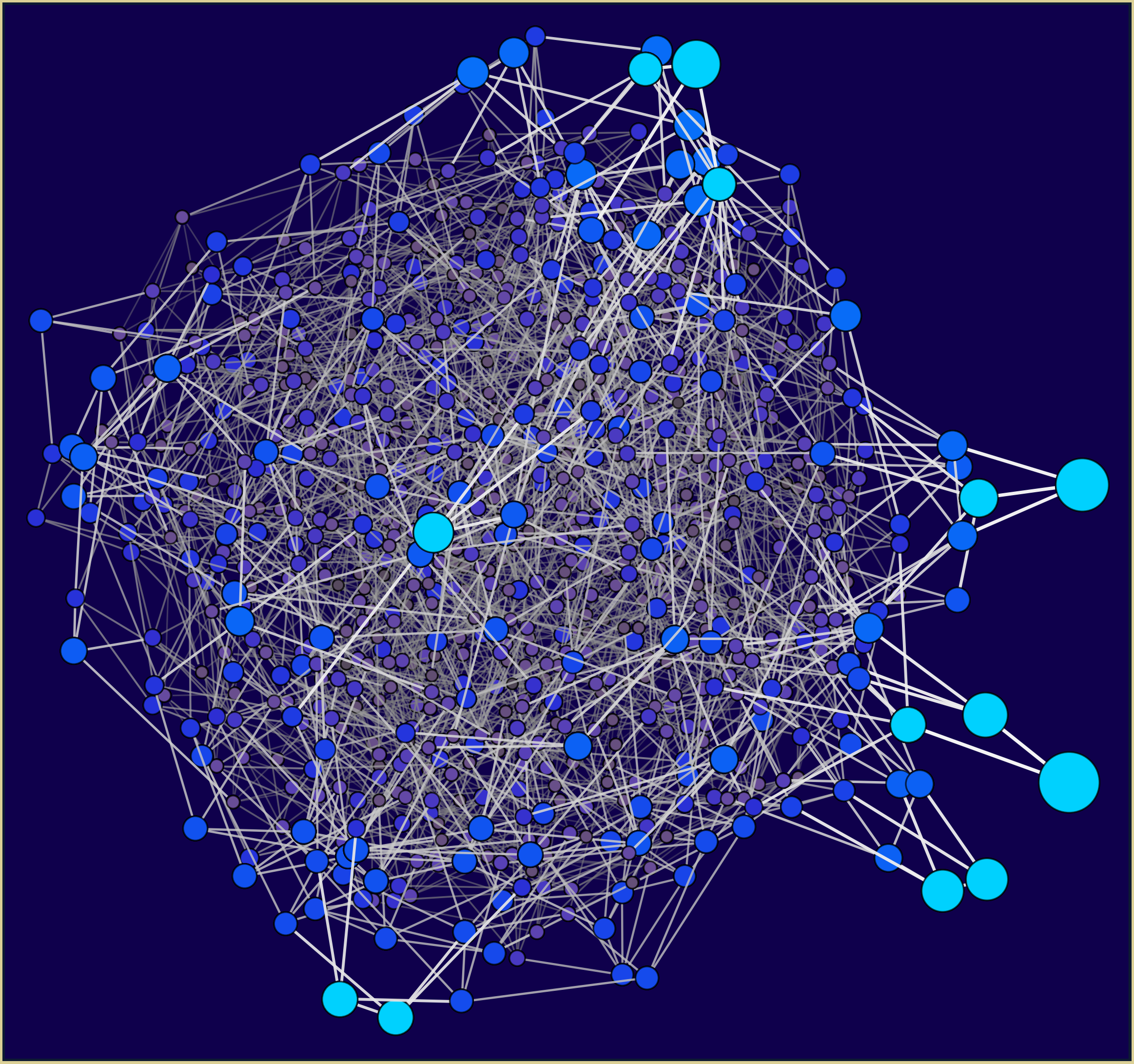
THE OPEN BOOK SERIES 4

# ANTS XIV
Proceedings of the Fourteenth
Algorithmic Number Theory Symposium

## Lifting low-gonal curves for use in Tuitman's algorithm

Wouter Castryck and Floris Vermeulen



msp

THE OPEN BOOK SERIES **4** (2020)
**Fourteenth Algorithmic Number Theory Symposium**
https://doi.org/10.2140/obs.2020.4.109

# Lifting low-gonal curves for use in Tuitman's algorithm

Wouter Castryck and Floris Vermeulen

Consider a smooth projective curve $\overline{C}$ over a finite field $\mathbb{F}_q$, equipped with a simply branched morphism $\overline{C} \to \mathbb{P}^1$ of degree $d \leq 5$. Assume $\operatorname{char} \mathbb{F}_q > 2$ if $d \leq 4$, and $\operatorname{char} \mathbb{F}_q > 3$ if $d = 5$. In this paper we describe how to efficiently compute a lift of $\overline{C}$ to characteristic zero, such that it can be fed as input to Tuitman's algorithm for computing the Hasse–Weil zeta function of $\overline{C}/\mathbb{F}_q$. Our method relies on the parametrizations of low rank rings due to Delone and Faddeev, and Bhargava.

## 1. Introduction

About 20 years ago, Kedlaya published an influential paper [22], showing how one can employ Monsky–Washnitzer cohomology to efficiently compute Hasse–Weil zeta functions of hyperelliptic curves over finite fields having small odd characteristic. Its many follow-up works include several generalizations to geometrically larger classes of curves, first to superelliptic curves [18], then to $C_{ab}$ curves [13] and then further to nondegenerate curves [6], i.e., smooth curves in toric surfaces. A more significant step was taken in 2016, when Tuitman [28; 29] published a Kedlaya-style algorithm that potentially covers arbitrary curves, and at the same time beats the methods from [6; 13] in terms of efficiency. Unfortunately, the user of Tuitman's algorithm is expected to provide a lift of the input curve to characteristic zero that meets the technical requirements from [29, Assumption 1]. Beyond nondegenerate curves, this is a nontrivial task. As a result, the exact range of applicability of Tuitman's method remains unclear.

A partial approach to lifting curves having gonality at most four was sketched in [7], with concrete details being limited to curves of genus five. In the current paper we present a different method, which is faster, works for curves of gonality at most five, and is much easier to implement. Concretely, we assume that we are given an absolutely irreducible curve over a finite field $\mathbb{F}_q$ of characteristic $p > 2$, defined by a polynomial of the form

$$\bar{f}_d(x)y^d + \bar{f}_{d-1}(x)y^{d-1} + \cdots + \bar{f}_0(x) \in \mathbb{F}_q[x, y] \tag{1}$$

for some $d \leq 5$. Moreover, the morphism $\bar{\varphi}$ from its nonsingular projective model $\overline{C}$ to the projective line, induced by $(x, y) \mapsto x$, is assumed to be simply branched of degree $d$; in other words, all fibers of

*MSC2010*: 11G20, 11Y99, 14Q05.
*Keywords*: point counting, Tuitman's algorithm, Delone–Faddeev correspondence, Bhargava correspondence.

$\bar{\varphi}$ should consist of either $d-1$ or $d$ geometric points. Finally, if $d=5$ then it is assumed that $p>3$. Then our method efficiently produces a lift satisfying the main requirement from [29, Assumption 1], which therefore can be fed as input to Tuitman's algorithm, modulo Heuristic H discussed below.

In terms of moduli, the locus of genus $g$ curves admitting a simply branched morphism to $\mathbb{P}^1$ of degree at most 5 has dimension $\min\{2g+5, 3g-3\}$ by a result of Segre [27]. For $g=6$ and $g \geq 8$ this exceeds the locus of nondegenerate curves (and hence the locus of curves for which point counting was previously feasible) by four dimensions; see [10]. In particular, our lifting procedure applies to all sufficiently general curves of genus $g \leq 8$.

**Remark 1.1.** Expecting our curve to be given in the form (1) is essentially equivalent to assuming *knowledge* of an $\mathbb{F}_q$-rational degree $d$ morphism $\bar{C} \to \mathbb{P}^1$ that is simply branched, in contrast with the assumptions from [7]. If such a morphism to $\mathbb{P}^1$ exists but is not known, then one can try to resort to methods due to Schicho, Schreyer and Weimann [24] or Derickx [14, Section 2.3] for finding one.

***Lifting strategy.*** Write $q=p^n$ and fix a degree $n$ number field $K$ in which $p$ is inert. Let $\mathcal{O}_K$ denote its ring of integers and identify $\mathbb{F}_q$ with $\mathcal{O}_K/(p)$. To *lift* the curve $\bar{C}$ means to produce a nonsingular projective curve $C/K$ whose reduction mod $p$ is isomorphic to $\bar{C}/\mathbb{F}_q$; necessarily, the genus of $C$ should be equal to that of $\bar{C}$. Our actual goal is to lift the morphism $\bar{\varphi}$, which means that we want to equip $C$ with a morphism $\varphi : C \to \mathbb{P}^1$ reducing to $\bar{\varphi} : \bar{C} \to \mathbb{P}^1$ mod $p$, up to isomorphism. Our approach to solving this problem is based on the parametrization of low rank rings by Delone and Faddeev [17, Proposition 4.2], and Bhargava [2; 3], in combination with algorithms due to Hess for computing reduced bases [21]. In doing so, we will find concrete, typically nonplanar equations for $\bar{C}$ over $\mathbb{F}_q$ that have "free coefficients", which can be lifted to $\mathcal{O}_K$ naively,[1] in order to obtain a nonsingular projective curve $C/K$ along with a morphism $\varphi : C \to \mathbb{P}^1$ of the said kind. We refer to Section 2 for a more elaborate discussion.

