



Goppa codes and Tschirnhausen modules

D. Coles and E. Previato

REPORT No. 06, 2006/2007

ISSN 1103-467X

ISRN IML-R- -06-06/07- -SE

Goppa codes and Tschirnhausen modules

Drue Coles

*Department of Mathematics, Computer Science, and Statistics,
Bloomsburg University, Bloomsburg PA 17815, USA
E-mail: dcoles@bloomu.edu*

Emma Previato

*Institut Mittag-Leffler
S-18262 Djursholm, Sweden
Permanent:
Department of Mathematics and Statistics,
Boston University, Boston MA 02215-2411
E-mail: ep@bu.edu*

We review the use of rank-2 vector bundles in error-correcting coding theory, introduce the issue of maximal subbundles in this context and give an explicit example of rank-2 bundles naturally associated to an elliptic subcover of the Klein curve. We also describe how codes on curves (and therefore certain associated rank-2 bundles and their maximal subbundles) can be formulated in terms of adeles.

Keywords: Goppa codes; Vector bundles; Klein curve.

Introduction

Goppa codes (more properly, *geometric* Goppa codes, for the earliest codes introduced by Goppa were still associated with rational functions on the line) provide a fertile area of interaction between coding theory and algebraic geometry, specifically algebraic curves over finite fields. Goppa's original idea is based on the explicit representation of the space of sections of a line bundle over the curve, and deep issues regarding 'curves with many points' and asymptotic bounds on the genus and ramification of towers of curves have been brought up in view of this application, cf. [9] for a brief survey. More recently, rank-2 vector bundles over the curve have been interpreted as error-correcting devices^{4-6,12} but not so explicitly. Their line subbundles of highest possible degree are of particular interest for decoding,

and our goal in this small note is to initiate a study of these objects in the finite field setting.

Higher-rank vector bundles (meaning higher than 1, for line bundles are quite different and better-known objects) come with a concept of “maximal subbundle” for which we refer to the paper [15] although it made earlier appearances (Corrado Segre 1889), since degrees of subbundles can be related to the self-intersection numbers of sections of the bundle projectivized fiberwise into a ruled surface. We restrict attention to rank-2 bundles, and for these, a maximal subbundle is a line subbundle of largest possible degree. There has been enormous activity on the topic of maximal subbundles in algebraic geometry, which we do not reference here, and this prompts our proposed line of research. On one hand, the results of [15] are given over an algebraically closed field of characteristic zero. Even from the pure viewpoint of algebraic geometry, it would be worth extending the study to any characteristic, and in addition, restricting the analysis to finite fields. In the same vein as counting (rational) points on curves and points of Brill-Noether loci, we propose to count the number of maximal subbundles. Here we give but one example. We decided to use the Klein curve X as a test case, in part because it is so full of beautiful unique properties among curves of genus 3 (small enough yet highly non-trivial), and partly because its large number of automorphisms has already made it popular in coding theory. Over the finite field \mathbb{F}_q the Klein quartic has 24 points, hence it attains Serre’s improvement of the Hasse-Weil bound, $|\#X(\mathbb{F}_q) - (q + 1)| \leq g[2\sqrt{q}]$.

As regards the link with error-correcting, a weakness might be that the bundles which correspond to correctable messages are unstable, hence their maximal subbundles have very large degree, too large, roughly speaking, to be interesting in algebraic geometry (except perhaps for the suggestions of [12], to the effect of blowing up unstable strata). Our present result concerns bundles whose maximal subbundles have degree zero, yet we regard it as work towards a potential link with coding theory, for example pursuing the suggestion in [12], that is to look at stable points whose lack of correctability (exceeding the distance from a unique codeword) is not too large, so that error-correction is possible in practice (“For practical purposes this would be almost as good as unique decoding (...) one is then interested in maximal sublinebundles”). Other potential uses of stable bundles are discussed in Section 1.

We adopt three approaches which we believe to be new. The first uses the ideas of [15] to construct all rank-2 bundles with largest-dimensional

varieties of subbundles; part of this approach is the study of quotients of the curve by an automorphism, which was done relatively recently.²¹ The second approach pertains to one of the constructions of [15], and it consists in determining the rank-2 bundle that presents the curve as a triple cover; this approach has the advantage of bringing in another higher-rank bundle, very natural to the situation and proposed by Miranda in [17], the Tschirnhausen module. In the third approach, we formulate Goppa codes in terms of adeles and pseudo-differentials. Adeles provide another way of looking at the rank-2 bundles that appear in connection to codes on curves, a fact used in [6] to investigate an aspect of code construction. For practical implementation of a (de-)coding algorithm, which is one goal of our program, the first step will necessitate an explicit criterion for (maximal) subbundles in terms of adeles. Then, turning to varieties of maximal subbundles, the Tschirnhausen module will provide the multiplicative structure of the covering curve, thus we believe that determining this bundle is the next step in the direction of the ultimate goal.

1. Goppa Codes and rank-2 Vector Bundles

In this section we review the role of vector bundles in error-correction for Goppa codes.

Let X be a smooth projective curve of genus g defined over a finite field k , with a set of k -rational points denoted Q, P_1, P_2, \dots, P_n . Define the divisor $D = P_1 + \dots + P_n$ and choose an integer m so that $n > m > 2g - 2$.

The one-point Goppa code

$$C_L(D, mQ) = \{(f(P_1), \dots, f(P_n)) : f \in \mathcal{L}(mQ)\}$$

has dimension $l(mQ) = m - g + 1$ by the Riemann-Roch theorem. Its minimum distance is at least $n - m$, since any non-zero $f \in \mathcal{L}(mQ)$ can vanish at no more than m of the points P_i .

The space of message functions can be taken more generally as $\mathcal{L}(G)$ for an arbitrary divisor G of degree m supported by k -rational points outside the support of D . However, one-point codes (i.e., G a multiple of a single point) are used in practice to maximize the length n of the code and to simplify the construction of a basis for $\mathcal{L}(G)$.

The dual code to $C_L(D, mQ)$ is also a Goppa code, often described in a more convenient form by defining

$$C_\Omega(D, mQ) = \{(Res_{P_1}(\omega), \dots, Res_{P_n}(\omega)) : \omega \in \Omega_X(mQ - D)\}.$$

The fact that $C_L(D, mQ)$ and $C_\Omega(D, mQ)$ are dual codes is a consequence of the residue theorem, which states the sum of residues of a differential over all points is zero.

Requiring $m > 2g - 2$ makes computing the dimension of $\mathcal{L}(mQ)$ and hence of the code $C_L(D, mQ)$ a simple application of the Riemann-Roch theorem. We actually want $m > 2g$ so that the rational map $\varphi : X \rightarrow \mathbb{P}^{m-g}$ determined by the complete linear system $|mQ|$ is guaranteed to be an embedding.

