HYPERELLIPTIC JACOBIANS AND $U_3(2^m)$

YURI G. ZARHIN

1. Introduction

In [12] the author proved that in characteristic 0 the jacobian $J(C) = J(C_f)$ of a hyperelliptic curve

$$C = C_f : y^2 = f(x)$$

has only trivial endomorphisms over an algebraic closure $K_a$ of the ground field $K$ if the Galois group $\text{Gal}(f)$ of the irreducible polynomial $f \in K[x]$ is “very big”. Namely, if $n = \deg(f) \geq 5$ and $\text{Gal}(f)$ is either the symmetric group $S_n$ or the alternating group $A_n$ then the ring $\text{End}(J(C_f))$ of $K_a$-endomorphisms of $J(C_f)$ coincides with $\mathbb{Z}$. Later the author [13] proved that $\text{End}(J(C_f)) = \mathbb{Z}$ for an infinite series of $\text{Gal}(f) = \text{PSL}_2(F_{2^r})$ and $n = 2^r + 1$ (with $\dim(J(C_f)) = 2^{r-1}$) or when $\text{Gal}(f)$ is the Suzuki group $\text{Sz}(2^{2r+1})$ and $n = 2^{2(2r+1)+1}$ (with $\dim(J(C_f)) = 2^{4r+1}$). We refer the reader to [9], [10], [6], [7], [12], [13], [14] for a discussion of known results about, and examples of, hyperelliptic jacobians withot complex multiplication.

We write $\mathfrak{R} = \mathfrak{R}_f$ for the set of roots of $f$ and consider $\text{Gal}(f)$ as the corresponding permutation group of $\mathfrak{R}$. Suppose $q = 2^m > 2$ is an integral power of 2 and $F_{q^2}$ is a finite field consisting of $q^2$ elements. Let us consider a non-degenerate Hermitian (wrt $x \mapsto x^q$) sesquilinear form on $F_{q^2}^3$. In the present paper we prove that $\text{End}(J(C_f)) = \mathbb{Z}$ when $\mathfrak{R}_f$ can be identified with the corresponding “Hermitian curve” of isotropic lines in the projective plane $\mathbb{P}^2(F_{q^2})$ in such a way that $\text{Gal}(f)$, becomes either the projective unitary group $\text{PGU}_3(F_{q^2})$ or the projective special unitary group $U_3(q) := \text{PSU}_3(F_q)$. In this case $n = \deg(f) = q^3 + 1 = 2^{3m} + 1$ and $\dim(J(C_f)) = q^3/2 = 2^{3m-1}$.

Our proof is based on an observation that the Steinberg representation is the only absolutely irreducible nontrivial representation (up to an isomorphism) over $F_2$ of $U_3(2^m)$, whose dimension is a power of 2.

2. Main results

Throughout this paper we assume that $K$ is a field with $\text{char}(K) \neq 2$. We fix its algebraic closure $K_a$ and write $\text{Gal}(K)$ for the absolute Galois group $\text{Aut}(K_a/K)$. If $X$ is an abelian variety defined over $K$ then we write $\text{End}(X)$ for the ring of $K_a$-endomorphisms of $X$.

Suppose $f(x) \in K[x]$ is a separable polynomial of degree $n \geq 5$. Let $\mathfrak{R} = \mathfrak{R}_f \subset K_a$ be the set of roots of $f$, let $K(\mathfrak{R}_f) = K(\mathfrak{R})$ be the splitting field of $f$ and $\text{Gal}(f) := \text{Gal}(K(\mathfrak{R})/K)$ the Galois group of $f$, viewed as a subgroup of $\text{Perm}(\mathfrak{R})$. Let $C_f$ be the hyperelliptic curve $y^2 = f(x)$. Let $J(C_f)$ be its jacobian, $\text{End}(J(C_f))$ the ring of $K_a$-endomorphisms of $J(C_f)$.

