On unramified normal coverings of hyperelliptic curves

Yolanda Fuertes and Gabino González-Diez*
Departamento de Matemáticas
Universidad Autónoma de Madrid
28049. Madrid
e-mail: yolanda.fuertes@uam.es
e-mail: gabino.gonzalez@uam.es

Abstract

It is well known that the number of *unramified* normal coverings of an irreducible complex algebraic curve C with group of covering transformations isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is $(2^{4g} - 3 \cdot 2^{2g} + 2)/6$. Assume that C is hyperelliptic, say $C : y^2 = \prod_{d=1}^{2g+2}(x - \mu_d)$. Horiouchi has given the explicit algebraic equations of the subset of those covers which turn out to be hyperelliptic themselves. There are $\binom{2g+2}{3}$ of this particular type. In this article we provide algebraic equations for the remaining ones.

1 Introduction

Throughout this article we will use the same term curve *to refer to an affine algebraic curve, its complete non singular model and its associated compact Riemann surface.*

The problem of describing the smooth normal coverings of a given hyperelliptic Riemann surface C of genus g, say with equation

$$C : y^2 = \prod_{d=1}^{2g+2}(x - \mu_d), \tag{1}$$

was raised by Maclachlan who showed (see [10]) that any *smooth*, or *unramified*, normal covering between hyperelliptic Riemann surfaces has covering group isomorphic to either $\mathbb{Z}_2$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2$ being the cyclic group of order 2.

It was Farkas ([3]) who initiated the study of the $\mathbb{Z}_2$ case by proving that $\binom{2g+2}{2}$ of the $2^{2g} - 1$ smooth double covers of C are again hyperelliptic. Then

2000 *Mathematics Subject Classification.* 14H37, 14H45, 30F10

*Both authors partially supported by Grant BFM2003–04964 of the MCYT.

Horiouchi ([9]) provided algebraic equations for these $\binom{2g+2}{2}$ covers (and, indeed, for all normal covers of C, unramified or not, which are again hyperelliptic). Later on Bujalance ([1], see also [4]) showed that any unramified double cover $\widetilde{C}$ of C is, in addition, a ramified double cover of a Riemann surface of genus p, for some $p = 0, ..., \left[\frac{g-1}{2}\right]$. Curves enjoying this second property are usually termed *p-hyperelliptic*, the case $p = 0$ being the hyperelliptic case. Recently the authors ([5]) have been able to produce explicit algebraic equations for the remaining $2^{2g} - 1 - \binom{2g+2}{2}$ non hyperelliptic covers too.

As for the $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ case, Kato proved that precisely $\binom{2g+2}{3}$ of the $(2^{4g} - 3 \cdot 2^{2g} + 2)/6$ degree four smooth normal covers of C are again hyperelliptic (see Horiouchi's paper cited above). This same paper [9] contains explicit algebraic equations for these $\binom{2g+2}{3}$ hyperelliptic covers. Here we provide algebraic equations for all unramified $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ covers of C including the non hyperelliptic ones. We also prove that all of them are p-hyperelliptic for some $p \leq \left[\frac{g}{2}\right] + g - 1$.

The interest of having at one's disposal explicit algebraic equations for covers of a given hyperelliptic curve is that, for its simplicity, hyperelliptic curves have proved very useful to illustrate known results or to test new conjectures. For instance, the equations of the smooth hyperelliptic normal 4 to 1 covers obtained in Corollary 2 of this paper have been used by the authors in [6] to provide examples of hyperelliptic curves whose *field of moduli* is $\mathbb{Q}$ but such that the minimum real field over which they can be (hyperelliptically) defined is a degree 3 extension of $\mathbb{Q}$.

Here we give an application of the same kind. It is well known (see e.g. [7]) that if a curve is defined over a field $k \subset \mathbb{C}$, then all its unramified coverings can be defined over the algebraic closure of k. In Corollary 4 of this paper we show that, for suitable hyperelliptic curves defined over $\mathbb{Q}$, their smooth $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ coverings are also defined over $\mathbb{Q}$.