Since the rows of a generator matrix for $C_L(D, mQ)$ are obtained by evaluating the functions of a basis for $\mathcal{L}(mQ)$ at P_1, \dots, P_n , we can view the columns as points $\varphi(P_i)$ on the curve in \mathbb{P}^{m-g} . These columns are parity checks for the dual code $C_\Omega(D, mQ)$, so a corrupted codeword of the dual is in effect a linear combination of some of the points $\varphi(P_i)$, namely those points at which errors occurred. More explicitly, if H denotes the parity check matrix and $y = (c+e)$ a received word, with codeword $c \in C_\Omega(D, mQ)$ and error vector e , then $Hy = H(c+e) = He$, and the received word $y = e_1 \cdot \varphi(P_1) + \dots + e_n \cdot \varphi(P_n)$ can be viewed as a point in the j -secant variety of the curve in \mathbb{P}^{m-g} , where $j = |\{i : e_i \neq 0\}|$.

We call $A = \sum_{e_i \neq 0} P_i$ the error divisor. The received word $y = c + e$ is said to be correctable if $\deg A < (d-1)/2$, where $d = m - 2g + 2$ is a lower bound on the minimum distance, since in this case the received word is closer to the transmitted codeword c than to any other codeword.

We also consider an error vector (e) as a point in $H^0(X, \Omega_C(mQ - D))^*$, and then identify it with the isomorphism class of a rank-2 extension E of the form

$$0 \rightarrow \mathcal{O}_X \rightarrow E \rightarrow \mathcal{O}_X(D - mQ) \rightarrow 0$$

in a standard way through

$$\begin{aligned} H^0(X, \Omega(mQ - D))^* &\cong H^1(X, \mathcal{O}_X(mQ - D)) \\ &\cong \text{Ext}_{\mathcal{O}_X}(\mathcal{O}_X, \mathcal{O}_X(mQ - D)) \\ &\cong \text{Ext}_{\mathcal{O}_X}(\mathcal{O}_X(D - mQ), \mathcal{O}_X). \end{aligned}$$

Lange and Narasimhan¹⁵ showed that $s(E)(:=\deg E - 2\max(\deg L)$, where L is a subbundle of E) is determined by the smallest integer j such that (e) is contained in the j -secant variety of the curve. Applying their results to our situation and with our notation, we get that A is the error divisor for a correctable word if and only if $\mathcal{O}_X(D - mQ - A)$ is the unique

maximal subbundle of E . This abstract connection between decoding and maximal subbundles of rank-2 extensions was first noticed by Johnsen.¹²

A decoding algorithm based on this idea would determine the rank-2 bundle E corresponding to the syndrome $He = Hy$ of the received word $y = c + e$, in concrete form for instance as a transition matrix, and then compute its unique maximal subbundle $\mathcal{O}_X(D - mQ - A)$. One might then expect to extract the error divisor A and so obtain the error positions (and then the actual error values via simple linear algebra), but with a caveat: we cannot distinguish $\mathcal{O}_X(D - mQ - A)$ from $\mathcal{O}_X(D - mQ - A')$ when $A \sim A'$, so the most that can be guaranteed about the error divisor computed by such an algorithm without additional assumptions (such as the number of errors being less than the gonality of the curve) is that it is linearly equivalent to the true error divisor.

We note that for correctable words, the associated bundle E is necessarily unstable.¹² Still, computing maximal subbundles of *stable* E 's in our extension space may be useful for decoding. If the number of errors in a word y exceeds the error correction capacity of the code, it may happen that there are several codewords of precisely equal Hamming distance from y . In that case, finding maximal subbundles amounts to producing a small list of candidate error divisors, though the issue of linear equivalence discussed above applies here as well. There is a vast coding theory literature on *list decoding*, as it is called.

The study of stable rank-2 bundles on curves with many maximal subbundles defined over a finite field may, in addition to its inherent interest, have a coding theory application, since for particular code parameters the maximum possible number of closest codewords to a given (uncorrectable) word may not be known. This point was discussed in [4], where it was also observed that the recent discovery of families of Goppa codes with exponentially many minimum weight codewords¹ is somewhat related: this result says that for a certain code there is a Hamming sphere of radius d centered at 0 with a huge number of codewords on its boundary; a stable bundle with many maximal subbundles (over the base field) would describe a Hamming sphere of radius greater than d centered at an uncorrectable word with a huge number of codewords on its boundary. One possible way to find rank-2 bundles with lots of maximal subbundles over a finite field is to construct examples with infinitely many in the algebraic closure and then count the ones defined over the base field. We turn to this construction next.

2. The Klein Curve as Cover

In this section, which is composed of old-and-new facts about the Klein curve, we recall some results that were given in characteristic zero in the original references; however, they hold in our more general situation provided the characteristic of the base field k is not 2, 3 or 7 (the divisors of 168 which is the order of $\text{Aut}X$ in any other characteristic), and provided k contains a seventh root of unity, as noted in the text, because the results we use are obtained by algebraic operations defined over the integers.

The two most familiar ways (for a third one cf. 2.4) to write an algebraic equation for Klein's curve X are:

$$s^7 = t(1-t)^2,$$

$$x_1^3 x_2 + x_2^3 x_0 + x_0^3 x_1 = 0.$$

Klein, already in his original definition¹⁴ of the unique curve of genus 3 that has the maximal number of automorphisms, presented it at first as a modular curve, then as a (canonical) plane quartic. This double feature already exhibits the curve as a cover, on one hand, a $(7 : 1)$ cover of \mathbb{P}^1 , on the other, true of every non-hyperelliptic curve of genus 3, as a $(3 : 1)$ trigonal cover in a 1-dimensional manifold way. More surprisingly, [3, VIII.75] shows that the Jacobian of the curve is isomorphic as a complex manifold (without principal polarization) to the product of three elliptic curves; more precisely, using the $(7 : 1)$ cover, Baker computes the period matrix

$$Z = \begin{bmatrix} -\frac{1}{8} + \frac{3\sqrt{7}i}{8} & -\frac{1}{4} - \frac{\sqrt{7}i}{4} & -\frac{3}{8} + \frac{\sqrt{7}i}{8} \\ -\frac{1}{4} - \frac{\sqrt{7}i}{4} & \frac{1}{2} + \frac{\sqrt{7}i}{2} & -\frac{1}{4} - \frac{\sqrt{7}i}{4} \\ -\frac{3}{8} + \frac{\sqrt{7}i}{8} & -\frac{1}{4} - \frac{\sqrt{7}i}{4} & \frac{7}{8} + \frac{3\sqrt{7}i}{8} \end{bmatrix}.$$

As observed in [22], all entries lie in the field generated (over the field k of definition of the curve, $k = \mathbb{Q}$, e.g.) by the character of the representation induced on the differentials of the first kind by the automorphism group of the curve. But another interesting phenomenon occurs: $\text{Jac}(X) = \mathbb{C}^3/\Lambda$, where Λ is the lattice corresponding to $[I \ Z]$, is actually isomorphic to the product of 3 elliptic curves. Indeed, Baker shows that it can be brought by an integral (but not unimodular) transformation into diagonal form:

$$\begin{bmatrix} 1 & 0 & 0 & \frac{1+i\sqrt{7}}{4} & 0 & 0 \\ 0 & 1 & 0 & 0 & 2\frac{1+i\sqrt{7}}{4} & 0 \\ 0 & 0 & 1 & 0 & 0 & 2\frac{1+i\sqrt{7}}{4} \end{bmatrix}.$$

He also remarks that this transformation does not give us an algebraic map from X to an elliptic curve; for that we use recent work,²¹ which gives a bit more: the three elliptic curves are isomorphic as opposed to 2-isogenous as in Baker's decomposition.