Partially supported by NSF grant DMS-0070664.
Theorem 2.1. Assume that there exist a positive integer \( m > 1 \) such that \( n = 2^{3m+1} + 1 \) and \( \text{Gal}(f) \) contains a subgroup isomorphic to \( \text{U}_3(2^m) \). Then either \( \text{End}(J(C_f)) = \mathbb{Z} \) or \( \text{char}(K) > 0 \) and \( J(C_f) \) is a supersingular abelian variety.

We will prove Theorems 2.1 in §5.

3. Permutation groups, permutation modules and very simplicity

Let \( B \) be a finite set consisting of \( n \geq 5 \) elements. We write \( \text{Perm}(B) \) for the group of permutations of \( B \). A choice of ordering on \( B \) gives rise to an isomorphism \( \text{Perm}(B) \cong S_n \).

Let \( G \) be a subgroup of \( \text{Perm}(B) \). For each \( b \in B \) we write \( G_b \) for the stabilizer of \( b \) in \( G \); it is a subgroup of \( G \). Further we always assume that \( n \) is odd.

Remark 3.1. Assume that the action of \( G \) on \( B \) is transitive. It is well-known that each \( G_b \) is of index \( n \) in \( G \) and all the \( G_b \)'s are conjugate in \( G \). Each conjugate of \( G_b \) in \( G \) is the stabilizer of a point of \( B \). In addition, one may identify the \( G \)-set \( B \) with the set of cosets \( G/G_b \) with the standard action by \( G \).

We write \( \mathbb{F}_2^B \) for the \( n \)-dimensional \( \mathbb{F}_2 \)-vector space of maps \( h : B \to \mathbb{F}_2 \). The space \( \mathbb{F}_2^B \) is provided with a natural action of \( \text{Perm}(B) \) defined as follows. Each \( s \in \text{Perm}(B) \) sends a map \( h : B \to \mathbb{F}_2 \) into \( sh : b \mapsto h(s^{-1}(b)) \). The permutation module \( \mathbb{F}_2^B \) contains the \( \text{Perm}(B) \)-stable hyperplane \( Q_B := \{ h : B \to \mathbb{F}_2 \mid \sum_{b \in B} h(b) = 0 \} \) and the \( \text{Perm}(B) \)-invariant line \( \mathbf{1}_B \) where \( \mathbf{1}_B \) is the constant function 1. Since \( n \) is odd, there is a \( \text{Perm}(B) \)-invariant splitting \( \mathbb{F}_2^B = Q_B \oplus \mathbb{F}_2 \cdot \mathbf{1}_B \).

Clearly, \( \dim_{\mathbb{F}_2}(Q_B) = n - 1 \) and \( \mathbb{F}_2^B \) and \( Q_B \) carry natural structures of \( G \)-modules. Clearly, \( Q_B \) is a faithful \( G \)-module. It is also clear that the \( G \)-module \( Q_B \) can be viewed as the reduction modulo 2 of the \( \mathbb{Q}[G] \)-module \( (Q_B)^0 := \{ h : B \to \mathbb{Q} \mid \sum_{b \in B} h(b) = 0 \} \).

It is well-known that the \( \mathbb{Q}[G] \)-module \( (Q_B)^0 \) is absolutely simple if and only if the action of \( G \) on \( B \) is doubly transitive ([11], Sect. 2.3, Ex. 2).

Remark 3.2. Assume that \( G \) acts on \( B \) doubly transitively and \( #(B) - 1 = \dim_{\mathbb{Q}}((Q_B)^0) \) coincides with the largest power of 2 dividing \( #(G) \). Then it follows from a theorem of Brauer-Nesbitt ([11], Sect. 16.4, pp. 136–137; [4], p. 249) that \( Q_B \) is an absolutely simple \( \mathbb{F}_2[G] \)-module. In particular, \( Q_B \) is (the reduction of) the Steinberg representation \([4],[2]\).