2 Results

In order to state our results more rigorously it will be convenient to introduce some notation. We shall denote by X the set $X = \{1, ..., 2g+2\}$. For a subset $A \subseteq X$, we will denote by $|A|$ its *cardinality* and by A^C its *complement* in X. If $B \subseteq X$ is another subset, $A \triangle B$ will stand for the *symmetric difference* $A \triangle B = (A \cap B^C) \cup (B \cap A^C)$. If both A and B are non empty subsets, $C_{A,B}$ will stand for the space curve

$$C_{A,B} : \begin{cases} z^2 = \prod_{k \in A}(x - \mu_k) \\ \\ w^2 = \prod_{j \in B}(x - \mu_j). \end{cases} \tag{2}$$

In this article we prove the following

Theorem 1 *Let C be an arbitrary hyperelliptic curve given by equation (1). Then* *i) Every unramified normal covering of C with group of covering transformations isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is a compact Riemann surface of genus $1+4(g-1)$ isomorphic to a curve $\widetilde{C}_A^B$ given in affine 4-dimensional space by*

$$\widetilde{C}_A^B = \widetilde{C}_B^A : \begin{cases} y^2 = \prod_{d=1}^{2g+2}(x-\mu_d) \\ \\ z^2 = \prod_{k\in A}(x-\mu_k) \\ \\ w^2 = \prod_{j\in B}(x-\mu_j) \end{cases} \tag{3}$$

where A and B range among all nonempty proper subsets of X with even cardinality $\leq g+1$ and such that $A \neq B$ and $A \neq B^C$. The covering group is generated by the involutions $\alpha_1(x,y,z,w) = (x,y,z,-w)$, $\alpha_2(x,y,z,w) = (x,y,-z,w)$ and the covering map π is given by projection onto the (x,y)-coordinates.

ii) Any two such curves $\widetilde{C}_A^B$ and $\widetilde{C}_E^F$ are isomorphic coverings of C if and only if the unordered pair $\{E,F\}$ equals $\{A,B\}, \{A\triangle B, A\}$ or $\{A\triangle B, B\}$.

iii) The curve $\widetilde{C}_A^B$ is a double cover of the curves $C_{E,F}$, for $\{E,F\}$ equal to any of the following pairs $\{X,A\}$, $\{X,B\}$, $\{X,A\triangle B\}$, $\{A,B\}$, $\left\{A^C,B\right\}$, $\left\{A,B^C\right\}$ and $\left\{A^C,B^C\right\}$. The corresponding covering groups being $<\alpha_1>$, $<\alpha_2>$, $<\alpha_1\circ\alpha_2>$, $<\alpha_3(x,y,z,w)=(x,-y,z,w)>$, $<\alpha_2\circ\alpha_3>$, $<\alpha_1\circ\alpha_3>$ and $<\alpha_1\circ\alpha_2\circ\alpha_3>$, respectively.

iv) The curve C_E^F has genus $p = |E\cup F| - 3$. In particular $\widetilde{C}_A^B$ is p-hyperelliptic for some $p \leq \left[\frac{g}{2}\right] + g - 1$.

In order to identify the hyperelliptic covers of C among all covers described in Theorem 1, let us recall (see [11]) that if $\widetilde{C}_A^B$ is hyperelliptic, its hyperelliptic involution $\tilde{J}$ has to be a lift of the hyperelliptic involution of C, $J(x,y) = (x,-y)$, that is, we must have $\pi\circ\tilde{J} = J\circ\pi$. It readily follows that, $\tilde{J}$ has to be one of the following automorphisms: α_3, $\alpha_3\circ\alpha_1$, $\alpha_3\circ\alpha_2$ or $\alpha_1\circ\alpha_2\circ\alpha_3$. Therefore, combining parts iii) and iv) of Theorem 1, we see that hyperelliptic covers arise only when $p = |A\cup B| - 3 = 0$. In other words, the hyperelliptic covers are precisely the curves $\widetilde{C}_A^B := C_{ijk}$ with A and B of the form $A = \{i,j\}$ and $B = \{i,k\}$. Moreover, by part ii) of Theorem 1 any permutation of the indices i,j,k gives rise to the same covering. We, thus, see that there are exactly $\binom{2g+2}{3}$ inequivalent coverings C_{ijk} of this type. Each of them can be expressed as a space curve as follows:

$$C_{ijk} : \begin{cases} y_1^2 = \prod_{d\neq i,j}^{2g+2}\left(t^2 - \frac{\mu_d-\mu_j}{\mu_d-\mu_i}\right) \\ w^2 = (x-\mu_i)(x-\mu_k) \end{cases}$$