**Remark 1.2.** In general, the polynomial (1), which defines a plane curve that is birationally equivalent with $\bar{C}$, is not liftable directly: there may be many singularities, which typically disappear when lifting the coefficients of (1) naively to $\mathcal{O}_K$, causing an increase of the genus.

**Remark 1.3.** In Kedlaya's original algorithm, corresponding to the case $d=2$, an implicit first step is to rewrite (1) into Weierstrass form. Indeed, Weierstrass models have "free coefficients" that can be lifted naively to $\mathcal{O}_K$, always resulting in a hyperelliptic curve over $K$ having the same genus. From now on we assume $d \geq 3$.

Through elimination of variables (i.e., projection) we then obtain a planar model of the form $f_d(x)y^d + f_{d-1}(x)y^{d-1} + \cdots + f_0(x) = 0$, for polynomials $f_i \in \mathcal{O}_K[x]$ which, in general, do not reduce to $\bar{f}_i$ mod $p$; here, the lifted morphism $\varphi$ again corresponds to $(x,y) \mapsto x$. The change of variables $y \leftarrow y/f_d(x)$ yields a monic defining equation

$$Q(x,y) = y^d + f_{d-1}(x)y^{d-1} + \cdots + f_0(x)f_d(x)^{d-1}, \tag{2}$$

[1] Lifting $\bar{a} \in \mathbb{F}_q \setminus \{0\}$ *naively* to $\mathcal{O}_K$ means producing an element $a \in \mathcal{O}_K$ such that $a$ mod $p = \bar{a}$.

having the right shape to serve as input for Tuitman's algorithm. All subsequent arithmetic in Tuitman's algorithm is done in the $p$-adic completion $\mathbb{Z}_q$ of $\mathcal{O}_K$ (or rather its fraction field $\mathbb{Q}_q$), up to some finite $p$-adic precision. But for the lifting step it suffices to work over $\mathcal{O}_K$, and this has some implementation-technical advantages [7, Remark 2].

***On Tuitman's assumption.*** Let us discuss the specific requirements from [29, Assumption 1] in more detail. A first assumption concerns the polynomial $r(x) = \Delta / \gcd(\Delta, d\Delta/dx)$ with $\Delta$ the discriminant of (2), when viewed as a polynomial in $y$ over $\mathcal{O}_K[x]$:

(a) The discriminant of $r(x)$ is a unit in $\mathbb{Z}_q$.

Next, consider the ring $\mathcal{R} = \mathbb{Z}_q[x, 1/r, y]/(Q)$ and write $\mathbb{Q}_q(x, y)$ for the field of fractions of $\mathcal{R} \otimes \mathbb{Q}_q$ and $\mathbb{F}_q(x, y)$ for the field of fractions of $\mathcal{R} \otimes \mathbb{F}_q$. A second assumption is that we know explicit matrices

$$W_0 \in \mathrm{GL}_d(\mathbb{Z}_q[x, 1/r]) \quad \text{and} \quad W_\infty \in \mathrm{GL}_d(\mathbb{Z}_q[x^{\pm 1}, 1/r])$$

such that, if we write $b_{j,0} = \sum_{i=0}^{d-1} (W_0)_{i+1,j+1} y^i$ and $b_{j,\infty} = \sum_{i=0}^{d-1} (W_\infty)_{i+1,j+1} y^i$, then:

(b) $\{b_{0,0}, \dots, b_{d-1,0}\}$ is an integral basis for $\mathbb{Q}_q(x, y)$ over $\mathbb{Q}_q[x]$ and its reduction mod $p$ is an integral basis for $\mathbb{F}_q(x, y)$ over $\mathbb{F}_q[x]$,

(c) $\{b_{0,\infty}, \dots, b_{d-1,\infty}\}$ is an integral basis for $\mathbb{Q}_q(x, y)$ over $\mathbb{Q}_q[x^{-1}]$ and its reduction mod $p$ is an integral basis for $\mathbb{F}_q(x, y)$ over $\mathbb{F}_q[x^{-1}]$.

Finally, writing

$$\mathcal{R}_0 = \mathbb{Z}_q[x]b_{0,0} + \cdots + \mathbb{Z}_q[x]b_{d-1,0} \quad \text{and} \quad \mathcal{R}_\infty = \mathbb{Z}_q[x^{-1}]b_{0,\infty} + \cdots + \mathbb{Z}_q[x^{-1}]b_{d-1,\infty},$$

it is assumed that

(d) the discriminants of the finite $\mathbb{Z}_q$-algebras $(\mathcal{R}_0/(r))_{\mathrm{red}}$ and $(\mathcal{R}_\infty/(1/x))_{\mathrm{red}}$ are units.

Here the subscript "red" means that we consider the reduced ring obtained by quotienting out the nilradical.[2]

The geometric meaning of assumptions (a) and (d) is discussed in [29, Proposition 2.3]; see also [28, Remark 2.3]. They express that all branch points of $\varphi : C \to \mathbb{P}^1$, as well as all points lying over these branch points, should be distinct mod $p$. In our context, these properties are automatic. Indeed, since $p > 2$ and $\bar{\varphi} : \bar{C} \to \mathbb{P}^1$ is simply branched, there is no wild ramification, hence the ramification divisor of $\varphi$ reduces mod $p$ to that of $\bar{\varphi}$. Thus, again because $\bar{\varphi}$ is simply branched, we see that the ramification points of $\varphi$ must reduce to $2g + 2d - 2$ distinct points that take distinct images under $\bar{\varphi}$, as wanted; here $g$ denotes the genus of $\bar{C}$. We also see that $\varphi$ is simply branched as well.

Assumptions (b) and (c), on the other hand, ask for an explicit description of our lift $\varphi : C \to \mathbb{P}^1$ in terms of two affine patches $\varphi^{-1}(\mathbb{P}^1 \setminus \{\infty\})$ and $\varphi^{-1}(\mathbb{P}^1 \setminus \{0\})$, glued together using $W = W_0^{-1} W_\infty$, that is compatible with reduction mod $p$. In Tuitman's own `pcc_p` and `pcc_q` code,[3] the matrices $W_0$

[2] This takes into account the erratum pointed out in https://jtuitman.github.io/erratum.pdf.

[3] `https://github.com/jtuitman/pcc`, see `mat_W0()` and `mat_Winf()` in `coho_p.m` and `coho_q.m`.

and $W_\infty$ are found by computing integral bases for the function field extension $K(x) \subseteq K(C)$ defined by (2), using the Magma intrinsic `MaximalOrderFinite()`, and hoping that these have good reduction mod $p$. There is a nonzero probability that this approach fails, in which case Tuitman's code outputs "bad model for curve", but in practice this probability become negligible very rapidly as $q$ grows; see the tables in [7]. We therefore content ourselves with relying on the same bet, which we call Heuristic H:

**Definition 1.4** (informal). The output (2) satisfies *Heuristic H* if the associated integral bases of $K(C)$ over $K[x]$ and $K[x^{-1}]$, computed using Magma as in Tuitman's implementation, meet the requirements from [29, Assumption 1].

Of course, if through some other method one manages to find integral bases with good reduction, then this would bypass Heuristic H. In particular, if $d = 3$ then, as explained in Remark 3.4, such integral bases can be extracted as by-products of our lifting procedure.

***Combined runtime.*** The running time of our lifting procedure is strongly dominated by that of Tuitman's algorithm, as should be clear from the discussions in Sections 3, 4 and 5 below. We will therefore omit a detailed analysis, although it is crucial to note that lifting does not inflate the input size too badly. Concretely, if we let $\delta = \max_{0 \le i \le d} \deg \overline{f}_i$, then:

- The reader can check that all $f_i$ are of degree $O(g)$, which in turn is $O(\delta)$ thanks to Baker's bound [1, Theorem 2.4].
- When lifting coefficients from $\mathbb{F}_q$ to $\mathcal{O}_K$ naively, we can choose them to be of bit size $O(n \log q)$, and as a result the same asymptotic estimate applies to the size of the coefficients of the $f_i$.
- As discussed in [29, pages 313–314], the matrices $W_0$, $W_\infty$ produced by the Magma intrinsic, as well as their inverses, involve $K(x)$-coefficients whose pole orders are in $O(\delta)$, as required by [29, Assumption 2]; for $d = 3$, the reader can check that the same bound applies to the integral bases from Remark 3.4.

From [29, Theorem 4.10] it follows that $\tilde{O}(p\delta^4 n^3)$ bit operations suffice for computing the Hasse–Weil zeta function of any curve $\overline{C}/\mathbb{F}_q$ of the form (1), where we recall our dependence on Heuristic H if $d = 4, 5$.