We refer to [13] for a discussion of the following definition.
Definition 3.3. Let $V$ be a vector space over a field $F$, let $G$ be a group and
\( \rho : G \to \text{Aut}_F(V) \) a linear representation of $G$ in $V$. We say that the $G$-module $V$ is very simple if it enjoys the following property:

If $R \subseteq \text{End}_F(V)$ is an $F$-subalgebra containing the identity operator $\text{Id}$ such that

\[
 \rho(\sigma)R\rho(\sigma)^{-1} \subseteq R \quad \forall \sigma \in G
\]

then either $R = F \cdot \text{Id}$ or $R = \text{End}_F(V)$.

Remarks 3.4. (i) If $G'$ is a subgroup of $G$ and the $G'$-module $V$ is very simple then obviously the $G$-module $V$ is also very simple.
(ii) A very simple module is absolutely simple (see [13], Remark 2.2(ii)).
(iii) If $\dim_F(V) = 1$ then obviously the $G$-module $V$ is very simple.
(iv) Assume that the $G$-module $V$ is very simple and $\dim_F(V) > 1$. Then $V$ is not induced from a subgroup $G$ (except $G$ itself) and is not isomorphic to a tensor product of two $G$-modules, whose $F$-dimension is strictly less than $\dim_F(V)$ (see [13], Examples 7.1).
(v) If $F = F_2$ and $G$ is perfect then properties (ii)-(iv) characterize the very simple $G$-modules (see [13], Th. 7.7).

The following statement provides a criterion of very simplicity over $F_2$.

Theorem 3.5. Suppose a positive integer $N > 1$ and a group $H$ enjoy the following properties:

- $H$ does not contain a subgroup of index dividing $N$ except $H$ itself.
- Let $N = ab$ be a factorization of $N$ into a product of two positive integers $a > 1$ and $b > 1$. Then either there does not exist an absolutely simple $F_2[H]$-module of $F_2$-dimension $a$ or there does not exist an absolutely simple $F_2[H]$-module of $F_2$-dimension $b$.

Then each absolutely simple $F_2[H]$-module of $F_2$-dimension $N$ is very simple.

Proof. This is Corollary 4.12 of [12].

4. Steinberg representation

We refer to [11] and [2] for a definition and basic properties of Steinberg representations.

Let us fix an algebraic closure of $F_2$ and denote it by $\mathcal{F}$. We write $\phi : \mathcal{F} \to \mathcal{F}$ for the Frobenius automorphism $x \mapsto x^2$. Let $q = 2^m$ be a positive integral power of two. Then the subfield of invariants of $\phi^m : \mathcal{F} \to \mathcal{F}$ is a finite field $F_q$ consisting of $q$ elements. Let $q'$ be an integral positive power of $q$. If $d$ is a positive integer and $i$ is a non-negative integer then for each matrix $u \in \text{GL}_d(\mathcal{F})$ we write $u^{(i)}$ for the matrix obtained by raising each entry of $u$ to the $2^i$-th power.

Remark 4.1. Recall that an element $\alpha \in F_q$ is called primitive if $\alpha \neq 0$ and has multiplicative order $q - 1$ in the cyclic multiplicative group $F_q^*$.

Let $M < q - 1$ be a positive integer. Clearly, the set

\[
 \mu_M(F_q) = \{ \alpha \in F_q \mid \alpha^M = 1 \}
\]

is a cyclic multiplicative subgroup of $F_q^*$ and its order $M'$ divides both $M$ and $q - 1$. Since $M < q - 1$ and $q - 1$ is odd, the ratio $(q - 1)/M'$ is an odd integer $> 1$. This implies that $3 \leq (q - 1)/M'$ and therefore

\[
 M' = \#(\mu_M(F_q)) \leq (q - 1)/3.
\]
Lemma 4.2. Let \( q > 2 \), let \( d \) be a positive integer and let \( G \) be a subgroup of \( \text{GL}_d(\mathbb{F}_q') \). Assume that one of the following two conditions holds:

(i) There exists an element \( u \in G \subseteq \text{GL}_d(\mathbb{F}_q') \), whose trace \( \alpha \) lies in \( \mathbb{F}_q^* \) and has multiplicative order \( q - 1 \);

(ii) There exist a positive integer \( r > \frac{q-1}{2} \), distinct \( \alpha_1, \cdots, \alpha_r \in \mathbb{F}_q^* \) and elements

\[
\alpha_1, \cdots, \alpha_r \in G \subseteq \text{GL}_d(\mathbb{F}_q')
\]

such that the trace of \( \alpha_i \) for all \( i = 1, \cdots, r \).