where $t = z \diagup (x-\mu_i)$, hence $x = (\mu_j - t^2\mu_i)\diagup\left(1-t^2\right)$, and
$y_1 = y\left(1-t^2\right)^{g+1} \diagup t(\mu_j-\mu_i)\sqrt{\prod_{d\neq i,j}^{2g+2}(\mu_d-\mu_i)}$. Replacing x by its expression as a function of t on the second defining equation of C too, we get

$$C_{ijk} : \begin{cases} y_1^2 = \prod_{d\neq i,j}^{2g+2}\left(t^2 - \frac{\mu_d-\mu_j}{\mu_d-\mu_i}\right) \\ \eta^2 = t^2 - \frac{\mu_k-\mu_j}{\mu_k-\mu_i} \end{cases}$$

where $\eta = \frac{(1-t^2)w}{\sqrt{(\mu_k-\mu_i)(\mu_j-\mu_i)}}$. Furthermore, if we now put $s = \frac{\eta}{t-\sqrt{\frac{\mu_k-\mu_j}{\mu_k-\mu_i}}}$, we find that $s^2 = \frac{t+\sqrt{\frac{\mu_k-\mu_j}{\mu_k-\mu_i}}}{t-\sqrt{\frac{\mu_k-\mu_j}{\mu_k-\mu_i}}}$ which shows that t can be written as $t = \frac{s^2+1}{s^2-1}\sqrt{\frac{\mu_k-\mu_j}{\mu_k-\mu_i}}$. Performing this last substitution, we finally arrive at the following plane model

$$C_{ijk} : y_2^2 = \prod_{d\neq i,j,k}^{2g+2}\left(s^4 + 2s^2\left(1 - 2\frac{(\mu_i-\mu_k)(\mu_d-\mu_j)}{(\mu_d-\mu_k)(\mu_i-\mu_j)}\right) + 1\right)$$

where

$$y_2 = y_1\frac{\left(s^2-1\right)^{2g}}{2s}\sqrt{\frac{\mu_k-\mu_i}{\mu_k-\mu_j}}\sqrt{\prod_{d\neq i,j,k}\frac{(\mu_d-\mu_i)(\mu_k-\mu_i)}{(\mu_d-\mu_k)(\mu_i-\mu_j)}}.$$

We can also keep track of the expressions for the covering map $C_{ijk} \to C$ and for the covering group in these coordinates. The result we obtain is the following

Corollary 2 *Let C be an arbitrary hyperelliptic curve of genus g given by equation (1). Then C admits precisely $\binom{2g+2}{3}$ smooth normal hyperelliptic coverings C_{ijk} with group of covering transformations isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, each of them corresponding to the choice of an unordered triple of the set $\{1, 2, \ldots, 2g+2\}$. The covering corresponding to a triple $\{i, j, k\}$ is the Riemann surface C_{ijk} isomorphic to the plane curve*

$$C_{ijk} : y^2 = \prod_{d\neq i,j,k}^{2g+2}\left(x^4 + 2x^2\left(1 - 2\frac{(\mu_i-\mu_k)(\mu_d-\mu_j)}{(\mu_d-\mu_k)(\mu_i-\mu_j)}\right) + 1\right)$$

with covering map $F_{ijk} = (F_1, F_2) : C_{ijk} \to C$ given by

$$F_1 = \frac{\mu_j - \mu_i\left(\frac{x^2+1}{x^2-1}\right)^2\frac{(\mu_k-\mu_j)}{(\mu_k-\mu_i)}}{1-\left(\frac{x^2+1}{x^2-1}\right)^2\frac{(\mu_k-\mu_j)}{(\mu_k-\mu_i)}}$$

$$F_2 = \frac{\sqrt{\prod_{d\neq i,j,k}^{2g+2}(\mu_d-\mu_k)(\mu_i-\mu_j)}(\mu_k-\mu_j)(\mu_j-\mu_i)(\mu_k-\mu_i)2x\left(x^4-1\right)y}{\left(\mu_j(x^2+1)^2-\mu_i(x^2-1)^2-4x^2\mu_k\right)^{g+1}}.$$

Moreover, the covering group is generated by the involutions $\widetilde{\alpha}_1(x,y) = (-x,-y)$ and $\widetilde{\alpha}_2(x,y) = (1/x, -y/x^{4(g-1)})$.