***Practical performance.*** This paper comes with an implementation of our lifting procedure in Magma [4], which can be found in the online supplement. The arxiv version [8] of our paper contains an appendix reporting on how the code performs in combination with Tuitman's implementation for computing Hasse–Weil zeta functions. As discussed there, this gives satisfactory results for $d = 3$ and $d = 4$, leading to a substantial enlargement of the class of curves admitting fast computation of their zeta function (over finite fields with small odd characteristic). In degree $d = 5$ the combined code is considerably slower. This is almost entirely due to the seemingly harmless "elimination of variables" step, which is needed to put the lifted curve $C/K$ in the form (2) and which produces large hidden constants in the above $O(g)$ and $O(n \log q)$ estimates. Nevertheless, here too, it is practically feasible to compute zeta functions in a nontrivial range.

***Tracks for future work.*** Besides mitigating the effect of variable elimination and getting rid of Heuristic H, a challenging goal is to dispose of the conditions on $p$ and of the condition that $\bar{\varphi}$ is simply branched. This seems to require changes to Tuitman's algorithm that are similar to how Denef and Vercauteren managed to make Kedlaya's algorithm work in even characteristic [12]. Also, as explained in Section 2, our naive lifting strategy using "free coefficients" is closely related to Schreyer's proof [25, Corollary 6.8] of the unirationality of $\mathcal{H}_{g,d}$, the moduli space of simply branched degree $d$ covers of $\mathbb{P}^1$ by curves of genus $g$, for $d \leq 5$. Such unirationality results are known to be false for $d \geq 7$, where there is no hope for our strategy to work. This leaves $d = 6$ as an interesting open case, on which several partial (positive) results have been proved by Geiss [20]; see [26, Figure 1] for an overview. It seems worth investigating how Geiss' results combine with our approach.

## 2. Preliminaries

***Reduced bases and Maroni invariants.*** Let $k$ be any field, which in the next sections will be specialized to $k = \mathbb{F}_q$ and/or $k = K$. Consider a nonsingular projective curve $C/k$ of genus $g$, along with a $k$-rational degree $d$ morphism $\varphi : C \to \mathbb{P}^1$. Consider the inclusion of function fields $k(x) \subseteq k(C)$ corresponding to $\varphi$. Let $k[C]_0$ and $k[C]_\infty$, denote the integral closure of $k[x]$ and $k[1/x]$ inside $k(C)$, respectively.

**Theorem 2.1.** *There exist unique negative integers $r_1 \geq r_2 \geq \cdots \geq r_{d-1}$ for which there is a basis $1, \alpha_1, \dots, \alpha_{d-1}$ of $k[C]_0$ over $k[x]$ such that $1, x^{r_1}\alpha_1, \dots, x^{r_{d-1}}\alpha_{d-1}$ is a basis of $k[C]_\infty$ over $k[1/x]$.*

See [21] for a proof; it is standard to call $e_i = -r_i - 2$ the *Maroni invariants* of $C$ with respect to $\varphi$ (e.g., if $\varphi$ is a degree 2 cover, then there is just one Maroni invariant, namely $g-1$). A corresponding basis $1, \alpha_1, \dots, \alpha_{d-1}$ is called a *reduced basis*. In our cases of interest, the integers $r_i$ and an accompanying reduced basis can be computed efficiently: if $k$ is a finite field or a number field, then the Magma command `ShortBasis()` takes care of this.

**Remark 2.2.** In more geometric language, the integers $r_i$ are characterized by the sheaf decomposition $\varphi_* \mathcal{O}_C \cong \mathcal{O}_{\mathbb{P}^1} \oplus \mathcal{O}_{\mathbb{P}^1}(r_1) \oplus \mathcal{O}_{\mathbb{P}^1}(r_2) \oplus \cdots \oplus \mathcal{O}_{\mathbb{P}^1}(r_{d-1})$ which, according to a theorem due to Grothendieck, is indeed unique. As a consequence to the Riemann–Roch theorem, the Maroni invariants satisfy the following basic properties:

(i) $-1 \leq e_1 \leq e_2 \leq \cdots \leq e_{d-1}$,

(ii) $e_1 + e_2 + \cdots + e_{d-1} = g - d + 1$,

(iii) $e_{d-1} \leq (2g-2)/d$.

***Models with "free coefficients".*** As mentioned in the introduction, every cover $\varphi : C \to \mathbb{P}^1$ of degree $3 \leq d \leq 5$ admits a nonsingular projective model with "free coefficients" that can be lifted naively from $\mathbb{F}_q$ to $\mathcal{O}_K$. This follows from Schreyer's proof [25, Corollary 6.8] of the unirationality of $\mathcal{H}_{g,d}$ for $d \leq 5$. The natural ambient space for this model is a *rational normal scroll*, which can be obtained by gluing together

$$(\mathbb{P}^1 \setminus \{\infty\}) \times \mathbb{P}^{d-2} \quad \text{and} \quad (\mathbb{P}^1 \setminus \{0\}) \times \mathbb{P}^{d-2}$$

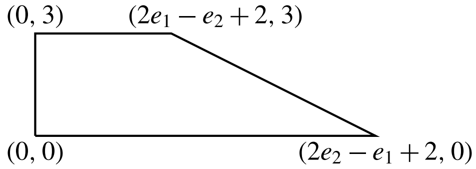


**Figure 1.** Polygon describing covers of degree 3.

in a nonstandard way; the gluing depends on the Maroni invariants $e_1, \dots, e_{d-1}$ of $C$ with respect to $\varphi$. We refer to [15; 25] for more details on this construction, as well as on the claims below. For the sake of conciseness we only describe what the model looks like on the left copy $\mathbb{A}^1 \times \mathbb{P}^{d-2}$, which we equip with coordinates $x, Y_1, \dots, Y_{d-1}$.

First assume that $d = 3$. Then $C$ admits a defining equation of the form

$$\sum_{l_1+l_2=3} f_{l_1,l_2}(x) Y_1^{l_1} Y_2^{l_2} = 0 \tag{3}$$

with $\deg f_{l_1,l_2} \le l_1 e_1 + l_2 e_2 + 4 - g$, such that $\varphi$ corresponds to projection on the $x$-coordinate. Conversely, every irreducible polynomial of the form (3) defines a curve having genus at most $g$; this can also be seen using Baker's bound [1, Theorem 2.4], because the dehomogenization with respect to $Y_2$ is supported on the polygon from Figure 1. If equality holds then this polynomial defines a nonsingular projective curve (on the entire rational normal scroll) and projection on the $x$-coordinate yields a degree 3 morphism to $\mathbb{P}^1$ whose associated Maroni invariants are $e_1, e_2$.

Next, assume that $d = 4$. Then $C$ arises as the intersection of two surfaces defined by

$$\sum_{l_1+l_2+l_3=2} f_{i,l_1,l_2,l_3}(x) Y_1^{l_1} Y_2^{l_2} Y_3^{l_3} = 0 \tag{4}$$

for $i = 1, 2$, where $\deg f_{i,l_1,l_2,l_3} \le l_1 e_1 + l_2 e_2 + l_3 e_3 - b_i$ for unique integers $-1 \le b_1 \le b_2$ with $b_1 + b_2 = g - 5$, called the Schreyer invariants of $C$ with respect to $\varphi$. Conversely, every irreducible such intersection defines a curve of genus at most $g$; this too can be seen using (a three-dimensional version of) Baker's bound [23, Theorem 1], by noting that the dehomogenizations with respect to $Y_3$ are supported on the polytopes from Figure 2. If equality holds then it concerns a nonsingular projective curve, and projection

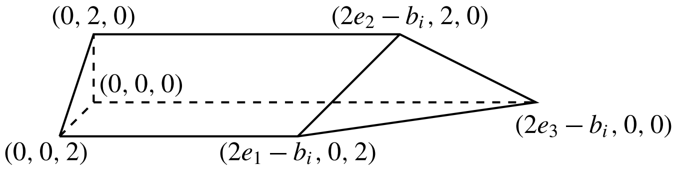


**Figure 2.** Polytope describing covers of degree 4.

on the $x$-coordinate defines a degree 4 morphism to $\mathbb{P}^1$ with associated Maroni invariants $e_1, e_2, e_3$ and Schreyer invariants $b_1, b_2$.

Finally, assume $d = 5$, which comes with five Schreyer invariants $b_1 \leq \cdots \leq b_5$ summing up to $2g - 12$. In this case $C$ can be viewed as the intersection of five hypersurfaces, which are all obtained from a single $5 \times 5$ skew-symmetric matrix $M$ over $k[x][Y_1, Y_2, Y_3, Y_4]$ whose $(i, j)$-th entry is of the form

$$M_{1,i,j}(x)Y_1 + M_{2,i,j}(x)Y_2 + M_{3,i,j}(x)Y_3 + M_{4,i,j}(x)Y_4 \tag{5}$$

with $M_{r,i,j}(x) \in k[x]$ of degree at most $e_r + b_i + b_j + 6 - g$. More precisely, our hypersurfaces are cut out by the five $4 \times 4$ sub-Pfaffians of $M$.[4] Conversely, whenever the $4 \times 4$ sub-Pfaffians of such a matrix define an irreducible curve, it has genus at most $g$. If equality holds then it concerns a nonsingular projective curve, and projection on the $x$-coordinate defines a degree 5 morphism to $\mathbb{P}^1$ with Maroni invariants $e_1, e_2, e_3, e_4$ and Schreyer invariants $b_1, b_2, b_3, b_4, b_5$.