We recall some notation and standard facts from [21]. The following three elements generate the automorphism group of X , which is isomorphic to $\mathbb{P}\mathrm{SL}_2(\mathbb{F}_7)$: $\sigma(x_0, x_1, x_2) = (x_1, x_2, x_0)$ of order 3, $\tau(x_0, x_1, x_2) = \left(x_1 + \mu_1 x_2 + \frac{1}{\mu_3} x_0, \mu_1 x_1 + \frac{1}{\mu_3} x_2 + x_0, \frac{1}{\mu_3} x_1 + x_2 + \mu_1 x_0\right)$ of order 2 and $\epsilon(x_0, x_1, x_2) = (x_0, \zeta x_1, \zeta^5 x_2)$ of order 7, where ζ is a primitive 7th root of 1 and we let $\mu_i = \zeta^i + \zeta^{-i}$.

Proposition 2.1.²¹ *The quotient of X by σ^i , $i = 0, 1, 2$ gives three (canonically isomorphic) elliptic curves T_i with Weierstrass equations:*

$$T_i : y^2 + 3\zeta^{4i}xy + \zeta^{5i}y = x^3 - 2\zeta^{2i}x - 3\zeta^{3i}, \quad i = 0, 1, 2,$$

with the $(3 : 1)$ -morphisms $X \rightarrow T_i$ given by $\phi_i(x_1, x_2) = (-w_i, v_i)$ where

$$w_i = x + \zeta^{6i}\frac{1}{y} + \zeta^{4i}\frac{y}{x}, \quad v_i = y + \zeta^{6i}\frac{1}{x} + \zeta^{2i}\frac{x}{y}.$$

Given that the above result is algebraic, we can simply replace $\mathbb{Q}[\zeta]$ by a finite field that contains a seventh root of unity, and keep the notation ζ for a primitive one. In fact, it is quite interesting and non-trivial to find $\mathrm{Aut}X$ over an algebraically closed field of any characteristic. This was accomplished in [30–32]: if the characteristic is $p \neq 3, 7$ the group is again $\mathrm{GL}(3, 2)$. For $p = 3$ (resp. $p = 7$), the group properly contains $\mathrm{GL}(3, 2)$ and is of order 6048 (resp. 672). It is thus not true (as had also been observed earlier) that the Hurwitz bound $84(g - 1)$ holds for the number of automorphisms of a curve of genus g (> 1), if the characteristic is not zero; a bound does exist, modified by the contribution of wild ramification in the Riemann-Hurwitz formula, has degree 4 in g , and it is known which curves attain it.

Our program is now the study of maximal subbundles in positive characteristic. Following the seminal article [15], for a rank-2 (algebraic) vector bundle over a curve X of genus g , we define the numerical invariant:

$$s(E) = \deg E - 2\max(\deg L),$$

where L is a line-subbundle of E . By definition, the degree of E and $s(E)$ have the same parity. It is known that $s(E) \leq g$, and the study in [15] addresses the case $s(E) > 0$ (equivalent to E being a stable bundle) or $s(E) \geq 0$ (semi-stable). The relevant geometric object then is $M(E)$, the subvariety of maximal subbundles. This variety can be identified canonically

with the space of minimal sections of the ruled surface $\mathbb{P}(E)$, minimal in the sense of having smallest self-intersection number. Let us also denote by $M(d)$ the moduli space of stable bundles of rank 2 and degree d over a curve X of genus $g \geq 2$, and by $M(d, s)$ its stratification into locally closed subsets according to the value of the invariant $s(E)$. For generic E , $M(E)$ is smooth and projective and its dimension is described in terms of the rank and degree of E and the genus of X . It has exactly the Chern numbers of an étale cover of the symmetric product $S^n X$, where $n = \dim M(E)$.²⁰ In particular, for the general bundle, $s(E) = g$ if the degree of E has the same parity as the genus, and $s(E) = g - 1$ otherwise. When $s(E) = g$, the variety of maximal subbundles of E is a curve, but when $s(E) = g - 1$, it is generically a finite number of points. It is this number that in the case of positive characteristic could conceivably be smaller, in the case the field is not algebraically closed and the subbundle as a variety is not rational over the field of definition, or perhaps larger, as is the case for the number of automorphisms, due to the wild-ramification contribution in the Riemann-Hurwitz formula, in view of the fact that in [15] a manifold of maximal line subbundles are identified by using covering maps. The number of subbundles does have a topological-degree significance, because of the cited result²⁰ which computes it as a Chern number, 2^g times a Castelnuovo number, but so does the number of inflections of a plane curve; in point of fact, the Klein curve is the “funny curve” in characteristic 3, and all of its points are inflections [11, Exercise IV.2.4]. It is also interesting to note that the dimension of $M(E)$ can jump, as in the following example [20, Remark 1.5]: the general bundle E with trivial determinant on a curve of genus 3 has a finite number of maximal subbundles, $2^3 = 8$, since $s(E) = g - 1$ as we recalled. But $M(E)$ is isomorphic to the curve for the 64 bundles $E = \kappa^{-1} \otimes V$, where κ is a theta characteristic and V is the unique stable rank-2 bundle whose determinant is the canonical bundle, and whose space of sections has the maximal possible $\dim H^0(X, V) = 3$. In fact, in this programmatic note we focus on such ‘richest’ case only, namely $s(E) = g - 1 (= 2$ in our case) and $\dim M(E) = 1$, strictly larger than for general E . In [15] it is determined exactly which E have this property, providing a negative answer to a conjecture of M. Maruyama, to the effect of $\dim M(E)$ being zero for all, not merely general, bundles that have $s(E) \leq g - 1$.

Proposition 2.2 (after 15, Theorem 5.1). *Every degree-2 cover $X \rightarrow T$ of an elliptic curve gives a g -dimensional subvariety of $M(d, 2)$, where d is an even number, for all of whose points E , $\dim M(E) = 1$. If X is of genus 3, any trigonality of X gives a 3-dimensional subvariety of $M(d, 2)$*

for all of whose points E , $\dim M(E) = 1$. For any other $E \in M(d, 2)$, $\dim M(E) = 0$.