Let \( V_0 = \mathcal{F}^d \) and \( \rho_0 : G \subseteq \text{GL}_d(\mathbb{F}_q') \subseteq \text{GL}_d(\mathcal{F}) = \text{Aut}_\mathcal{F}(V_0) \) be the natural \( d \)-dimensional representation of \( G \) over \( \mathcal{F} \). For each positive integer \( i < m \) we define a \( d \)-dimensional \( \mathcal{F} \)-representation

\[
\rho_i : G \to \text{Aut}(V_i)
\]

as the composition of

\[
G \mapsto \text{GL}_d(\mathbb{F}_q'), \quad x \mapsto x^{(i)}
\]

and the inclusion map

\[
\text{GL}_d(\mathbb{F}_q') \subseteq \text{GL}_d(\mathcal{F}) \cong \text{Aut}_\mathcal{F}(V_i).
\]

Let \( S \) be a subset of \( \{0, 1, \ldots, m-1\} \). Let us define a \( d\#(S) \)-dimensional \( \mathcal{F} \)-representation \( \rho_S \) of \( G \) as the tensor product of representations \( \rho_i \) for \( i \in S \). If \( S \) is a proper subset of \( \{0, 1, \ldots, m-1\} \) then there exists an element \( u \in G \) such that the trace of \( \rho_S(u) \) does not belong to \( \mathbb{F}_2 \). In particular, \( \rho_S \) could not be obtained by extension of scalars to \( \mathcal{F} \) from a representation of \( G \) over \( \mathbb{F}_2 \).

Proof. Clearly,

\[
\text{tr}(\rho_i(u)) = (\text{tr}(\rho_0(u)))^{2^i} \quad \forall u \in G.
\]

This implies easily that

\[
\text{tr}(\rho_S(u)) = \prod_{i \in S} \text{tr}(\rho_i(u)) = (\text{tr}(\rho_0(u)))^M
\]

where \( M = \sum_{i \in S} 2^i \). Since \( S \) is a proper subset of \( \{0, 1, \ldots, m-1\} \), we have

\[
0 < M < \sum_{i=0}^{m-1} 2^i = 2^m - 1 = \#(\mathbb{F}_q^*).
\]

Assume that the condition (i) holds. Then there exists \( u \in G \) such that \( \alpha = \text{tr}(\rho_0(u)) \) lies in \( \mathbb{F}_q^* \) and the exact multiplicative order of \( \alpha \) is \( q - 1 = 2^m - 1 \).

This implies that \( 0 \neq \alpha^M \neq 1 \). Since \( \mathbb{F}_2 = \{0, 1\} \), we conclude that \( \alpha^M \notin \mathbb{F}_2 \).

Therefore

\[
\text{tr}(\rho_S(u)) = (\text{tr}(\rho_0(u)))^M = \alpha^M \notin \mathbb{F}_2.
\]

Now assume that the condition (ii) holds. It follows from Remark 1.1 that there exists \( \alpha = \alpha_i \neq 0 \) such that \( \alpha^M \neq 1 \) for some \( i \) with \( 1 \leq i \leq r \). This implies that if we put \( u = u_i \) then

\[
\text{tr}(\rho_S(u)) = (\text{tr}(\rho_0(u)))^M = \alpha^M \notin \mathbb{F}_2.
\]
Now, let us put \( q' = q^2 = p^{2m} \). We write \( x \mapsto \bar{x} \) for the involution \( a \mapsto a^q \) of \( F_q \). Let us consider the special unitary group \( SU_3(F_q) \) consisting of all matrices \( A \in SL_3(F_{q^2}) \) which preserve a nondegenerate Hermitian sesquilinear form on \( F_{q^2}^3 \) say,

\[
\begin{align*}
  x, y &\mapsto x_1y_3 + x_2y_2 + x_3y_1 \\
  \forall x = (x_1, x_2, x_3), y = (y_1, y_2, y_3).
\end{align*}
\]