2.1 The unramified normal hyperelliptic covers of a hyperelliptic curve

According to Maclachlan ([10]) any unramified covering between hyperelliptic curves has covering group G isomorphic to either $\mathbb{Z}_2$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. We are now in position to write down the (hyperelliptic) equations of all unramified normal hyperelliptic covers of a given hyperelliptic curve.

Theorem 3 *Let*

$$C : y^2 = \prod_{d=1}^{2g+2} (x - \mu_d)$$

be an arbitrary hyperelliptic curve of genus g and $F = (F_1, F_2) : \widetilde{C} \to C$ an unramified normal hyperelliptic cover of C with covering group G. Then, $F : \widetilde{C} \to C$ is isomorphic to one of the following coverings:

*1) ($G \cong \mathbb{Z}_2$-**case**)*

$$\begin{cases} \widetilde{C} : y^2 = \prod_{k \neq i,j}^{2g+2} \left(x^2 - \frac{\mu_k - \mu_i}{\mu_k - \mu_j} \right) \\ \\ G = \langle \alpha(x, y) = (-x, -y) \rangle \\ \\ F(x, y) = \left(\frac{\mu_i - \mu_j x^2}{1 - x^2}, xy(\mu_i - \mu_j) \frac{\sqrt{\prod_{d \neq i,j} (\mu_d - \mu_j)}}{(1 - x^2)^{g+1}} \right) \end{cases}$$

where i, j ranges among the $\binom{2g+2}{2}$ unordered pairs of the set $\{1, 2, \ldots, 2g+2\}$. The covering corresponding to the pair $\{i, j\}$ being characterized, up to equivalence, by the property that $P_i = (\mu_i, 0), P_j = (\mu_j, 0)$ are the only Weierstrass points of C which are not covered by Weierstrass points of the covering curve.

*2) ($G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$-**case**)*

$$\begin{cases} \widetilde{C} : y^2 = \prod_{d \neq i,j,k}^{2g+2} \left(x^4 + 2x^2 \left(1 - 2 \frac{(\mu_i - \mu_k)(\mu_d - \mu_j)}{(\mu_d - \mu_k)(\mu_i - \mu_j)} \right) + 1 \right) \\ \\ G = \langle \widetilde{\alpha}_1(x, y) = (-x, -y), \ \widetilde{\alpha}_2(x, y) = (1/x, -y/x^{4(g-1)}) \rangle \\ \\ F_1 \text{ and } F_2 \text{ as in Corollary 2} \end{cases}$$

where i, j, k ranges among the $\binom{2g+2}{3}$ unordered triples of the set $\{1, \ldots, 2g+2\}$. Up to equivalence, the covering corresponding to the triple $\{i, j, k\}$ is characterized by the property that P_i, P_j, P_k are the only Weierstrass points of C which are not covered by Weierstrass points of the covering curve.

Proof. The $\mathbb{Z}_2$-case was carried out in [5] (c.f. [9]).

The $\mathbb{Z}_2 \oplus \mathbb{Z}_2$-case is the content of Corollary 2 except for the fact that P_i, P_j, P_k are the only Weierstrass points of C which are not covered by Weierstrass points of $\widetilde{C}$. This follows once we check that the solutions of

$$0 = x^4 + 2x^2 \left(1 - 2 \frac{(\mu_i - \mu_k)(\mu_d - \mu_j)}{(\mu_d - \mu_k)(\mu_i - \mu_j)} \right) + 1$$

agree with the solutions of $F_1(x, y) = \mu_d$, for each $d \neq i, j, k$. To do that, we work out the last equality to obtain

$$\mu_d = \frac{\mu_k(\mu_j - \mu_i)x^4 - 2x^2(\mu_k(\mu_i + \mu_j) - 2\mu_i\mu_j) + \mu_k(\mu_j - \mu_i)}{(\mu_j - \mu_i)x^4 + 2x^2((\mu_i + \mu_j) - 2\mu_k) + (\mu_j - \mu_i)}$$

or equivalently,

$$0 = (\mu_d - \mu_k)(\mu_j - \mu_i) \left(x^4 + 2x^2 \left(\frac{(\mu_i + \mu_j)(\mu_d + \mu_k) - 2\mu_i\mu_j - 2\mu_k\mu_d}{(\mu_d - \mu_k)(\mu_j - \mu_i)} \right) + 1 \right)$$

as desired. ■

2.2 A remark concerning fields of definition

There are in the literature several papers (see e.g [2] and the references given there) studying the relationship between the field of definition of a curve and that of its coverings. In view of that it may be worth recording here the following corollary to Theorem 1