We also record the construction of the rank-2 bundles that have a non-generic $\dim M(E)$:

Lemma 2.1 (after 15, Section 5). (i) *If $\pi : X \rightarrow T$ is a $(2 : 1)$ elliptic cover and $g(X) \geq 3$ then to every $L \in \text{Pic}^g T$ where $g = g(X)$ there is associated a vector bundle $E \in M(2, 2)$ on X with $\dim M(E) = 1$. Varying $L \in \text{Pic}^g T$ and twisting the associated E by a line bundle of degree $\frac{d-2}{2}$ on X yields other elements of $M(d, 2)$, while ‘factoring’ by the one-dimensional families of their maximal subbundles finally gives a g -dimensional algebraic family in $M(d, 2)$.* (ii) *To any trigonality $\pi : X \rightarrow \mathbb{P}^1$ of a curve of genus 3 there is associated in a canonical way a vector bundle $E \in M(2, 2)$ on X .*

Proof. (i) Pulling back any rank-2 bundle F on the elliptic curve with $s(F) = 1$ as well as the family of line subbundles of appropriate degree gives the examples. They can be described geometrically: the embedding $H^0(T, L) \rightarrow H^0(X, \pi^*L)$ (which is of codimension 1) defines a point in $\mathbb{P}^g = \mathbb{P}(H^0(X, \pi^*L))$ which is not on the image of X . This point can be interpreted as a non-split exact sequence on X whose central element is a vector bundle of rank 2 with $s(E) = 2$ and $\det E = \pi^*L \otimes K_X^{-1}$, where K_X is the canonical divisor of X . Projection from the point has degree 2 on the image of X and represents the 2-secants of X through that point, so the maximal subbundles are represented by the points of the elliptic curve embedded in the hyperplane covered by the projection, except possibly the projection of the singular point of the image of X . (ii) Here the bundle E is the middle term of the extension given by the embedding $H^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(2)) \rightarrow H^0(X, \pi^*\mathcal{O}_{\mathbb{P}^1}(2))$ so $\det E = \pi^*\mathcal{O}_{\mathbb{P}^1}(2) \otimes K_X^{-1}$ and again the 3-dimensional family of bundles is parametrized by $\text{Pic}^{d-2/2} X$ plus the trigonalities minus 1 for the maximal subbundles, which correspond to the trisecant lines of the embedded curve in \mathbb{P}^3 which go through the extension point. \square

This lemma together with the proof (which we do not produce) that no other bundle exhibits the jump phenomenon, proves Proposition 2.2.

We are next faced with the task of giving (in an algebraic and explicit way) a $(2 : 1)$ elliptic subcover of X or a trigonal rationality. We begin with the latter. Rather than take the approach of [7] and determine the quotient of the Klein curve under all cyclic subgroups of automorphisms, we use the interesting analysis proposed in [18], by addressing the additional

question: given a trigonality obtained by projecting a smooth plane quartic to a line from a point on it, when is this cover Galois? We take this point of view because we find it potentially interesting to give an addendum to Kowalevski's early result: she proved that a plane quartic is a $(2 : 1)$ cover of an elliptic curve if and only if four of its 28 bitangents are concurrent, as we recall in Prop. 2.4.

The gonality of a curve is the smallest possible degree of the function field of the curve over a rational field of one variable. We now adapt statements from [18], which assumes the field of definition k to be algebraically closed of characteristic zero. For our purposes we assume that all maps are defined over k in case k isn't algebraically closed (such as a finite field). The Klein curve is not hyperelliptic, hence it is trigonal. For a plane smooth m -gonal curve of degree d the gonality is $d - 1$ and any extension $K/k(t)$, where K is the function field of the curve and $k(t)$ is any rational field of degree 1, corresponds to an $(m : 1)$ projection from a point of the curve onto a line.¹⁸ In [18], the authors determine the following objects pertaining to a smooth quartic (such as our Klein curve – in fact, their worked-out example is the Fermat curve, whose automorphism group³³ has order 96): for $P \in X$, the projection of X from P to a line is a degree-3 cover, and the Galois group as well as the genus of the corresponding cover are calculated, together with the (finite) number of points P for which the cover is Galois.

Proposition 2.3 (after 18, Theorem 2.1). *For any smooth plane quartic X and any point $P \in X$, the projection from P to a line corresponds to a field extension that does not depend on the line, and if we call $g(P)$ the genus of the smooth curve whose function field is the Galois closure of the field extension corresponding to the projection and P a Galois point when the extension is Galois, then: $g(P) = 3, 6, 7, 8, 9$, or 10 , with $g(P) = 10$ for the general point, with Galois group isomorphic to S_3 . The number of Galois points can be $0, 1$, or 4 , and it is zero for a general quartic.*

In [18], part of the criterion for P to be a Galois point is that P be a 2-inflection point. In particular, for the Klein curve, none exists, since the inflections are all distinct and comprise the 24 Weierstrass points, so none of the trigonal covers is Galois.

Similar issues are treated in [18] for the case $P \notin X$, there being more cases to analyze and slightly less complete results. The Klein curve does admit a double cover to an elliptic curve. Indeed, as noted in [14], there are 21 subgroups of order 2 of $\text{Aut} X$, each corresponding to a collineation; the centers of projection give $(4 : 1)$ maps of X to a line which factor

through an elliptic curve, the ramification given by the four bitangents to X through the center (each bitangent contains three centers so that there are $\frac{21 \times 4}{3} = 28$ bitangents). We note however that none of the 4-gonal covers given by projection from $P \notin X$ of the Klein (unlike the Fermat!) quartic are Galois either; the 21 elliptic subfields of $K(X)$ fixed by involutions are one orbit under $\text{Aut}X$.¹⁶

It seems worth recalling Kowalewski's criterion for a smooth plane quartic to be a $(2 : 1)$ elliptic cover, which again is proved in characteristic zero. Her proof was analytic, a contribution to the theory of reduction, part of her dissertation supervised by Weierstrass. An algebraic proof is given in [8], as part of the properties of Weierstrass points of curves with involution.

Proposition 2.4 (Chap. III, Art. 71, 72, 76 in [3]). *A canonically embedded plane curve of genus 3 admits a $(2 : 1)$ cover to an elliptic curve if and only if four of its bitangents are concurrent, equivalently in suitable coordinates it has an equation:*

$$(z^2 - \phi_2)^2 = 4xy(ax + by)(cx + dy),$$

with ϕ_2 a homogeneous form of degree 2 in x, y .