***Lifting strategy revisited.*** In the next sections we show how results on ring parametrizations due to Delone and Faddeev [17, Proposition 2.4] and Bhargava [2; 3] can be used to efficiently produce such a "free coefficient" model for our input curve $\overline{C}/\mathbb{F}_q$. Then, by the above discussion, and using that the genus cannot increase under reduction mod $p$, any naive coefficient-wise lift of this model to $\mathcal{O}_K$ will define a nonsingular projective curve $C/K$ along with a morphism $\varphi : C \to \mathbb{P}^1$ lifting $\overline{C}$ and $\overline{\varphi}$.

**Remark 2.3.** From a nonalgorithmic viewpoint, the fact that the Delone–Faddeev and Bhargava correspondences produce nonsingular curves in rational normal scrolls might have been known to some specialists (e.g., for $d = 3$ this can be read in Zhao's Ph.D. thesis [31]).

## 3. Lifting curves in degree $d = 3$

For $R$ a PID, we recall that a *ring of rank $d$* over $R$ is a commutative $R$-algebra which is free of rank $d$ as a module over $R$. Every ring $S$ of rank $d$ over $R$ admits an $R$-basis of the form $1, \alpha_1, \ldots, \alpha_{d-1}$. This can be seen by applying the structure theorem for finitely generated free modules over PIDs to the submodule $R \cdot 1$ of $S$.

***Parametrizing cubic rings.*** Let $R$ be a PID. Cubic rings over $R$ admit a parametrization using binary cubic forms over $R$, considered modulo a natural action by $\mathrm{GL}_2(R)$: for an element

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(R),$$

and $f = f_3Y_1^3 + f_2Y_1^2Y_2 + f_1Y_1Y_2^2 + f_0Y_2^3$ a cubic form over $R$, we let

$$A * f(Y_1, Y_2) = \frac{1}{\det A} f(aY_1 + cY_2, bY_1 + dY_2).$$

[4] The square roots of the determinants of the five $4 \times 4$ skew-symmetric submatrices.

**Theorem 3.1** (Delone–Faddeev). *There is a canonical bijection between the set of cubic $R$-rings up to isomorphism and binary cubic forms over $R$, modulo the action of* $\mathrm{GL}_2(R)$.

For a proof see e.g., [17, Proposition 4.2]. For use below we briefly describe how this bijection is constructed. Let $S$ be a cubic $R$-ring with basis $1, \alpha_1, \alpha_2$. By adding elements of $1 \cdot R$ to $\alpha_1$ and $\alpha_2$ we can assume that $\alpha_1\alpha_2$ is in $R$. We call such bases *normal*. Now write out the multiplication table of $S$:

$$\begin{aligned} \alpha_1\alpha_2 &= -g_0, \\ \alpha_1^2 &= -g_1 + f_2\alpha_1 - f_3\alpha_2, \\ \alpha_2^2 &= -g_2 + f_0\alpha_1 - f_1\alpha_2. \end{aligned} \tag{6}$$

By associativity of $S$ we have $\alpha_1^2 \cdot \alpha_2 = \alpha_1 \cdot (\alpha_1\alpha_2)$ and $\alpha_1 \cdot \alpha_2^2 = (\alpha_1\alpha_2) \cdot \alpha_2$. This gives

$$\begin{aligned} g_0 &= f_0 f_3, \\ g_1 &= f_1 f_3, \\ g_2 &= f_0 f_2, \end{aligned} \tag{7}$$

so the $g_i$ are determined by the $f_i$. One then associates to $S$ the cubic form $f = f_3Y_1^3 + f_2Y_1^2Y_2 + f_1Y_1Y_2^2 + f_0Y_2^3$. Conversely, given such a form $f$, associate to this the cubic ring, formally equipped with basis $1, \alpha_1, \alpha_2$ and multiplication defined by (6) and (7). The $\mathrm{GL}_2(R)$-action on cubic forms corresponds precisely to changing one normal basis to another on the level of cubic rings.

**Remark 3.2.** A cubic form $f = f_3Y_1^3 + f_2Y_1^2Y_2 + f_1Y_1Y_2^2 + f_0Y_2^3$ is irreducible if and only if its associated cubic $R$-ring is a domain. In this case, we may describe it as the subring of

$$\mathrm{Frac}\left(\frac{R[y]}{(f_3y^3 + f_2y^2 + f_1y + f_0)}\right)$$

generated by $1, \alpha_1 = f_3y, \alpha_2 = -f_0y^{-1} = f_3y^2 + f_2y + f_1$. This point of view is especially nice when $R = k[x]$ for some field $k$. Indeed, then $f(y, 1) = 0$ defines a curve in $\mathbb{A}^2$ over $k$ and the cubic ring associated to $f$ has as its field of fractions the function field of this curve.

***Lifting degree* 3 *covers.*** Consider the function field

$$\mathbb{F}_q(\overline{C}) = \mathrm{Frac}\left(\frac{\mathbb{F}_q[x, y]}{(\overline{f}_3y^3 + \overline{f}_2y^2 + \overline{f}_1y + \overline{f}_0)}\right)$$

defined by our input polynomial, and consider the integral closure $\mathbb{F}_q[\overline{C}]_0$ of $\mathbb{F}_q[x]$ inside it; this is a cubic $\mathbb{F}_q[x]$-ring. Let $e_1, e_2$ be the Maroni invariants of $\overline{C}$ with respect to $\overline{\varphi}$ and let $1, \alpha_1, \alpha_2$ be a corresponding reduced basis. After adding to $\alpha_1$ and $\alpha_2$ elements of $\mathbb{F}_q[x]$ we may assume that this basis is normal. In more detail, if $\alpha_1\alpha_2 = a\alpha_1 + b\alpha_2 + c$, for $a, b, c \in \mathbb{F}_q[x]$, then we replace $\alpha_1$ by $\alpha_1 - b$ and $\alpha_2$ by $\alpha_2 - a$. This operation will not change the fact that the basis is reduced. Applying the Delone–Faddeev correspondence to this basis produces a new cubic form

$$\overline{f}(Y_1, Y_2) = \overline{f}_3Y_1^3 + \overline{f}_2Y_1^2Y_2 + \overline{f}_1Y_1Y_2^2 + \overline{f}_0Y_2^3$$

whose coefficients we, abusingly, again denote by $\overline{f}_i$.

**Lemma 3.3.** *Let $\overline{f}$ be obtained through the Delone–Faddeev correspondence as above. Then this is a model for $\overline{C}$ of the form (3).*

*Proof.* Note that the curve $\overline{f}(y,1)=0$ is indeed birationally equivalent with $\overline{C}$, in view of Remark 3.2. Denote by $e_1, e_2$ the Maroni invariants of $\overline{C}$. Since $1, \alpha_1, \alpha_2$ is a reduced basis, the elements $1, x^{-e_1-2}\alpha_1$, $x^{-e_2-2}\alpha_2$ form a basis for $\mathbb{F}_q[\overline{C}]_\infty$, the integral closure of $\mathbb{F}_q[x^{-1}]$ inside $\mathbb{F}_q(\overline{C})$. Writing out the multiplication for this ring gives

$$\begin{aligned}
x^{-e_1-e_2-4}\alpha_1\alpha_2 &= -x^{-e_1-e_2-4}\overline{f}_0\overline{f}_3,\\
x^{-2e_1-4}\alpha_1^2 &= -x^{-2e_1-4}\overline{f}_1\overline{f}_3+x^{-e_1-2}\overline{f}_2x^{-e_1-2}\alpha_1-x^{-2e_1+e_2-2}\overline{f}_3x^{-e_2-2}\alpha_2,\\
x^{-2e_2-4}\alpha_2^2 &= -x^{-2e_2-4}\overline{f}_0\overline{f}_2+x^{-2e_2+e_1-2}\overline{f}_0x^{-e_1-2}\alpha_1-x^{-e_2-2}\overline{f}_1x^{-e_2-2}\alpha_2.
\end{aligned}$$

Since the coefficients of this table must be elements of $\mathbb{F}_q[x^{-1}]$ we see that $\deg \overline{f}_i \le (i-1)e_1+(2-i)e_2+2$ for $i=1,2$, hence $\overline{f}(y,1)$ is supported on the polygon from Figure 1. □

Thus we can proceed as follows. We compute a reduced basis for the function field $\mathbb{F}_q(\overline{C})$ over $\mathbb{F}_q[x]$, make it normal if needed, and apply the Delone–Faddeev correspondence to it to obtain a model $\overline{f}=0$ of the form (3). As discussed in Section 2, any naive coefficient-wise lift of the polynomial $\overline{f}(y,1)$ to a polynomial $f=f_3y^3+f_2y^2+f_1y+f_0\in\mathcal{O}_K[x]$ defines a good lift. After making the polynomial $f$ monic as in (2), it can be fed to Tuitman's algorithm to compute the zeta function of $\overline{C}$ over $\mathbb{F}_q$.