Corollary 4 *For any hyperelliptic curve given by $C : y^2 = f(x)$ as in (1), we have the following results:*

a) If $f(x)$ lies in $\mathbb{Q}[x]$ and splits over $\mathbb{Q}$ into different linear factors, then every smooth $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ covering of C is also defined over the rational numbers.

b) If $f(x)$ lies in $\mathbb{Q}[x]$ and splits into the product of two polynomials of even degree and with coefficients in $\mathbb{Q}$, then C admits at least one smooth $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ covering which is also defined over the rational numbers.

Proof. Part a) follows directly from part i) in Theorem 1 because in this case, the three defining equations of any smooth $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ covering of C, $\widetilde{C}_A^B$, lie in $\mathbb{Q}[x]$.

In order to prove part b), let us write $f(x) = p(x)q(x)$ with $p(x), q(x) \in \mathbb{Q}[x]$ polynomials of even degree. Then the covering in question is given by

$$\widetilde{C} : \begin{cases} y^2 = f(x) \\ z^2 = p(x) \\ w^2 = q(x). \end{cases}$$

■

3 Proof of Theorem 1

3.1 Some previous results

We shall make use of the following result

Theorem 5 *([5]) Let C be the hyperelliptic curve given by equation (1). Then i) Every unramified double cover of C is isomorphic to a space curve $C_{X,A}$ as in (2), where A ranges among all nonempty proper subsets of even cardinality of X. The covering map being given by projection onto the (x, y)-coordinates. ii) Two such curves $C_{X,A}$ and $C_{X,B}$ are isomorphic coverings of C if and only if $B = A$ or $B = A^C$.*

We will also need the following

Lemma 6 *Let $\widetilde{C}$ be a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ smooth covering of a given curve C. Let α_1 and α_2 be generators of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $\pi_i : \widetilde{C} \to C_i = C \diagup \langle \alpha_i \rangle$ and $f_i : C_i \to C \diagup \mathbb{Z}_2 \oplus \mathbb{Z}_2$ the obvious projection maps. Then $\widetilde{C}$ is isomorphic to the fibre product $C_1 \underset{C}{\times} C_2$ defined by the following diagram*

$$\begin{array}{ccc} \widetilde{C} & \overset{\pi_2}{\to} & C_2 \\ \pi_1 \downarrow & & \downarrow f_2 \\ C_1 & \overset{f_1}{\to} & C \end{array}$$

Proof. By the universal property defining the fibre product (see [8]), all we have to see is that for any commutative diagram of morphisms between compact Riemann surfaces as follows

$$\begin{array}{ccc} X & \overset{p_2}{\to} & C_2 \\ p_1 \downarrow & & \downarrow f_2 \\ C_1 & \overset{f_1}{\to} & C \end{array}$$

there is a unique morphism $\phi : X \to \widetilde{C}$ making commutative the following diagram

$$\begin{array}{ccccc} & & C_2 & & \\ & \overset{p_2}{\nearrow} & \uparrow \pi_2 & \overset{f_2}{\searrow} & \\ X & \overset{\phi}{\to} & \widetilde{C} & & C \\ & \underset{p_1}{\searrow} & \downarrow \pi_1 & \underset{f_1}{\nearrow} & \\ & & C_1 & & \end{array} \tag{4}$$

Now, if such morphism $\phi : X \to \widetilde{C}$ is going to exist, we must have $\pi_i \phi(x) = p_i(x)$ hence $\phi(x) \in \pi_i^{-1}(p_i(x))$, $i = 1, 2$. Therefore, the result would follow if we could prove that, for all points $x \in X$, the set $\pi_1^{-1}(p_1(x)) \cap \pi_2^{-1}(p_2(x))$ contains exactly one point of $\widetilde{C}$, for in that case the morphism ϕ would be the holomorphic map $x \mapsto \pi_1^{-1}(p_1(x)) \cap \pi_2^{-1}(p_2(x))$. The proof of this fact will be done in several steps.