Here the bitangents are patently represented by the linear forms $x, y, ax + by$ and $cx + dy$, whose cross-ratio is an invariant of the elliptic curve. Note the analogy with genus one: an elliptic curve is the Fermat curve if and only if it can be represented as a plane cubic with three concurrent bitangents, the projection from their common point being Galois. As recalled above, Klein's curve can be written in this way by virtue of its automorphisms of order two. An actual geometric model of the elliptic curve together with the $(2 : 1)$ projection can be found by embedding X in \mathbb{P}^3 via the divisor of degree 6 that pulls back an $L \in \text{Pic}^3 T$, precisely as in Lemma 2.1, obtaining an extension E to be viewed as a point in \mathbb{P}^3 and projecting the image of X from that point to a plane; Baker (*loc. cit.* in Prop. 2.4) states this fact concretely presenting the image of X as a space sextic with equations:

$$z^2 - \phi_2 = xt, \quad xt^2 = 4y(ax + by)(cx + dy),$$

as obtained by sending $[x, y, z] \mapsto [x, y, z, t] \sim [1, y/x, z/x, (z^2 - \phi_2)/x^2]$ by the pole-divisor map of $3P_1 + 3P_2$, P_1 and P_2 being the points of contact of the bitangent $x = 0$.

Remark. One subtle issue that we do not address in this note is the following. A classical result reprised and refined in [13] says that if an abelian surface has more than two elliptic subgroups, then it has infinitely many;

[13] shows also that it has finitely many ones for each bounded degree (the degree can be taken to be the intersection number with any fixed ample divisor). In our case, we would ask how many genuinely distinct (elliptic) subcovers the Klein curve has, in particular over each finite field. We note that much current work is devoted to classifying subcovers of Hermitian curves (of key interest in the area of Goppa codes), for example in [7] a classification is given of the quotients of Hermitian curves by all prime-order automorphisms. For the genus-2 case, an explicit detection of isogenous/isomorphic degree-2 and degree-3 subcovers, as well as partial results for higher degree, is given in [24–27].

Summary. Let X be the Klein curve. For each fixed determinant, the rank-2 bundles $E \in M(2, 2)$ with $\dim M(E) = 1$ correspond to a given elliptic-hyperelliptic map or trigonality. The 64 points E mentioned above that exhibit the jump phenomenon as regards $\dim M(E)^{20}$ have fixed (even-degree) determinant. It follows from the above construction that each map gives rise to one bundle; the 21 subgroups of order 2 of $\text{Aut} X$ come with three maps each (each group of 4 concurrent bitangents gives an elliptic curve and each bitangent contains three centers), so we recover the $64 = 21 \times 3 + [\text{one trigonality}]$ bundles of [20], on which $\text{Aut} X$ acts by permutations. To compute the number of these bundles over a finite field \mathbb{F}_q , one of our goals, first we fix a determinant of degree d that is an element of $\text{Pic}^d X(\mathbb{F}_q)$ (there exists one for each degree, and the number of distinct ones is independent of the degree [19, Chap. 3]), then there are as many bundles (semistable and with that determinant), with ‘too many subbundles’, as there are points of order 2 in $\text{Pic}^0 X(\mathbb{F}_q)$, found¹⁹ (since the Jacobian splits) by splitting the characteristic p in $\mathbb{Z}[\sqrt{-7}]$.

Example. Consider the Klein curve X defined by $x_1^3 x_2 + x_2^3 x_0 + x_0^3 x_1 = 0$ over $\mathbb{F}_8 = \mathbb{F}_2[\beta]/(\beta^3 + \beta + 1)$. Since the characteristic is 2, we cannot expect the same situation as in characteristic zero, in fact there are no odd theta-characteristics since the tangent line at any point is an inflectionary tangent. However, the maximal-subbundle geometry survives. Fix coordinates so that on the line at infinity $z = 0$, parametrized as $[a, b]$, $P_\infty = [1, 0]$ and let $\pi : X \rightarrow \mathbb{P}^1$ be the projection from $Q_3 = [0, 0, 1]$ to the line at infinity, so that $2P_\infty$ pulls back to $6Q_1$, where $Q_1 = [1, 0, 0]$.

Let $\varphi : \mathbb{P}^1 \rightarrow \mathbb{P}^2$ denote the embedding $[a, b] \mapsto [1, a/b, a^2/b^2]$. The divisor map $\varphi_{6Q_1} : X \rightarrow \mathbb{P}^3$ that makes the following diagram commute is given by $[a, b, c] \mapsto [1, a/b, a^2/b^2, ab/c^2]$.

The injection $H^0(\mathbb{P}^1, 2P_\infty) \xrightarrow{\pi^*} H^0(X, 6Q_1)$ corresponds to the point

$(e) = [0, 0, 0, 1] \in \mathbb{P}^3$. The projection p in the commutative diagram

$$\begin{array}{ccc} \mathbb{P}^3 - \{e\} & \xrightarrow{p} & \mathbb{P}^2 \\ \varphi_{6Q_1} \uparrow & & \uparrow \varphi \\ X & \xrightarrow{\pi} & \mathbb{P}^1 \end{array}$$

is $[a, b, c, d] \xrightarrow{p} [a, b, c]$. The points $\varphi(\mathbb{P}^1)$ parametrize the trisecant lines of $\varphi_{6Q_1}(X)$ containing (e) .

Choose a point $Q = [a, 1]$ on the projective line, $a \in \mathbb{F}_8^*$. Then the three points $[a, 1, *] \in \pi^{-1}(Q)$ are mapped by φ^* to a trisecant line containing (e) . Any two of these points determine a maximal subbundle of E , the rank-2 bundle corresponding to (e) . We can compute

$$\pi^{-1}(Q) = \{[a, 1, a^3\beta], [a, 1, a^3\beta^2], [a, 1, a^3\beta^4]\}$$

and it follows that E has $7 \cdot \binom{3}{2} = 21$ maximal subbundles that are rational over \mathbb{F}_8 , namely those of the form

$$\mathcal{O}_X([a, 1, a^3\beta^i] + [a, 1, a^3\beta^j])$$

where $a \in \mathbb{F}_8^*$ and $(i, j) \in \{(1, 2), (1, 4), (2, 4)\}$.

3. The Tschirnhausen Module of the Cover

In [17], the author sets out to “develop the foundations of the theory of triple coverings in algebraic geometry”, working on an algebraically closed field of characteristic unequal to 2 or 3; his result in summary:

A triple cover of an irreducible variety Y is determined by a locally free rank-2 \mathcal{O}_Y -module E and a map $\Phi : S^3 E \rightarrow \wedge^2 E$, and conversely.

It may be worthwhile to determine this rank-2 bundle in our situation, in view of what we described above, even when the cover does not pertain to one of the exceptional rank-2 bundles over the Klein curve. We believe that the object introduced by Miranda has not yet been widely used while being potentially useful in coding theory. We restrict attention to one of the above triple covers $X \rightarrow T$, where X is the Klein curve, or one of the trigonalities $X \rightarrow \mathbb{P}^1$; we denote the target by Y in either case.

Definition 3.1. E is the Tschirnhausen module of \mathcal{O}_X over \mathcal{O}_Y , namely the direct summand in $\mathcal{O}_X = \mathcal{O}_Y \oplus E$ consisting of the functions $a \in \mathcal{O}_X \setminus \mathcal{O}_Y$ whose minimal polynomial over \mathcal{O}_Y has trace zero.