It is well-known that the conjugacy class of the special unitary group in \( GL_3(F_{q^2}) \) does not depend on the choice of Hermitian form and \( #(SU_3(F_q)) = (q^3 + 1)q^3(q^2 - 1) \). Clearly, for each \( \beta \in F_q^* \), the group \( SU_3(F_q) \) contains the diagonal matrix \( u = \text{diag}(\beta, 1, \beta^{-1}) \) with eigenvalues \( \beta, 1, \beta^{-1} \); clearly, the trace of \( u \) is \( \beta + \beta^{-1} + 1 \).

**Theorem 4.3.** Suppose \( G = SU_3(F_q) \). Suppose \( V \) is an absolutely simple nontrivial \( F_2[G] \)-module. Assume that \( m > 1 \). If \( \text{dim}_{F_2}(V) \) is a power of 2 then it is equal to \( q^3 \). In particular, \( V \) is the Steinberg representation of \( SU_3(F_q) \).

**Proof.** Recall ([1], p. 77, 2.8.10c), that the adjoint representation of \( G \) in \( \text{End}_{F_{q^2}}(F_3^3) \) splits into a direct sum of the trivial one-dimensional representation (scalars) and an absolutely simple \( F_{q^2}[G] \)-module \( \text{St}_2 \) of dimension 8 (traceless operators). The kernel of the natural homomorphism

\[
G = SU_3(F_q) \to \text{Aut}_{F_{q^2}}(\text{St}_2) \cong GL_8(F_{q^2})
\]

coincides with the center \( Z(G) \) which is either trivial or a cyclic group of order 3 depending on whether \( (3, q + 1) = 1 \) or 3. In both cases we get an embedding

\[
G' := G/Z(G) = U_3(q) = PSU_3(F_q) \subset GL_8(F_{q^2}).
\]

If \( m = 2 \) (i.e., \( q = 4 \)) then \( G = SU_3(F_4) = U_3(4) \) and one may use Brauer character tables [3] in order to study absolutely irreducible representations of \( G \) in characteristic 2. Notice ([1], p. 284) that the reduction modulo 2 of the irrational constant \( b_5 \) does not lie in \( F_2 \). Using the Table on p. 70 of [1], we conclude that there is only one (up to an isomorphism) absolutely irreducible representation of \( G \) defined over \( F_2 \) and its dimension is \( 64 = q^3 \). This proves the assertion of the theorem in the case of \( m = 2, q = 4 \). So further we assume that

\[
m \geq 3, \quad q = 2^m \geq 8.
\]

Clearly, for each \( u \in G \subset GL_3(F_{q^2}) \) with trace \( \delta \in F_{q^2} \) the image \( u' \) of \( u \) in \( G' \) has trace \( \delta \delta - 1 \in F_q \). In particular, if \( u = \text{diag}(\beta, 1, \beta^{-1}) \) with \( \beta \in F_q^* \), then the trace of \( u' \) is

\[
t_{\beta} := \text{tr}(u') = (1 + \beta + \beta^{-1})(1 + \beta + \beta^{-1}) - 1 = (\beta + \beta^{-1})^2.
\]

Now let us start to vary \( \beta \) in the \( q - 2 \)-element set

\[
F_q \setminus F_2 = F_q^* \setminus \{1\}.
\]

One may easily check that the set of all \( t_{\beta} \)'s consists of \( \frac{q-2}{2} \) elements of \( F_q^* \). Since \( q \geq 8, \)

\[
r := \frac{q - 2}{2} > \frac{q - 1}{3}.
\]