(i) The restriction of π_1 to $\pi_2^{-1}(p_2(x))$ is injective.

Suppose $P, Q \in \pi_2^{-1}(p_2(x))$ with $\pi_1(P) = \pi_1(Q)$, then we have $\pi_i(P) = \pi_i(Q)$, $i = 1, 2$. If $P \neq Q$ this implies that $Q = \alpha_1(P) = \alpha_2(P)$, and hence $\alpha_2^{-1}\alpha_1(P) = P$, hence $\alpha_2^{-1}\alpha_1 = id$. Contradiction.

(ii) The set $\pi_1^{-1}(p_1(x)) \cap \pi_2^{-1}(p_2(x))$ contains, at most, one point.

This follows from (i) once we observe that π_1 takes the constant value $p_1(x)$ at all points of $\pi_1^{-1}(p_1(x))$.

(iii) $\pi_1(\pi_2^{-1}(p_2(x))) \subset f_1^{-1}(f_1 p_1(x))$.

Let $P \in \pi_2^{-1}(p_2(x))$. We have $f_1\pi_1(P) = f_2\pi_2(P) = f_2 p_2(x) = f_1 p_1(x)$, hence $\pi_1(P) \in f_1^{-1}(f_1 p_1(x))$.

(iv) For all points $x \in X$ we have $\pi_1(\pi_2^{-1}(p_2(x))) = f_1^{-1}(f_1 p_1(x))$.

As $deg(f_1) = deg(\pi_2) = 2$, the sets $f_1^{-1}(f_1 p_1(x))$ and $\pi_2^{-1}(p_2(x))$ contain both exactly 2 points. Using (i) we see that same statement holds for the set $\pi_1(\pi_2^{-1}(p_2(x)))$. We now apply (iii) to conclude our argument.

(v) For all points $x \in X$ the set $\pi_1^{-1}(p_1(x)) \cap \pi_2^{-1}(p_2(x))$ is non empty.

¿From (iv) we deduce that the point $p_1(x) \in f_1^{-1}(f_1 p_1(x))$ can be written as $p_1(x) = \pi_1(P)$ for some $P \in \pi_2^{-1}(p_2(x))$, thus $P \in \pi_1^{-1}(p_1(x)) \cap \pi_2^{-1}(p_2(x))$.

The proof of the Lemma is now concluded. ■

3.2 Proof of Theorem 1

The key point in proving this theorem is the observation that, by definition (see e.g. [8]), the curve $\widetilde{C}_A^B$ is nothing but the fibre product $C_{X,A} \underset{C}{\times} C_{X,B}$ determined by the diagram

$$\begin{array}{ccc} \widetilde{C}_A^B = C_{X,A} \underset{C}{\times} C_{X,B} & \xrightarrow{\pi_B} & C_{X,B} \\ \downarrow \pi_A & & \downarrow f_2 \\ C_{X,A} & \xrightarrow{f_1} & C \end{array}$$

where the maps f_i are the projection morphisms $f_1(x, y, z) = (x, y)$, $f_2(x, y, w) = (x, y)$ and the maps π_A and π_B are defined by $\pi_A(x, y, z, w) = (x, y, z)$ and $\pi_B(x, y, z, w) = (x, y, w)$. It is clear that the morphisms π_A and π_B are the quotient maps induced by the action of the automorphisms of $\widetilde{C}_A^B$ given by $\alpha_1(x, y, z, w) = (x, y, z, -w)$ and $\alpha_2(x, y, z, w) = (x, y, -z, w)$, respectively. It is also clear that these two automorphisms generate a group $\langle\alpha_1, \alpha_2\rangle$ isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ whose quotient $\widetilde{C}_A^B / \langle\alpha_1, \alpha_2\rangle$ is isomorphic to C, such that $f_1 \circ \pi_A = f_2 \circ \pi_B$ is the corresponding quotient map. Now, by Theorem 5, f_1 and f_2 are unramified morphisms. It then follows from general facts concerning fibre products of curves (see e.g. [12], p. 116) that both maps π_A and π_B are unramified. Thus, $\widetilde{C}_A^B$ is indeed a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ unramified covering of C. We now claim that, in fact, any unramified $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ cover of C is of the form $\widetilde{C}_A^B$. This is because, first, Lemma 6 tells us that any such cover is isomorphic to $C_1 \underset{C}{\times} C_2$, where C_i, $i = 1$ and 2, are smooth double covers of C, and then Theorem 5 states that C_1 and C_2 are curves of the form $C_{X,A}$ and $C_{X,B}$.