The name given by Miranda to the module refers to the Tschirnhausen transformation,²⁹ used in several instances of reduction of degree of alge-

braic equations; another important example, the quintic equation, is also related to curves.¹⁰ The conventional way to perform a Tschirnhausen transformation is to allow a substitution $y = x^m + r_{m-1}x^{m-1} + \dots + r_1x + r_0$, in order to simultaneously eliminate (by using the r 's as free parameters) intermediate terms of any n th- (say) degree equation^a. In the case of a quintic, to bring it to Bring-Jerrard form: $x^5 + ax + b$, with $y = \sum_{j=0}^4 a_j x^j$ one has to solve three equations of degrees 1, 2, and 3 in the coefficients of the original equation. In this case¹⁰ it is possible to intersect suitable hypersurfaces in \mathbb{P}^4 and find solutions by solving equations of degree at most four. Bring's curve is then of genus four and can be explicitly uniformized as it possesses sufficiently many automorphisms, in particular a $(12 : 1)$ (Galois) cover to an elliptic curve. This provides a solution to the general quintic in terms of modular forms of weight -2 .

With this motivation, Miranda defines the Tschirnhausen module of the triple cover $X \rightarrow Y$ to be the submodule E in the decomposition of local k -algebras (where k is an algebraically closed field of characteristic unequal to 2 or 3), or sheaves, $\mathcal{O}_X = \mathcal{O}_Y \oplus E$ consisting of the elements $a \in \mathcal{O}_X \setminus \mathcal{O}_Y$ whose minimal polynomial is trace free.

In our situation, for the map in Prop. 2.1 given explicitly as above, the module consists of the elements $\frac{2}{3}a - a^\sigma - a^{\sigma^2}$, for all a in the function field of X that are not σ -invariant; is is enough to take $a = x$, y to span the module and the map σ is given explicitly: $x \mapsto y \mapsto z \mapsto x$ so x projects to $\frac{2}{3}x - y - z$ and y to $\frac{2}{3}y - z - x$. This would provide actual equations for the corresponding divisor; however, we give a more theoretic way to identify it.

Miranda computes the ramification and branch locus of the triple cover: the branch locus in Y is a divisor whose associated line bundle is $(\wedge^2 E)^{-2}$ so by the Riemann-Hurwitz formula (which has no inertia components under the assumptions we made on the characteristic), $2g(X) - 2 = 3(2g(Y) - 2) + \text{degree}(\wedge^2 E)$. In conclusion, in our case E has degree 4. Atiyah² gave a description of all the semistable bundles over an elliptic curve, but we are further restricted in our situation: the cover is by construction a Galois cover, and Miranda shows that E splits into the sum of two eigenline bundles: $f_*\mathcal{O}_X = \mathcal{O}_Y \oplus L^{-1} \oplus M^{-1}$, $E = L^{-1} \oplus M^{-1}$, where L^{-1} , M^{-1} are the eigenspaces for σ , σ^2 . Since there are exactly two σ -fixed points on X , namely $p_1 = [1, \epsilon, \epsilon^2]$ and $p_2 = [1, \epsilon^2, \epsilon]$ where ϵ is a primitive third root of 1, the bundles L and M are $\mathcal{O}(-2p_i)$.

^aWe acknowledge this clear and clever exemplification due to Titus Pierzas III posted on the web: A New Way To Derive The Bring-Jerrard Quintic in Radicals, www.geocities.com/titus_piezas/Tschirnhausen.pdf.

The trigonality, however, is never Galois as we saw. To compute the Tschirnhausen module which, being a rank-2 bundle over \mathbb{P}^1 , decomposes into $\mathcal{O}(n) \oplus \mathcal{O}(m)$, we refer to [17, Section 9] for an argument, essentially based on the Riemann-Hurwitz formula, yielding $n = -2$ and $m = -3$.

Summary. The Tschirnhausen module for the possible triple covers of the Klein curve to the elliptic curve T that admits multiplication by a primitive root of 7 as an endomorphism, or to the projective line, are respectively

$$\mathcal{O}_E(-2p_1) \oplus \mathcal{O}_E(-2p_2), \quad \mathcal{O}_{\mathbb{P}^1}(-2) \oplus \mathcal{O}_{\mathbb{P}^1}(-3).$$

4. Goppa Codes and Adeles

We observe in this section that Goppa codes can also be formulated in terms of adeles and pseudo-differentials, and in this setting the duality between $C_L(D, mQ)$ and $C_\Omega(D, mQ)$ can be established without direct appeal to the residue theorem or the analogous result for pseudo-differentials.

An introduction to adeles and pseudo-differentials can be found in the chapters on the Riemann-Roch theorem in the books by Moreno [19, Chap. 2] and Stichtenoth [28, Chap. I.5]. Basic definitions and results needed for our purposes are reviewed below.

4.1. Adeles and pseudo-differentials

Let K denote the function field of the curve X , and k the field of constants. In this subsection, D denotes an arbitrary divisor. As usual, $l(D) = \dim_k \mathcal{L}(D)$, where $\mathcal{L}(D)$ is the Riemann-Roch space of D . By Riemann's theorem, $l(D) \geq \deg D - g + 1$, and the *index of speciality* is $i(D) = l(D) - \deg D + g - 1$.

An *adele*^b is a mapping $\alpha : X \rightarrow K$ that associates a function α_P to every point $P \in X$ in such a way that $\alpha_P \in \mathcal{O}_P$ for all but finitely many points P . It is convenient to define the order of an adele α at a point P by $\text{ord}_P(\alpha) = \text{ord}_P(\alpha_P)$.

The set A of all adeles is called the *adele space*. We can add adeles componentwise: the P -component of $\alpha + \alpha'$ is $(\alpha + \alpha')_P = \alpha_P + \alpha'_P$, which is again an adele. Componentwise multiplication also makes sense, turning A into a ring. More to the point for our purposes, it is a vector space over

^bSome authors use the term *repartition* or *pre-adele* for what is here called an adele, reserving the term adele for when the functions α_P are allowed to lie in the completion of K with respect to the valuation ord_P .

k , and the k -subspace $A(D)$ for a divisor D is defined in analogy to $\mathcal{L}(D)$,

$$A(D) = \{\alpha \in A : \text{ord}_P(\alpha) + \text{ord}_P(D) \geq 0 \text{ for every } P \in X\}.$$

An embedding $K \hookrightarrow A$ is obtained by identifying $f \in K$ with the adele whose every component is equal to f . In particular, let f/Q for $Q \in X$ denote the adele $\alpha \in A$ defined by

$$\alpha_P = \begin{cases} f & : P = Q. \\ 0 & : P \neq Q. \end{cases}$$

For a divisor D , $A(D) + K$ is an infinite dimensional k -subspace of A , but the quotient space $A/(A(D) + K)$ is finite dimensional, in fact equal to the index of specialty $i(D)$ of D . This fact is implied by the canonical isomorphism (see [23, Prop. II.3], for example)

$$H^1(C, \mathcal{O}_X(D)) \cong \frac{A}{A(D) + K}$$

and can also be established directly, without cohomological arguments.¹⁹ The next proposition records this fact for ease of reference below.