This implies that \( G' \subset GL_8(F_{q^2}) \) satisfies the conditions of Lemma [12] with \( d = 8 \). In particular, none of representations \( \rho_S \) of \( G' \) could be realized over \( F_2 \) if \( S \) is a proper subset of \( \{0, 1, \ldots, m - 1\} \). On the other hand, it is known ([1], p. 77, Example 2.8.10c) that each absolutely irreducible representation of \( G \) over \( F \) either has dimension divisible by 3 or is isomorphic to the representation obtained from some \( \rho_S \) via \( G \to G' \). The rest is clear. \( \square \)
Theorem 4.4. Suppose \( m > 1 \) is an integer and let us put \( q = 2^m \). Let \( B \) be a \((q^3 + 1)\)-element set. Let \( G' \) be a group acting faithfully on \( B \). Assume that \( G' \) contains a subgroup \( G \) isomorphic to \( U_3(q) \). Then the \( G' \)-module \( Q_B \) is very simple.

Proof. First, \( U_3(q) \) is a simple non-abelian group, whose order is \( q^3(q^3 + 1)(q^2 - 1)/(3, q + 1) \) (\[\text{[1]}\], p. XVI, Table 6; \[\text{[3]}\], pp. 39–40). Second, notice that \( U_3(q) \subset G' \) acts transitively on \( B \). Indeed, the classification of subgroups of \( U_3(q) \) (\[\text{[3]}\], Th. 6.5.3 and its proof, p. 329–332) implies that each subgroup of \( U_3(q) \) has index \( \geq q^3 + 1 = \#(B) \). This implies that \( U_3(q) \) acts transitively on \( B \). Third, we claim that this action is, in fact, doubly transitive. Indeed, the stabilizer \( U_3(q)_b \) of a point \( b \in B \) has index \( q^3 + 1 \) in \( U_3(q) \). It follows easily from the same classification that \( U_3(q)_b \) is the (image of the) stabilizer (in \( SU_3(F_q) \)) of a proper subspace \( L \) in \( F_3^{q^3} \). If \( L \) is a plane then counting arguments imply that the restriction of the Hermitian form to \( L \) could not be non-degenerate and therefore \( U_3(q)_b \) coincides with (the image of) the stabilizer of certain isotropic line \( L' \subset L \subset F_3^{q^3} \). (The line \( L' \) is the orthogonal complement of \( L \)!) If \( L \) is a line then counting arguments imply that \( L \) is isotropic. Hence we may always assume that \( U_3(q)_b \) is (the image of) the stabilizer of an isotropic line in \( F_3^{q^3} \). Taking into account that the set of isotropic lines in \( F_3^{q^3} \) has cardinality \( q^3 + 1 = \#(B) \), we conclude that \( B = U_3(q)/U_3(q)_b \) is isomorphic (as \( U_3(q) \)-set) to the set of isotropic lines on which \( U_3(q) \) acts doubly transitively and we are done.

By Remark 4.2, the double transitivity implies that the \( F_2[U_3(q)] \)-module \( Q_B \) is absolutely simple. Since \( SU_3(F_q) \to U_3(q) \) is surjective, the \( F_2[SU_3(F_q)] \)-module \( Q_B \) is also absolutely simple. Also, in order to prove that \( F_2[U_3(q)] \)-module \( Q_B \) is very simple, it suffices to check that the \( F_2[SU_3(q)] \)-module \( Q_B \) is very simple.

Recall that \( \dim_{F_2}(Q_B) = \#(B) - 1 = q^3 = 2^{3m} \). By Theorem 4.3, there no absolutely simple nontrivial \( F_2[SU_3(F_q)] \)-modules, whose dimension strictly divides \( 2^{3m} \). This implies that \( Q_B \) is not isomorphic to a tensor product of absolutely simple \( F_2[SU_3(F_q)] \)-modules of dimension \( > 1 \). Therefore \( Q_B \) is not isomorphic to a tensor product of absolutely simple \( F_2[U_3(q)] \)-modules of dimension \( > 1 \).