We next observe that the three covers $\widetilde{C}_A^B$, $\widetilde{C}_{A\triangle B}^B$ and $\widetilde{C}_{A\triangle B}^A$ are isomorphic, by means of the isomorphism

$$(x, y, z, w) \in \widetilde{C}_A^B \mapsto \left(x, y, \frac{z \cdot w}{\prod_{l \in A \cap B}(x - \mu_l)}, w\right) \in \widetilde{C}_{A\triangle B}^B$$

(and a similar one between $\widetilde{C}_A^B$ and $\widetilde{C}_{A\triangle B}^A$). Thus, to conclude the proof of parts i) and ii) of the theorem, it only remains to convince ourselves that after identifying $\widetilde{C}_A^B$, $\widetilde{C}_{A\triangle B}^B$ and $\widetilde{C}_{A\triangle B}^A$ we are left with the right number of coverings, namely

$$\frac{2^{4g} - 3 \cdot 2^{2g} + 2}{2 \cdot 3}. \tag{5}$$

In order to do that we observe that the number of non empty proper subsets of even cardinality of X equals $\sum_{r=1}^{r=g}\binom{2g+2}{2r} = \sum_{r=1}^{r=g}\left(\binom{2g+1}{2r-1}+\binom{2g+1}{2r}\right) = \sum_{k=1}^{k=2g}\binom{2g+1}{k} = (1+1)^{2g+1}-2 = 2\left(2^{2g}-1\right)$. Therefore, the number of the pairs (A,B) which satisfy the conditions $|A|,|B| \leq g+1$ and $A \neq B^C$, if $|A| = g+1$, is $(2^{2g}-1)\times(2^{2g}-1)$. If we further require the condition $A \neq B$, then we see that the number of unordered pairs $\{A,B\}$ subject to these two restrictions is

$$\frac{(2^{2g}-1)\times(2^{2g}-1)-(2^{2g}-1)}{2} = \frac{2^{4g}-3\cdot 2^{2g}+2}{2}.$$

Now, if we identify each triple of coverings $\widetilde{C}_A^B$, $\widetilde{C}_{A\triangle B}^B$ and $\widetilde{C}_{A\triangle B}^A$ we are left with the right number of covers (5).

iii) The degree two morphisms from $\widetilde{C}_A^B$ to the curves $C_{X,A}$, $C_{X,B}$, $C_{X,A\triangle B}$, $C_{A,B}$, $C_{A^C,B}$, C_{A,B^C} and C_{A^C,B^C} whose existence is stated in part iii)are given by

$$\begin{array}{ccc}
(x,y,z,w) & \mapsto & (x,y,z) \\
(x,y,z,w) & \mapsto & (x,y,w) \\
(x,y,z,w) & \mapsto & \left(x,y,\frac{z\cdot w}{\prod_{r\in A\cap B}(x-\mu_r)}\right) \\
(x,y,z,w) & \mapsto & (x,z,w) \\
(x,y,z,w) & \mapsto & \left(x,\frac{y}{z},w\right) \\
(x,y,z,w) & \mapsto & \left(x,z,\frac{y}{w}\right) \\
(x,y,z,w) & \mapsto & \left(x,\frac{y}{z},\frac{y}{w}\right),
\end{array}$$

respectively. The corresponding covering groups are the groups generated by α_1, α_2, $\alpha_1\circ\alpha_2$, α_3, $\alpha_3\circ\alpha_2$, $\alpha_3\circ\alpha_1$ and $\alpha_1\circ\alpha_2\circ\alpha_3$.