Proposition 4.1. *With the given notation, $\dim_k A/(A(D) + K) = i(D)$.*

A *pseudo-differential* (also called a *Weil differential*) is a k -linear map $\omega : A \rightarrow k$ vanishing on $A(D) + K$ for some divisor D . Note that if ω_i vanishes on $A(D_i) + K$ ($i = 1, 2$) then $\omega_1 + \omega_2$ vanishes on $A(D) + K$ for any divisor D with $D \leq D_i$ ($i = 1, 2$). With scalar multiplication defined in the obvious way, the space of all pseudo-differentials becomes a vector space over k , which we denote by $\Omega_{K/k}^s$ following Moreno.¹⁹ The subspace

$$\Omega_{K/k}^s(D) = \{\omega \in \Omega_{K/k}^s : \omega \text{ vanishes on } A(D) + K\}$$

has dimension $i(D)$ by Prop. 4.1. Stichtenoth works out in full detail the correspondence between differentials and pseudo-differentials [28, Chap. IV]. Here we note only that for a given pseudo-differential ω there is a unique divisor W of smallest possible degree with the following property: if ω vanishes on $A(F) + K$ for some divisor F , then $F \leq W$. As expected, W is also the divisor of the corresponding differential.

4.2. Goppa codes and adeles

As in subsection 4.1, let $D = P_1 + \cdots + P_n$, where the P_i are k -rational points. Fix another k -rational point Q ($Q \neq P_i$) and an integer m with

$n > m > 2g - 2$. Let $n' = n + g - 1$ and $D_i = D - P_i$ for $1 \leq i \leq n$. Choose $f_i \in \mathcal{L}(n'Q - D_i)$ so that

$$f_i(P_j) = \begin{cases} 1 & : i = j. \\ 0 & : i \neq j. \end{cases} \quad (1)$$

Such functions f_i exist since $l(n'Q - D_i) \geq 1$. Also, $l(n'Q) = n$ and the f_i are linearly independent, so they form a basis for $\mathcal{L}(n'Q)$. Now consider the linear code

$$C = \{(c_1, \dots, c_n) \in k^n : \text{ord}_Q(c_1 f_1 + \dots + c_n f_n) \geq -m\}.$$

The distance and dimension of C are easy to compute. Choose a non-zero codeword (c_1, \dots, c_n) and let $f = \sum_i c_i f_i$. Define $I \subset \{1, \dots, n\}$ so that $c_i = 0 \leftrightarrow i \in I$, and note that $f(P_i) = 0$ for every $i \in I$. Now since $\text{ord}_Q(f) \geq -m$, we know that f has at most m zeros. This means that $|I| \leq m$, so (c_1, \dots, c_n) is non-zero in at least $n - m$ positions. As for the dimension, $f \in \mathcal{L}(mQ)$ by definition, so $\dim_k C = l(mQ) = m - g + 1$.

In fact, $C = C_L(D, mQ)$. To see this, note that for $f = \sum_i c_i f_i \in \mathcal{L}(mQ)$ we have $f(P_i) = c_i \cdot f_i(P_i) = c_i$. In other words, a codeword $(c_1, \dots, c_n) \in C$ is obtained by evaluating some $f \in \mathcal{L}(mQ)$ at the points P_i .

Fix a local parameter t at Q . Expanding each f_i around Q , we can write

$$f_i = \sum_{j=-n'}^{\infty} c_{i,j} \cdot t^j$$

with uniquely determined coefficients $c_{i,j} \in k$. A parity check matrix H for the code can be constructed using these coefficients: the i -th column is the vector of coefficients in the expansion of f_i up to (and including) the $t^{-(m+1)}$ term. The kernel of this matrix consists of linear combinations of the functions f_i with at most m poles at Q , that is to say, codewords.

We now proceed to interpret the parity check matrix H in terms of pseudo-differentials by way of the following two lemmas.

Lemma 4.1. *Letting t denote a local parameter at Q , the set $\mathcal{B} = \{t^{-i}/Q : m < i \leq n'\}$ is a basis for $A/(A(mQ - D) + K)$ as a vector space over k .*

Proof. Consider first an arbitrary adèle α . By the Strong Approximation Theorem,²⁸ there is a function $g \in K$ satisfying $\text{ord}_{P_i}(\alpha - g) > 0$ for each point P_i in the support of D , and $\text{ord}_P(\alpha - g) \geq 0$ for every other point of the curve except Q . It follows that $\alpha \equiv (\alpha_Q - g)/Q$ modulo $A(mQ -$

$D) + K$. In particular, $A/(A(mQ - D) + K)$ has a basis consisting of adeles everywhere zero except at Q .

If the pole order of $f \in K$ at Q is at most m , then $f/Q \in A(mQ - D)$. On the other hand, if f has more than n' poles at Q , say r poles, there is a non-zero $g \in \mathcal{L}(rQ - D)$ with $\text{ord}_Q(f - g) > -r$, and $f/Q - g \in A(mQ - D)$. This implies that if $f/Q \neq 0$ then $-n \leq \text{ord}_Q(f) < -m$.

We have established that there is a basis for $A/(A(mQ - D) + K)$ consisting of adeles of the form f/Q with $-n \leq \text{ord}_Q(f) < -m$. The basis has size $i(mQ - D) = |\mathcal{B}|$ by Prop. 4.1, and we clearly can obtain \mathcal{B} from it by a linear transformation. \square

Lemma 4.2. *With the functions f_i as defined in (1), we have $1/P_i \equiv f_i/Q \pmod{A(mQ - D) + K}$ for $1 \leq i \leq n$.*

Proof. Define $\alpha_i \in A(mQ - D)$ by

$$(\alpha_i)_P = \begin{cases} 0 & : P = Q. \\ f_i + 1 & : P = P_i. \\ f_i & : \text{otherwise.} \end{cases}$$

Then $\alpha_i - f_i = 1/P_i - f_i/Q$, so $1/P_i \equiv f_i/Q$ as claimed. \square

A pseudo-differential $\omega \in \Omega_{K/k}^s(mQ - D)$ is determined by a vector

$$\hat{a} = (a_{m+1}, a_{m+2}, \dots, a_{n'}) \in k^{n'-m}$$

describing the action of ω on elements of \mathcal{B} ; i.e., $\omega : t^{-i}/Q \mapsto a_i$. In particular, $\omega(1/P_i)$ can be computed as the inner product of \hat{a} and the i -th column of H , the parity check matrix for $C_L(D, mQ)$. And since a parity check matrix of a code is a generator matrix for its dual, we can define the dual code to $C_L(D, mQ)$ purely in terms of adeles by

$$C(D, mQ)^\perp = \left\{ (\omega(1/P_1), \dots, \omega(1/P_n)) : \omega \in \Omega_{K/k}^s(mQ - D) \right\}$$