**Remark 3.4.** Our discussion also shows that $1,\ f_3y,\ f_0y^{-1}=f_3y^2+f_2y+f_1$ is an integral basis of $K(C)$ over $K[x]$ that reduces to an integral basis of $\mathbb{F}_q[\overline{C}]$ over $\mathbb{F}_q[x]$. Using the variable change $\mathsf{x}=x^{-1}$ and $\mathsf{y}=y/x^{e_2-e_1}$ we find the patch

$$f_3^{\text{recipr.}}(\mathsf{x})\mathsf{y}^3+f_2^{\text{recipr.}}(\mathsf{x})\mathsf{y}^2+f_1^{\text{recipr.}}(\mathsf{x})\mathsf{y}+f_0^{\text{recipr.}}(\mathsf{x})$$

above infinity, which admits an analogous integral basis. Here $f_i^{\text{recipr.}}$ denotes the degree $(i-1)e_1+(2-i)e_2+2$ reciprocal of $f_i$. We can supply these bases as additional input to Tuitman's algorithm, thereby bypassing Heuristic H.

## 4. Lifting curves in degree $d=4$

***Parametrizing quartic rings.*** The parametrization of quartic $R$-rings $S$ is due to Bhargava [2]. This time, the objects involved are pairs of ternary quadratic forms, up to an action of $\mathrm{GL}_3(R)\times\mathrm{GL}_2(R)$. For an element

$$(A,B)\in\mathrm{GL}_3(R)\times\mathrm{GL}_2(R),$$

and a pair of ternary quadratic forms $(Q_1,Q_2)$ over $R$ represented as $3\times3$ matrices, the action is defined by

$$(A,B)*(Q_1,Q_2)=B\cdot\begin{pmatrix}AQ_1A^T\\ AQ_2A^T\end{pmatrix}.$$

Concretely, the quadratic forms associated with a quartic ring are obtained by specifying a *cubic resolvent* (the next paragraph provides more details).

**Theorem 4.1** (Bhargava). *There is a canonical bijection between pairs $(S, S')$ where $S$ is a quartic ring over $R$ and $S'$ is a cubic resolvent for $S$, considered up to isomorphism, and pairs of ternary quadratic forms over $R$, up to the action of* $\mathrm{GL}_3(R) \times \mathrm{GL}_2(R)$.

See [2, Theorem 1], although we will not explicitly rely on this theorem. But we will recycle its central map $\phi$, whose construction we briefly recall, while zooming in on our main case of interest, namely where $S$ is a domain, say with field of fractions $F$. We assume moreover that $F$ is a separable $S_4$-extension of $K = \operatorname{Frac} R$, i.e., its Galois closure $E/K$ has as Galois group the full symmetric group $S_4$. Then a cubic resolvent for $S$ is a certain full-rank subring $S' \subseteq E^{D_4} =: F^{\mathrm{res}}$, where $D_4 = \langle (12), (1324) \rangle$; see [2, Definition 8] for a precise definition. In general, there might be more than one cubic resolvent ring, but for maximal rings it is unique [2, Corollary 5]. Note that if $F = K[y]/(f)$ with

$$f = (y - r_1)(y - r_2)(y - r_3)(y - r_4) = y^4 + ay^3 + by^2 + cy + d$$

then $F^{\mathrm{res}} = K[y]/(\operatorname{res} f)$ with

$$\begin{aligned} \operatorname{res} f &= (y - r_1r_2 - r_3r_4)(y - r_1r_3 - r_2r_4)(y - r_1r_4 - r_2r_3) \\ &= y^3 - by^2 + (ac - 4d)y - (a^2d + c^2 - 4bd). \end{aligned}$$

This polynomial is famously known as *Lagrange's cubic resolvent*. The most important feature of the Bhargava correspondence is the natural quadratic map

$$\tilde{\phi} : F \to F^{\mathrm{res}} : \alpha \mapsto \alpha^{(1)}\alpha^{(2)} + \alpha^{(3)}\alpha^{(4)},$$

where the $\alpha^{(i)}$ denote the conjugates of $\alpha$ inside $E$ (numbered compatibly with the roots $r_i$). This map turns out to descend to a quadratic map of $R$-modules

$$\phi : \frac{S}{R} \to \frac{S'}{R}.$$

Upon taking bases for $S/R$ and $S'/R$ we obtain our two ternary quadratic forms over $R$. Changing bases of these modules then corresponds to an element of $\mathrm{GL}_3(R) \times \mathrm{GL}_2(R)$.

***Lifting degree* 4 *covers.*** We can assume that $\bar{f}_4 = 1$, i.e., our input polynomial (1) is monic. Let $\mathbb{F}_q(\bar{C})$ denote the function field it defines, which is a separable $S_4$-extension of $\mathbb{F}_q(x)$ because $\bar{\varphi}$ is simply branched [16, Lemma 6.10]. Similarly, consider the cubic resolvent

$$y^3 - \bar{f}_2 y^2 + (\bar{f}_1 \bar{f}_3 - 4\bar{f}_0)y - (\bar{f}_0 \bar{f}_3^2 + \bar{f}_1^2 - 4\bar{f}_0 \bar{f}_2) \tag{8}$$

defining $\mathbb{F}_q(\bar{C}^{\mathrm{res}}) := \mathbb{F}_q(\bar{C})^{\mathrm{res}}$. We let $\mathbb{F}_q[\bar{C}]_0$ and $\mathbb{F}_q[\bar{C}^{\mathrm{res}}]_0$ be the respective integral closures of $R = \mathbb{F}_q[x]$ inside these fields. It can be argued that $\mathbb{F}_q[\bar{C}^{\mathrm{res}}]_0$ is the unique cubic resolvent ring $S'$ for $S = \mathbb{F}_q[\bar{C}]_0$, but for our needs it suffices to know that $S' \subseteq \mathbb{F}_q[\bar{C}^{\mathrm{res}}]_0$, which is immediate since $\mathbb{F}_q[\bar{C}^{\mathrm{res}}]_0$ is maximal.

Let $e_1, e_2, e_3$ be the Maroni invariants of $\overline{C}$ with respect to $\overline{\varphi}$, and let $b_1, b_2$ be its Schreyer invariants. Take reduced $\mathbb{F}_q[x]$-bases $1, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q[\overline{C}]_0$ and $1, \beta_1, \beta_2 \in \mathbb{F}_q[\overline{C}^{\mathrm{res}}]_0$. With respect to these bases, the map $\phi$ above gives us two ternary quadratic forms $\overline{Q}_1, \overline{Q}_2 \in \mathbb{F}_q[x][Y_1, Y_2, Y_3]$. To properly bound the degrees of their coefficients, we have to understand how the Maroni invariants of the resolvent curve $\overline{C}^{\mathrm{res}}$ relate to data associated with $\overline{C}$. Surprisingly, up to a small shift, these turn out to be the Schreyer invariants of $\overline{C}$ with respect to $\overline{\varphi}$.

**Theorem 4.2.** *Let $k$ be a field of characteristic $\neq 2$ and consider a smooth projective curve over $k$ equipped with a simply branched degree $4$ morphism to $\mathbb{P}^1$, say with Schreyer invariants $b_1, b_2$. Then the Maroni invariants of its cubic resolvent are $b_1 + 2, b_2 + 2$.*

*Proof.* This result is due to Casnati [5, Definition 6.4], although he formulated it in terms of Recillas' trigonal construction, which is the geometric counterpart of Lagrange's cubic resolvent, as pointed out in [19, Section 8.6]. □

**Lemma 4.3.** *The quadratic forms $\overline{Q}_1, \overline{Q}_2$ obtained through Bhargava's correspondence as above are a model of $\overline{C}$ of the form (4).*

*Proof.* Note that the polynomials indeed cut out a curve that is birationally equivalent with $\overline{C}$, in view of [3, Section 2].[5] Since $1, \alpha_1, \alpha_2, \alpha_3$ and $1, \beta_1, \beta_2$ are reduced bases, by Theorem 4.2 we have that

$$1,\ x^{-e_1-2}\alpha_1,\ x^{-e_2-2}\alpha_2,\ x^{-e_3-2}\alpha_3 \quad \text{and} \quad 1,\ x^{-b_1-4}\beta_1,\ x^{-b_2-4}\beta_2$$

are bases of $\mathbb{F}_q[\overline{C}]_\infty$ and $\mathbb{F}_q[\overline{C}^{\mathrm{res}}]_\infty$, the integral closures of $\mathbb{F}_q[x^{-1}]$ in $\mathbb{F}_q(\overline{C})$ and $\mathbb{F}_q(\overline{C}^{\mathrm{res}})$, respectively. Now the quadratic map

$$\tilde{\phi} : \mathbb{F}_q(\overline{C}) \to \mathbb{F}_q(\overline{C}^{\mathrm{res}})$$

from above also descends to a quadratic map of $\mathbb{F}_q[x^{-1}]$-modules

$$\phi' : \frac{\mathbb{F}_q[\overline{C}]_\infty}{\mathbb{F}_q[x^{-1}]} \to \frac{\mathbb{F}_q[\overline{C}^{\mathrm{res}}]_\infty}{\mathbb{F}_q[x^{-1}]}.$$

With respect to the above bases, $\phi'$ is defined by two quadratic forms over $\mathbb{F}_q[x^{-1}]$, which are necessarily obtained from $\overline{Q}_1$ and $\overline{Q}_2$ by applying the corresponding (diagonal) change of basis matrices. In other words, $\phi'$ is represented by the quadratic forms

$$x^{b_1+4}\overline{Q}_1(x^{-e_1-2}Y_1, x^{-e_2-2}Y_2, x^{-e_3-2}Y_3), \quad x^{b_2+4}\overline{Q}_2(x^{-e_1-2}Y_1, x^{-e_2-2}Y_2, x^{-e_3-2}Y_3).$$

But these have coefficients in $\mathbb{F}_q[x^{-1}]$. Hence the degree of the $Y_iY_j$-coefficient in $\overline{Q}_1$ can be at most $e_i + e_j - b_1$, and similarly for $\overline{Q}_2$. In other words, the dehomogenized polynomials $\overline{Q}_1(y_1, y_2, 1)$ and $\overline{Q}_2(y_1, y_2, 1)$ are supported on the polytopes from Figure 2. □

[5] Alternatively, the reader can check that $\mathrm{res}_{y_2}(\overline{Q}'_1(y_1, y_2, 1), \overline{Q}'_2(y_1, y_2, 1)) = y_1^4 + \bar{f}_3 y_1^3 + \bar{f}_2 y_1^2 + \bar{f}_1 y_1 + \bar{f}_0$, where $\overline{Q}'_1$ and $\overline{Q}'_2$ are the quadratic forms from below.