iv) Let us prove first that a curve of the form $C_{E,F}$ has genus $p = (|E\cup F|-3)$. Again we regard the curve $C_{E,F}$ as the fibre product $C_E \underset{\mathbb{P}^1}{\times} C_F$ defined by the following commutative diagram

$$\begin{array}{ccc}
C_{E,F} \simeq C_E \underset{\mathbb{P}^1}{\times} C_F & \xrightarrow{\pi_F} & C_F \\
\downarrow \pi_E & & \downarrow h_2 \\
C_E & \xrightarrow{h_1} & \mathbb{P}^1
\end{array}$$

where $C_E : z^2 = \prod_{k\in E}(x-\mu_k)$, $C_F : w^2 = \prod_{j\in F}(x-\mu_j)$ and π_E, π_F, h_1 and h_2 are the obvious projection maps. Now, if $\mu \in \mathbb{P}^1$ is a regular value of h_1 or it is a branching value of both h_1 and h_2 with same branching order (necessarily equals 2) then π_F is unramified over the points of the fiber $(h_1\circ\pi_E)^{-1}(\mu)$ (see e.g. [12], p. 116). Thus branching of π_F may only occur at points $P \in (h_1\circ\pi_E)^{-1}(\mu)$ with $\mu = \mu_l$, $l \in E\setminus F$. On the other hand, the commutativity of the diagram implies that for each $l \in E\setminus F$ the double cover π_F is ramified with order 2 at the two points in $(h_1\circ\pi_E)^{-1}(\mu_l)$. Therefore, if we denote by q the genus of C_F, the Riemann-Hurwitz formula tells us that

$$2p-2 = 2\cdot(2q-2)+2\cdot|E\setminus F| = 2\cdot(|F|-4)+2\cdot|E\setminus F|$$

hence, $p = |E \cup F| - 3$ as was claimed.

Thus, to finish the proof of part iv) of Theorem 1, it is enough to show that at least one of the curves $C_{A,B}$, $C_{A^C,B}$ has genus smaller or equal than $\left[\frac{g}{2}\right] + g - 1$ which, by what has gone before, means that at least one of the integers $|A \cup B|$, $|A^C \cup B|$ is smaller or equal than $\left[\frac{g}{2}\right] + g + 2$.

Now, if $|A \setminus B| \leq \frac{g+1}{2}$ we have

$$|A \cup B| = |B| + |A \setminus B| \leq g + 1 + \left[\frac{g+1}{2}\right] \leq \left[\frac{g}{2}\right] + g + 2,$$

while if $|A \setminus B| > \frac{g+1}{2}$, we have

$$\begin{aligned} |A^C \cup B| &= |A^C| + |A \cap B| = 2g + 2 - |A| + |A \cap B| = 2g + 2 - |A \setminus B| < \\ &< 2g + 2 - \tfrac{g+1}{2} \leq \left[\tfrac{g}{2}\right] + g + 2. \end{aligned}$$

References

[1] E. Bujalance, *A classification of unramified double coverings of hyperelliptic Riemann surfaces*. Arch. Math. **47** (1986), 93-96.

[2] P. Dèbes and M. Emsalem, *On Fields of Moduli of Curves*. Journal of Algebra **211** (1999), 42-56.

[3] H. Farkas, *Unramified double coverings of hyperelliptic surfaces*. J. Analyse Math. **30** (1976), 150-155.

[4] H. Farkas, *Unramified double coverings of hyperelliptic surfaces II*. Proc. AMS. **101**, 3 (1987), 470-474.

[5] Y. Fuertes and G. González-Diez, *Smooth double coverings of hyperelliptic curves*. Proceedings of the III Iberoamerican Congress on Geometry (Salamanca, 2004). Contemp. Math. AMS. To appear.

[6] Y. Fuertes and G. González-Diez, *Fields of moduli and definition of hyperelliptic covers*. Submitted to Archiv der Mathematik.

[7] G. González-Diez, *Variations on Belyi's theorem*. Submitted.

[8] J. Harris, *Algebraic Geometry*. Springer-Verlag. GTM **133** (1992).

[9] R. Horiuchi, *Normal coverings of hyperelliptic Riemann surfaces*, J. Math. Kyoto Univ. **19-3** (1979), 497-523.

[10] C. Machlachlan, *Smooth coverings of hyperelliptic surfaces*. Quart. J. Math. Oxford (2) **22** (1971), 117-123.

[11] H. H. Martens, *Observations of morphisms of closed Riemann surfaces II*, Bull. London Math. Soc. **20** (1988), 253-254.

[12] J. P. Serre, *Topics in Galois theory*. Research Notes in Mathematics, **1**. Jones and Bartlett Publishers, Boston, MA (1992).