We close the circle by noting that from the correspondence between pseudo-differentials and differentials it can be shown that an arbitrary pseudo-differential maps the adele $1/P$ (for any $P \in X$) to the residue at P of the corresponding differential. Consequently, $C_\Omega(D, mQ)$ as defined in the first section is dual to $C_L(D, mQ)$, which we have established using the theory of adeles and pseudo-differentials and without appeal to the residue theorem. As noted earlier, since our extension space is isomorphic to $H^1(X, \mathcal{O}_X(mQ - D))$, it can be identified with the adelic space

$A/(A(mQ - D) + K)$. One angle from which we propose to study rank-2 extensions and their maximal subbundles over finite fields is through this connection to adeles. We showed that every adele is equivalent, modulo $A(mQ - D) + K$, to an adele of the form f/Q ; in fact, each such f determines a transition function for a rank-2 bundle in our space of extensions.

Acknowledgements

Both authors are thankful for partial research-travel support under NSA grant MDA904-03-1-0119 [*any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Security Agency*]. E.P. is currently benefiting from the scholarly atmosphere of the Institut Mittag-Leffler in the *Moduli Spaces* program and is deeply grateful for the hospitality extended to her.

References

1. A. Ashikhmin, A. Barg, S. Vladut, Linear codes with exponentially many light vectors, *J. Combin. Theory Ser. A* **96** (2001), no. 2, 396-399.
2. M.F. Atiyah, Vector bundles over an elliptic curve, *Proc. London Math. Soc.* (3) **7** (1957), 414-452.
3. H.F. Baker, *An introduction to the theory of multiply-periodic functions*. University Press XVI, Cambridge, 1907.
4. T. Bouganis and D. Coles, A geometric view of decoding AG codes, in *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 2003)*, pp. 180-190, Lecture Notes in Comput. Sci., **2643**, Springer, Berlin, 2003.
5. D. Coles, Vector bundles and codes on the Hermitian curve, *IEEE Trans. Inform. Theory* **51** (2005), no. 6, 2113-2120.
6. D. Coles, On constructing AG codes without basis functions for Riemann-Roch spaces, in *Lecture Notes in Comput. Sci.*, **3857**, Springer, 2006, pp. 108-117.
7. A. Cossidente, G. Korchmáros and F. Torres, Curves of large genus covered by the Hermitian curve, *Comm. Algebra* **28** (2000), no. 10, 4707-4728.
8. H.M. Farkas and I. Kra, Branched two-sheeted covers, *Israel J. Math.* **74** (1991), no. 2-3, 169-197.
9. G. van der Geer, Curves over finite fields and codes, in *European Congress of Mathematics, Vol. II (Barcelona, 2000)*, pp. 225-238, Progr. Math., **202**, Birkhäuser, Basel, 2001.
10. M.L. Green, On the analytic solution of the equation of fifth degree, *Compositio Math.* **37** (1978), no. 3, 233-241.
11. R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, No. **52**. Springer-Verlag, New York-Heidelberg, 1977.
12. T. Johnsen, Rank two bundles on algebraic curves and decoding of Goppa codes, *Int. J. Pure Appl. Math.* **4** (2003), no. 1, 33-45.

13. E. Kani, Elliptic curves on abelian surfaces, *Manuscripta Math.* **84** (1994), no. 2, 199–223.
14. F. Klein, On the order-seven transformation of elliptic functions, in *Math. Sci. Res. Inst. Publ.*, **35**, *The eightfold way*, pp. 287–331, Cambridge Univ. Press, Cambridge, 1999.
15. H. Lange and S. Narasimhan, Maximal subbundles of rank two vector bundles on curves, *Math. Ann.* **266** (1983), no. 1, 55–72.
16. K. Magaard, S. Shpectorov and H. Völklein, A GAP package for braid orbit computation and applications, *Experiment. Math.* **12** (2003), no. 4, 385–393.
17. R. Miranda, Triple covers in algebraic geometry, *Amer. J. Math.* **107** (1985), no. 5, 1123–1158.
18. K. Miura and H. Yoshihara, Field Theory for Function Fields of Plane Quartic Curves, *J. Algebra* **226** (2000), no. 1, 283–294.
19. C. Moreno, *Algebraic Curves Over Finite Fields*, Cambridge Univ. Press, 1991.
20. W.M. Oxbury, Varieties of maximal line subbundles, *Math. Proc. Cambridge Philos. Soc.* **129** (2000), no. 1, 9–18.
21. D.T. Prapavessi, On the Jacobian of the Klein curve, *Proc. Amer. Math. Soc.* **122** (1994), no. 4, 971–978.
22. H.E. Rauch and J. Lewittes, The Riemann surface of Klein with 168 automorphisms, in *Problems in Analysis (papers dedicated to Salomon Bochner, 1969)*, Princeton Univ. Press, Princeton, NJ, 1970, pp. 297–308.
23. J.-P. Serre, *Algebraic Groups and Class Fields*, Springer Graduate Texts in Mathematics, 1988.
24. T. Shaska, Curves of genus 2 with (N, N) decomposable Jacobians, *J. Symbolic Comput.* **31** (2001), no. 5, 603–617.
25. T. Shaska, Genus 2 curves with $(3, 3)$ -split Jacobian and large automorphism group, in: *Algorithmic number theory* (Sydney, 2002), 205–218, Lecture Notes in Comput. Sci., **2369**, Springer, Berlin, 2002.
26. T. Shaska, Genus 2 fields with degree 3 elliptic subfields, *Forum Math.* **16** (2004), no. 2, 263–280.
27. T. Shaska and H. Völklein, Elliptic subfields and automorphisms of genus 2 function fields, in: *Algebra, arithmetic and geometry with applications* (West Lafayette, IN, 2000), 703–723, Springer, Berlin, 2004.
28. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag 1993.
29. E.W. von Tschirnhaus, Acta Eruditorium (1683).
30. S. Tufféry, Automorphismes d’ordre 3 et 7 sur une courbe de genre 3, *Exposition. Math.* **11** (1993), no. 2, 159–162.
31. S. Tufféry, Les automorphismes des courbes de genre 3 de caractéristique 2, *C. R. Acad. Sci. Paris Sér. I Math.* **321** (1995), no. 2, 205–210.
32. S. Tufféry, Déformations de courbes avec action de groupe. II, *Forum Math.* **8** (1996), no. 2, 205–218.
33. P. Tzermias, The group of automorphisms of the Fermat curve, *J. Number Theory* **53** (1995), no. 1, 173–178.