To compute these liftable quadrics $\overline{Q}_1, \overline{Q}_2$ in practice we will not directly compute the resolvent map $\phi$ with respect to reduced bases for $\mathbb{F}_q(\overline{C})$ and $\mathbb{F}_q(\overline{C}^{\mathrm{res}})$. Instead, we compute the map $\phi$ with respect to certain *naive bases* for $\mathbb{F}_q(\overline{C})$ and $\mathbb{F}_q(\overline{C}^{\mathrm{res}})$ and then apply change of basis to a reduced basis. In more detail, denoting by $\overline{f}'_i$ the coefficients of the cubic resolvent polynomial of $\overline{f}$ as in (8), we consider the bases

$$1, -\overline{f}_0 y^{-1}, y, y^2 \text{ for } \mathbb{F}_q(\overline{C}) \quad \text{and} \quad 1, y, -\overline{f}'_0 y^{-1} \text{ for } \mathbb{F}_q(\overline{C}^{\mathrm{res}}). \tag{9}$$

Computing the representation of the resolvent map $\phi$ with respect to these bases can be done symbolically by means of Vieta's formulas, yielding the quadrics

$$\overline{Q}'_1 = \begin{pmatrix} \overline{f}_0 & 0 & \overline{f}_1/2 \\ 0 & 1 & -\overline{f}_3/2 \\ \overline{f}_1/2 & -\overline{f}_3/2 & \overline{f}_2 \end{pmatrix}, \quad \overline{Q}'_2 = \begin{pmatrix} 0 & -1/2 & \overline{f}_3/2 \\ -1/2 & 0 & 0 \\ \overline{f}_3/2 & 0 & 1 \end{pmatrix}. \tag{10}$$

Now let $1, \alpha_1, \alpha_2, \alpha_3$ and $1, \beta_1, \beta_2$ be reduced bases for $\mathbb{F}_q[\overline{C}]_0$ and $\mathbb{F}_q[\overline{C}^{\mathrm{res}}]_0$, respectively, as above. To compute the cubic resolvent map with respect to these bases, we simply apply the change of basis action from the naive bases in (9) to these reduced bases. We note that this involves elements of $\mathrm{GL}_3(\mathbb{F}_q(x)) \times \mathrm{GL}_2(\mathbb{F}_q(x))$ rather than $\mathrm{GL}_3(\mathbb{F}_q[x]) \times \mathrm{GL}_2(\mathbb{F}_q[x])$. The resulting quadrics $\overline{Q}_1, \overline{Q}_2$ will be our model of the form (4). Then, as explained in Section 2, we can take any $Q_1, Q_2 \in \mathcal{O}_K[x][y_1, y_2]$ lifting the $\overline{Q}_i(y_1, y_2, 1)$ in a support-preserving way. In order to find a plane model, we can compute the resultant $\mathrm{res}_{y_2}(Q_1, Q_2)$, which is indeed of degree 4 in $y = y_1$. After making it monic, it can be fed as input to Tuitman's algorithm.

## 5. Lifting curves in degree $d = 5$

***Parametrizing quintic rings.*** The parametrization of quintic $R$-rings $S$ is also due to Bhargava [3]. We assume that char $R \neq 2, 3$. The objects involved in the parametrization are now quadruples of $5 \times 5$ skew-symmetric matrices over $R$. There is a natural action of $\mathrm{GL}_5(R) \times \mathrm{GL}_4(R)$ on such objects, given by

$$(A, B) * M = B \cdot \begin{pmatrix} AM_1A^T \\ AM_2A^T \\ AM_3A^T \\ AM_4A^T \end{pmatrix},$$

with $M = (M_1, M_2, M_3, M_4)$ a quadruple of $5 \times 5$ skew-symmetric matrices and $(A, B) \in \mathrm{GL}_5(R) \times \mathrm{GL}_4(R)$. Here the parametrization requires us to specify a *sextic resolvent* (see the next paragraph for details).

**Theorem 5.1** (Bhargava). *There is a canonical bijection between pairs $(S, S')$ where $S$ is a quintic ring and $S'$ is a sextic resolvent for $S$, considered up to isomorphism, and quadruples of* $5 \times 5$ *skew-symmetric matrices over $R$, up to the action of* $\mathrm{GL}_5(R) \times \mathrm{GL}_4(R)$.

See [3]; although as in the previous sections, we will not explicitly rely on this theorem. But we will need the fundamental resolvent map (11) below. Let us again focus on the setting where $S$ is a domain with field of fractions $F$, and let $K = \operatorname{Frac} R$. We assume that $F$ is a separable $S_5$-extension of $K$, i.e., its Galois closure $E/K$ has as Galois group the whole of $S_5$. Consider the order 20 subgroup $H = H^{(1)} = \mathrm{AGL}_1(\mathbb{F}_5) = \langle (12345), (1243) \rangle \subseteq S_5$. Then a sextic resolvent for $S$ is a certain full-rank subring $S' \subseteq E^H =: F^{\mathrm{res}}$; for a precise definition we refer to [3, Definition 5]. In general, such a sextic resolvent ring is not unique, but for maximal quintic rings it is [3, Corollary 19]. If $F = K[y]/(f)$ with

$$f = (y-r_1)(y-r_2)(y-r_3)(y-r_4)(y-r_5) = y^5 + ay^4 + by^3 + cy^2 + dy + e,$$

then $F^{\mathrm{res}} = K[y]/(\operatorname{res} f)$ with $\operatorname{res} f = (y-\rho_1)(y-\rho_2)(y-\rho_3)(y-\rho_4)(y-\rho_5)(y-\rho_6)$, where

$$\rho_1 = (r_1r_2 + r_2r_3 + r_3r_4 + r_4r_5 + r_5r_1 - r_1r_3 - r_3r_5 - r_5r_2 - r_2r_4 - r_4r_1)^2$$

and $\{\rho_1, \rho_2, \dots, \rho_6\}$ is the orbit of $\rho_1$ under the natural $S_5$-action permuting the $r_i$. Note that $\rho_1$ is stabilized by $H^{(1)}$. We choose $\rho_{2+i}$ to be stabilized by the conjugate subgroup

$$H^{(2+i)} = (12345)^{-i} \langle (13254), (3245) \rangle (12345)^i, \text{ for } 0 \le i \le 4.$$

The polynomial $\operatorname{res} f$ is known as *Cayley's sextic resolvent*; concrete expressions for its coefficients in terms of $a, b, c, d, e$ can be found in [11, Proof of Proposition 13.2.5].[6]

For an element $\alpha \in F^{\mathrm{res}}$ we denote by $\alpha^{(i)}$ the conjugates of $\alpha$ inside $E$, labeled so that $\alpha^{(i)}$ is fixed by $H^{(i)}$. Consider bases $\alpha_0 = 1, \alpha_1, \dots, \alpha_4$ for $S/R$ and $\beta_0 = 1, \beta_1, \dots, \beta_5$ for $S'/R$, and define

$$\sqrt{\operatorname{disc} S} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1^{(1)} & \alpha_1^{(2)} & \cdots & \alpha_1^{(5)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_4^{(1)} & \alpha_4^{(2)} & \cdots & \alpha_4^{(5)} \end{vmatrix}.$$

The central tool in Bhargava's correspondence is the *fundamental resolvent map*, which is the bilinear alternating form

$$g : F^{\mathrm{res}} \times F^{\mathrm{res}} \to F : (\alpha, \beta) \mapsto \sqrt{\operatorname{disc} S} \cdot \begin{vmatrix} 1 & 1 & 1 \\ \alpha^{(1)} + \alpha^{(2)} & \alpha^{(3)} + \alpha^{(6)} & \alpha^{(4)} + \alpha^{(5)} \\ \beta^{(1)} + \beta^{(2)} & \beta^{(3)} + \beta^{(6)} & \beta^{(4)} + \beta^{(5)} \end{vmatrix}. \tag{11}$$

This turns out to descend to a well-defined map $\tilde{S}' \times \tilde{S}' \to \tilde{S}$, where

$$\tilde{S} = R\alpha_1^* + R\alpha_2^* + R\alpha_3^* + R\alpha_4^* \subseteq F, \quad \tilde{S}' = R\beta_1^* + R\beta_2^* + R\beta_3^* + R\beta_4^* + R\beta_5^* \subseteq F^{\mathrm{res}}$$

are defined in terms of the dual bases $\alpha_0^*, \dots, \alpha_4^*$ and $\beta_0^*, \dots, \beta_5^*$ with respect to the trace pairing, i.e., $\mathrm{Tr}_{F/K}(\alpha_i \alpha_j^*) = \delta_{ij}$ (with $\delta_{ij}$ the Kronecker delta), and similarly for $\beta_j^*$. Note that the extensions $F/K$ and $F^{\mathrm{res}}/K$ are both separable and so their trace pairings are nondegenerate. With respect to the bases $\{\beta_i^*\}_i$

[6] Or they can be found hard-coded in our accompanying Magma file `precomputed_5.m`.

and $\{\alpha_i^*\}_i$, the map $g$ is represented by a quadruple $M = (M_1, M_2, M_3, M_4)$ of $5 \times 5$ skew-symmetric matrices. Changing bases of $\tilde{S}'$ and $\tilde{S}$ then corresponds to an element of $\mathrm{GL}_5(R) \times \mathrm{GL}_4(R)$.