Recall that all subgroups in \( G = U_3(q) \) different from \( U_3(q) \) itself have index \( \geq q^3 + 1 > q^3 = \dim_{F_2}(Q_B) \). It follows from Corollary 5.3 that the \( G \)-module \( Q_B \) is very simple.

\[\square\]

5. Proof of Theorems 2.1

Recall that \( \text{Gal}(f) \subset \text{Perm}(\mathfrak{M}) \). It is also known that the natural homomorphism \( \text{Gal}(K) \to \text{Aut}_{F_2}(J(C)_2) \) factors through the canonical surjection \( \text{Gal}(K) \to \text{Gal}(K(\mathfrak{M})/K) = \text{Gal}(f) \) and the \( \text{Gal}(f) \)-modules \( J(C)_2 \) and \( Q_{2\mathfrak{M}} \) are isomorphic (see, for instance, Th. 5.1 of \[\text{[13]}\]). In particular, if the \( \text{Gal}(f) \)-module \( Q_{2\mathfrak{M}} \) is very simple then the \( \text{Gal}(f) \)-modules \( J(C)_2 \) is also very simple and therefore is absolutely simple.

Lemma 5.1. If the \( \text{Gal}(f) \)-module \( Q_{2\mathfrak{M}} \) is very simple then either \( \text{End}(J(C_f)) = \mathbb{Z} \) or \( \text{char}(K) > 0 \) and \( J(C_f) \) is a supersingular abelian variety.

Proof. This is Corollary 5.3 of \[\text{[13]}\].
It follows from Theorem 1.4 that under the assumptions of Theorem 2.1, the \( \text{Gal}(f) \)-module \( Q_{2M} \) is very simple. Applying Lemma 5.1, we conclude that either \( \text{End}(J(C_f)) = \mathbb{Z} \) or \( \text{char}(K) > 0 \) and \( J(C_f) \) is a supersingular abelian variety.

**References**

[1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups. Clarendon Press, Oxford, 1985.

[2] Ch. W. Curtis, *The Steinberg character of a finite group with a \((B, N)\)-pair*. J. Algebra 4 (1966), 433–441.

[3] D. Gorenstein, R. Lyons, R. Solomon, The Classification of the finite simple groups, Number 3. AMS, Providence, RI, 1994.

[4] J. E. Humphreys, *The Steinberg representation*. Bull. AMS (N.S.) 16 (1987), 247–263.

[5] Ch. Jansen, K. Lux, R. Parker, R. Wilson, An Atlas of Brauer characters. Clarendon Press, Oxford, 1995.

[6] N. Katz, *Monodromy of families of curves: applications of some results of Davenport-Lewis*. In: Séminaire de Théorie des Nombres, Paris 1979-80 (ed. M.-J. Bertin); Progress in Math. 12, pp. 171–195, Birkhäuser, Boston-Basel-Stuttgart, 1981.

[7] N. Katz, *Affine cohomological transforms, perversity, and monodromy*. J. Amer. Math. Soc. 6 (1993), 149–222.

[8] D. Masser, *Specialization of some hyperelliptic jacobians*. In: Number Theory in Progress (eds. K. Györy, H. Iwaniec, J. Urbanowicz), vol. I, pp. 293–307; de Gruyter, Berlin-New York, 1999.

[9] Sh. Mori, *The endomorphism rings of some abelian varieties*. Japanese J. Math, 2(1976), 109–130.

[10] Sh. Mori, *The endomorphism rings of some abelian varieties. II*. Japanese J. Math, 3(1977), 105–109.

[11] J.-P. Serre, Linear representations of finite groups, Springer-Verlag, 1977.

[12] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Res. Letters 7(2000), 123–132.

[13] Yu. G. Zarhin, *Hyperelliptic jacobians and modular representations*. In: Moduli of abelian varieties (C. Faber, G. van der Geer, F. Oort, eds.), pp. 473–490, Progress in Math., Vol. 195, Birkhäuser, Basel–Boston–Berlin, 2001.

[14] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication in positive characteristic*. Math. Res. Letters 8 (2001), to appear.

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

E-mail address: zarhin@math.psu.edu