mail: giuliet@dipmat.unipg.it

Dipartimento di Matematica
Università della Basilicata
Campus Universitario Contrada Macchia Romana
85100 Potenza, Italy
E-mail: korchmaros@unibas.it

IMECC-UNICAMP
Cx.P. 6065
13083-970, Campinas SP, Brazil
E-mail: ftorres@ime.unicamp.br

Received on 8.6.2005
and in revised form on 6.2.2006 (4999)