**Remark 5.2.** Our fundamental resolvent map differs from Bhargava's original map by a factor $\frac{4}{3}$, which is not an issue in view of our restrictions on the field characteristic.

***Lifting degree 5 covers.*** As in the $d = 4$ case, we assume that our input polynomial $\overline{f}$ from (1) is monic (i.e., $\overline{f}_5 = 1$). Let $\mathbb{F}_q(\overline{C})$ be the corresponding function field; this is a separable $S_5$-extension of $\mathbb{F}_q(x)$ because $\overline{\varphi}$ is simply branched [16, Lemma 6.10]. We also consider Cayley's sextic resolvent associated with our input polynomial, defining $\mathbb{F}_q(\overline{C}^{\mathrm{res}}) := \mathbb{F}_q(\overline{C})^{\mathrm{res}}$. Let $\mathbb{F}_q[\overline{C}]_0$ and $\mathbb{F}_q[\overline{C}^{\mathrm{res}}]_0$ be the respective integral closures of $R = \mathbb{F}_q[x]$ inside these two function fields; it can be argued that $\mathbb{F}_q[\overline{C}^{\mathrm{res}}]_0$ is the unique sextic resolvent ring $S'$ for $S = \mathbb{F}_q[\overline{C}]_0$, but as in the $d = 4$ case it suffices to observe that $S' \subseteq \mathbb{F}_q[\overline{C}^{\mathrm{res}}]_0$.

Let $e_1, e_2, e_3, e_4$ be the Maroni invariants of $\overline{C}$ with respect to $\overline{\varphi}$, and let $b_1, b_2, b_3, b_4, b_5$ be its Schreyer invariants. Take reduced $\mathbb{F}_q[x]$-bases $1, \alpha_1, \dots, \alpha_4 \in \mathbb{F}_q[\overline{C}]_0$ and $1, \beta_1, \dots, \beta_5 \in \mathbb{F}_q[\overline{C}^{\mathrm{res}}]_0$ and consider the quadruple $(\overline{M}_1, \overline{M}_2, \overline{M}_3, \overline{M}_4)$ of $5 \times 5$ skew-symmetric matrices over $\mathbb{F}_q[x]$ arising along the above construction. We represent this by the single matrix

$$\overline{M} = \overline{M}_1 Y_1 + \overline{M}_2 Y_2 + \overline{M}_3 Y_3 + \overline{M}_4 Y_4 \in k[x][Y_1, Y_2, Y_3, Y_4]$$

whose entries are now linear and homogeneous in the $Y_i$. To get a handle on the degrees of their coefficients, we should again express the Maroni invariants of the resolvent curve $\overline{C}^{\mathrm{res}}$ in terms of data associated with $\overline{C}$. As in the case of the cubic resolvent, this can be done in a surprisingly explicit way.

**Theorem 5.3.** *Let $k$ be a field of characteristic $\neq 2$ and consider a smooth projective curve over $k$ equipped with a simply branched degree 5 morphism to $\mathbb{P}^1$, say with Schreyer invariants $b_1, \dots, b_5$. Then the Maroni invariants of its sextic resolvent are $g - 2 - b_5, \dots, g - 2 - b_1$.*

*Proof.* This theorem seems new and is part of a generalization of Theorem 4.2, which is currently being elaborated in collaboration with Yongqiang Zhao [9]. In the meantime, a proof of Theorem 5.3 can be found in the master thesis of the second listed author [30]. □

**Lemma 5.4.** *Denote by $\overline{M}_{r,i,j}$ the $(i, j)$-th entry of the matrix $\overline{M}_r$ constructed through Bhargava's correspondence as above. Then* $\deg \overline{M}_{r,i,j} \leq e_r + b_i + b_j + 6 - g$. *In particular, this defines a model for $\overline{C}$ of the form (5).*

*Proof.* The fact that the sub-Pfaffians of $\overline{M}$ cut out a curve birational to $\overline{C}$ follows again from [3, Section 2]. As for the claim on the degrees, we apply the same proof strategy as in the degree 4 case. Denote by $\mathbb{F}_q[\overline{C}]_\infty$ the integral closure of $\mathbb{F}_q[x^{-1}]$ in $\mathbb{F}_q(\overline{C})$. Let $g_0$ be the fundamental resolvent form attached to the basis $1, \alpha_1, \dots, \alpha_4$ of $\mathbb{F}_q[\overline{C}]_0$ over $\mathbb{F}_q[x]$, and let $g_\infty$ be the fundamental resolvent form attached to the basis $1, x^{-e_1-2}\alpha_1, \dots, x^{-e_4-2}\alpha_4$ of $\mathbb{F}_q[\overline{C}]_\infty$ over $\mathbb{F}_q[x^{-1}]$. We have that, for all $u, v \in \mathbb{F}_q(\overline{C}^{\mathrm{res}})$,

$$g_0(u, v) = \frac{\sqrt{\operatorname{disc} \mathbb{F}_q[\overline{C}]_0}}{\sqrt{\operatorname{disc} \mathbb{F}_q[\overline{C}]_\infty}} g_\infty(u, v) = x^{g+4} g_\infty(u, v).$$

Let $\alpha_0^*, \dots, \alpha_4^*$ and $\beta_0^*, \dots, \beta_5^*$ be dual bases for $1, \alpha_1, \dots, \alpha_4$ and $1, \beta_1, \dots, \beta_5$, respectively. Then the corresponding dual bases for the rings $\mathbb{F}_q[\bar{C}]_\infty$ and $\mathbb{F}_q[\bar{C}^{\mathrm{res}}]_\infty$ are

$$\alpha_0^*, x^{e_1+2}\alpha_1^*, \dots, x^{e_4+2}\alpha_4^* \text{ for } \mathbb{F}_q[\bar{C}]_\infty \quad \text{and} \quad \beta_0^*, x^{e'_1+2}\beta_1^*, \dots, x^{e'_5+2}\beta_5^* \text{ for } \mathbb{F}_q[\bar{C}^{\mathrm{res}}]_\infty,$$

where the $e'_i$ are the Maroni invariants of the resolvent. We now compute, for $i, j > 0$,

$$g_\infty(x^{e'_i+2}\beta_i^*, x^{e_j+2}\beta_j^*) = x^{e'_i+e'_j+4}x^{-g-4}g_0(\beta_i^*, \beta_j^*) \tag{12}$$

$$= \sum_{l=1}^{4} x^{-e_l-g-2+e'_i+e'_j}(\overline{M}_l)_{ij}(x^{e_l+2}\alpha_l^*). \tag{13}$$

It follows that $g_\infty$ is represented by the matrix whose entries have coefficients

$$x^{-e_l-g-2+e'_i+e'_j}(\overline{M}_l)_{ij}, \quad i, j = 1, \dots, 5, \ l = 1, \dots, 4.$$

But these coefficients belong to $\mathbb{F}_q[x^{-1}]$. Hence we find that $\deg(\overline{M}_l)_{ij} \le e_l + b_i + b_j + 6 - g$ by Theorem 5.3, as wanted. □

To compute such a liftable matrix in practice, we follow a similar approach as in the case of degree 4 covers. Namely, we will not be computing the fundamental resolvent map with respect to our reduced bases directly, but rather compute this for certain naive bases and apply change of basis. Concretely, consider the naive bases

$$1, y, y^2, y^3, y^4 \text{ for } \mathbb{F}_q(\bar{C}) \quad \text{and} \quad 1, y, y^2, y^3, y^4, y^5 \text{ for } \mathbb{F}_q(\bar{C}^{\mathrm{res}}),$$

along with the slightly altered fundamental resolvent map

$$g' : \mathbb{F}_q(\bar{C}^{\mathrm{res}}) \times \mathbb{F}_q(\bar{C}^{\mathrm{res}}) \to \mathbb{F}_q(\bar{C}) : (\alpha, \beta) \mapsto \sqrt{\operatorname{disc} \bar{f}} \cdot \begin{vmatrix} 1 & 1 & 1 \\ \alpha^{(1)} + \alpha^{(2)} & \alpha^{(3)} + \alpha^{(6)} & \alpha^{(4)} + \alpha^{(5)} \\ \beta^{(1)} + \beta^{(2)} & \beta^{(3)} + \beta^{(6)} & \beta^{(4)} + \beta^{(5)} \end{vmatrix}$$

where $\sqrt{\operatorname{disc} \bar{f}} = \det((y^i)^{(j)})_{0 \le i \le 4, 1 \le j \le 5}$. We compute the $\overline{M}'^{(r)}_{ij} \in \mathbb{F}_q[x]$ for which

$$g'(y^i, y^j) = \sum_{r=0}^{4} \overline{M}'^{(r)}_{ij} y^r,$$

giving five $5 \times 5$ skew-symmetric matrices $\overline{M}'^{(0)}, \dots, \overline{M}'^{(4)}$; here we used that $\overline{M}'^{(r)}_{ij} = 0$ as soon as $i$ or $j$ is zero, allowing us to disregard these terms. We call this the *naive model*.

**Remark 5.5.** It is important to note that these expressions can be computed symbolically in terms of the coefficients $\bar{f}_i$ of $\bar{f}$, by means of Vieta's formulas. Therefore this computation only has to be done once for all curves. This is in complete analogy with the degree 4 case, see (10). However, there the naive model was very simple, whereas this time the expressions involved are rather long. However, a computer has no trouble with these computations.

Now compute reduced bases $1, \alpha_1, \dots, \alpha_4$ for $\mathbb{F}_q[\bar{C}]_0$ and $1, \beta_1, \dots, \beta_5$ for $\mathbb{F}_q[\bar{C}^{\text{res}}]_0$ along with their corresponding dual bases. Acting on the naive model with a change of basis from the naive bases to the duals of these reduced bases, yields the altered resolvent map $g'$ with respect to these dual reduced bases. Note that this action will be by an element of $\mathrm{GL}_5(\mathbb{F}_q(x)) \times \mathrm{GL}_4(\mathbb{F}_q(x))$ rather than $\mathrm{GL}_5(\mathbb{F}_q[x]) \times \mathrm{GL}_4(\mathbb{F}_q[x])$. To obtain instead the resolvent map $g$ we have to multiply by

$$\frac{\sqrt{\operatorname{disc} \mathbb{F}_q[\bar{C}]_0}}{\sqrt{\operatorname{disc} \bar{f}}}.$$

Since we already have the reduced bases at hand, this factor is easiest to compute as the determinant of the change of basis matrix from the naive basis for $\mathbb{F}_q(\bar{C})$ to the reduced basis $1, \alpha_1, \dots, \alpha_4$.

At this point, we have a representation of the fundamental resolvent map $g$ with respect to the duals of the reduced bases for $\mathbb{F}_q[\bar{C}]_0$ and $\mathbb{F}_q[\bar{C}^{\text{res}}]_0$ as a $5 \times 5$ skew-symmetric matrix $\bar{M}$ with entries in $k[x][Y_1, Y_2, Y_3, Y_4]$, linear and homogeneous in the $Y_i$. This is the desired model, which we can lift naively, in a skew-symmetry preserving way, to a matrix having entries in $\mathcal{O}_K[x][Y_1, Y_2, Y_3, Y_4]$. Computing its five $4 \times 4$ sub-Pfaffians, dehomogenizing, and then eliminating variables finally returns our output (2), ready to be fed as input to Tuitman's algorithm.

## Acknowledgements

We thank Jan Tuitman and Yongqiang Zhao for several inspiring conversations, and the anonymous reviewers for their many helpful comments. This work is supported by CyberSecurity Research Flanders with reference VR20192203 and by KU Leuven with references C14/17/083 and C14/18/067.

## References

[1] P. Beelen, *A generalization of Baker's theorem*, Finite Fields and Their Applications **15**(5), pp. 558–568 (2009).

[2] M. Bhargava, *Higher composition laws III: The parametrization of quartic rings*, Annals of Mathematics **159**(3), pp. 1329–1360 (2004).

[3] M. Bhargava, *Higher composition laws IV: The parametrization of quintic rings*, Annals of Mathematics **167**(1), pp. 53–98 (2008).

[4] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24**(3–4), pp. 235–265 (1997).

[5] G. Casnati, *Covers of algebraic varieties III. The discriminant of a cover of degree 4 and the trigonal construction*, Transactions of the American Mathematical Society **350**(4), pp. 1359–1378 (1998).

[6] W. Castryck, J. Denef, F. Vercauteren, *Computing zeta functions of nondegenerate curves*, International Mathematics Research Papers **2006**, pp. 1–57 (2006).

[7] W. Castryck, J. Tuitman, *Point counting on curves using a gonality preserving lift*, The Quarterly Journal of Mathematics **69**(1), pp. 33–74 (2018).

[8] W. Castryck, F. Vermeulen, *Lifting low-gonal curves for use in Tuitman's algorithm*, preprint, arxiv (2020).

[9] W. Castryck, F. Vermeulen, Y. Zhao, *Syzygies, Galois representations and the geometry of function fields*, in preparation (2020).

[10] W. Castryck, J. Voight, *On nondegeneracy of curves*, Algebra & Number Theory **3**(3), pp. 255–281 (2009).

[11] D. A. Cox, *Galois theory*, $2^{\text{nd}}$ edition, John Wiley & Sons (2012).

[12] J. Denef, F. Vercauteren, *Computing zeta functions of hyperelliptic curves over finite fields of characteristic* 2, Advances in Cryptology – CRYPTO 2002, Lecture Notes in Computer Science **2442**, pp. 369–384 (2002).

[13] J. Denef, F. Vercauteren, *Counting points on $C_{ab}$ curves using Monsky–Washnitzer cohomology*, Finite Fields and Their Applications **12**(1), pp. 78–102 (2006).

[14] M. Derickx, *Torsion points on elliptic curves and gonalities of modular curves*, Master thesis, Universiteit Leiden (2012).

[15] D. Eisenbud, J. Harris, *On varieties of minimal degree (a centennial account)*, Proceedings of Symposia in Pure Mathematics **46**, pp. 3–13 (1987).

[16] W. Fulton, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Annals of Mathematics **90**(3), pp. 542–575 (1969).

[17] W.-T. Gan, B. Gross, G. Savin, *Fourier coefficients of modular forms on $G_2$*, Duke Mathematical Journal **115**(1), pp. 105–169 (2002).

[18] P. Gaudry, N. Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, Advances in Cryptology – ASIACRYPT 2001, Lecture Notes in Computer Science **2248**, pp. 480–494 (2001).

[19] B. van Geemen, *Some remarks on Brauer groups of K3 surfaces*, Advances in Mathematics **197**, pp. 222–247 (2005).

[20] F. Geiss, *The unirationality of Hurwitz spaces of* 6*-gonal curves of small genus*, Documenta Mathematica **17**, pp. 627–640 (2012).

[21] F. Hess, *Computing Riemann–Roch spaces in algebraic function fields and related topics*, Journal of Symbolic Computation **33**(4), pp. 425–445 (2002).

[22] K. S. Kedlaya, *Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology*, Journal of the Ramanujan Mathematical Society **16**(4), pp. 323–338 (2001).

[23] A. Khovanskii, *Newton polyhedra and the genus of complete intersections*, Functional Analysis and its Applications **12**(1), pp. 38–46 (1978).

[24] J. Schicho, F.-O. Schreyer, M. Weimann, *Computational aspects of gonal maps and radical parametrization of curves*, Applicable Algebra in Engineering, Communication and Computing **24**(5), pp. 313–341 (2013).

[25] F.-O. Schreyer, *Syzygies of canonical curves and special linear series*, Mathematische Annalen **275**(1), pp. 105–137 (1986).

[26] F.-O. Schreyer, F. Tanturri, *Matrix factorizations and curves in $\mathbb{P}^4$*, Documenta Mathematica **23**, pp. 1895–1924 (2018).

[27] B. Segre, *Sui moduli delle curve poligonale, e sopra un complemento al teorema diesistenza di Riemann*, Mathematische Annalen **100**, pp. 537–551 (1928)

[28] J. Tuitman, *Counting points on curves using a map to $\mathbb{P}^1$*, Mathematics of Computation **85**(298), pp. 961–981 (2016).

[29] J. Tuitman, *Counting points on curves using a map to $\mathbb{P}^1$, II*, Finite Fields and Their Applications **45**, pp. 301–322 (2017).

[30] F. Vermeulen, *Lifting curves of low gonality*, Master thesis, KU Leuven (2019), available at https://sites.google.com/view/floris-vermeulen/.

[31] Y. Zhao, *On sieve methods for varieties over finite fields*, Ph.D. thesis, University of Wisconsin Madison (2013).

Received 23 Feb 2020. Revised 19 Jul 2020.

WOUTER CASTRYCK: wouter.castryck@kuleuven.be
*Department ESAT, imec-COSIC, KU Leuven, Leuven, Belgium*

and

*Department of Mathematics: Algebra and Geometry, Ghent University, Belgium*

FLORIS VERMEULEN: floris.vermeulen@kuleuven.be
*Department of Mathematics, KU Leuven, Leuven, Belgium*

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

The cover image is based on an illustration from the article “Supersingular curves with small noninteger endomorphisms”, by Jonathan Love and Dan Boneh (see p. 9).

Electronic copies can be obtained free of charge from http://msp.org/obs/4 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.

msp

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org http://msp.org

THE OPEN BOOK SERIES 4

# Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

## TABLE OF CONTENTS