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

Wouter Castryck and Floris Vermeulen

KU Leuven

July 2020

Tuitman's algorithm

- Given $\overline{C}/\mathbb{F}_q$, how can we efficiently compute the zeta function of $\overline{C}$?

Tuitman's algorithm

- Given $\overline{C}/\mathbb{F}_q$, how can we efficiently compute the zeta function of $\overline{C}$?
- Kedlaya: hyperelliptic curves.

Tuitman's algorithm

- Given $\overline{C}/\mathbb{F}_q$, how can we efficiently compute the zeta function of $\overline{C}$?
- Kedlaya: hyperelliptic curves.
- Subsequently generalized to larger classes of curves by Gaudry–Gürel, (Castryck–)Denef–Vercauteren, ...

Tuitman's algorithm

- Given $\overline{C}/\mathbb{F}_q$, how can we efficiently compute the zeta function of $\overline{C}$?
- Kedlaya: hyperelliptic curves.
- Subsequently generalized to larger classes of curves by Gaudry–Gürel, (Castryck–)Denef–Vercauteren, ...
- Tuitman: arbitrary* curves $\overline{C}$ equipped with a map $\overline{\varphi} : \overline{C} \to \mathbb{P}^1$.

Tuitman's algorithm

- Given $\overline{C}/\mathbb{F}_q$, how can we efficiently compute the zeta function of $\overline{C}$?
- Kedlaya: hyperelliptic curves.
- Subsequently generalized to larger classes of curves by Gaudry–Gürel, (Castryck–)Denef–Vercauteren, ...
- Tuitman: arbitrary* curves $\overline{C}$ equipped with a map $\overline{\varphi} : \overline{C} \to \mathbb{P}^1$.
- Tuitman's algorithm requires a *lift* of $(\overline{C}, \overline{\varphi})$ to (C, φ) defined over K with some technical conditions.

The lifting problem

Fix a number field K, with $\mathcal{O}_K/p = \mathbb{F}_q$.

The lifting problem

Fix a number field K, with $\mathcal{O}_K/p = \mathbb{F}_q$. Consider a planar curve over $\mathbb{F}_q$ defined by

$$\overline{f}(x,y) = \overline{f}_d(x)y^d + \overline{f}_{d-1}(x)y^{d-1} + ... + \overline{f}_0(x) = 0,$$

with $d \leq 5$ and denote by $\overline{C}$ the non-singular model. Let $\overline{\varphi}$ be projection onto x and assume that $\overline{\varphi}$ is simply branched.

The lifting problem

Fix a number field K, with $\mathcal{O}_K/p = \mathbb{F}_q$. Consider a planar curve over $\mathbb{F}_q$ defined by

$$\overline{f}(x,y) = \overline{f}_d(x)y^d + \overline{f}_{d-1}(x)y^{d-1} + \ldots + \overline{f}_0(x) = 0,$$

with $d \leq 5$ and denote by $\overline{C}$ the non-singular model. Let $\overline{\varphi}$ be projection onto x and assume that $\overline{\varphi}$ is simply branched. The lifting problem asks for a non-singular curve C defined over K, together with a map $\varphi : C \to \mathbb{P}^1$ such that

- the reduction of C mod p is isomorphic to $\overline{C}$, in particular the genus is preserved, and

The lifting problem

Fix a number field K, with $\mathcal{O}_K/p = \mathbb{F}_q$. Consider a planar curve over $\mathbb{F}_q$ defined by

$$\overline{f}(x,y) = \overline{f}_d(x)y^d + \overline{f}_{d-1}(x)y^{d-1} + \ldots + \overline{f}_0(x) = 0,$$

with $d \leq 5$ and denote by $\overline{C}$ the non-singular model. Let $\overline{\varphi}$ be projection onto x and assume that $\overline{\varphi}$ is simply branched. The lifting problem asks for a non-singular curve C defined over K, together with a map $\varphi : C \to \mathbb{P}^1$ such that

- the reduction of C mod p is isomorphic to $\overline{C}$, in particular the genus is preserved, and
- the reduction of φ mod p is $\overline{\varphi}$.

Reduced bases

Let $\mathbb{F}_q[\overline{C}]_0$ (resp. $\mathbb{F}_q[\overline{C}]_\infty$) be the integral closure of $\mathbb{F}_q[x]$ (resp. $\mathbb{F}_q[1/x]$) inside $\mathbb{F}_q(\overline{C})$.

Reduced bases

Let $\mathbb{F}_q[\overline{C}]_0$ (resp. $\mathbb{F}_q[\overline{C}]_\infty$) be the integral closure of $\mathbb{F}_q[x]$ (resp. $\mathbb{F}_q[1/x]$) inside $\mathbb{F}_q(\overline{C})$.

Theorem (Hess)

Let k be a field and $k(C)$ a degree d function field. There exist unique negative integers $r_1 \geq r_2 \geq \ldots \geq r_{d-1}$ for which there is a basis $1, \alpha_1, \ldots, \alpha_{d-1}$ of $k[C]_0$ over $k[x]$ such that $1, x^{r_1}\alpha_1, \ldots, x^{r_{d-1}}\alpha_{d-1}$ is a basis of $k[C]_\infty$ over $k[1/x]$.

Reduced bases

Let $\mathbb{F}_q[\overline{C}]_0$ (resp. $\mathbb{F}_q[\overline{C}]_\infty$) be the integral closure of $\mathbb{F}_q[x]$ (resp. $\mathbb{F}_q[1/x]$) inside $\mathbb{F}_q(\overline{C})$.

Theorem (Hess)

Let k be a field and $k(C)$ a degree d function field. There exist unique negative integers $r_1 \geq r_2 \geq \ldots \geq r_{d-1}$ for which there is a basis $1, \alpha_1, \ldots, \alpha_{d-1}$ of $k[C]_0$ over $k[x]$ such that $1, x^{r_1}\alpha_1, \ldots, x^{r_{d-1}}\alpha_{d-1}$ is a basis of $k[C]_\infty$ over $k[1/x]$.

Compare with Minkowski reduced bases.

Reduced bases

Let $\mathbb{F}_q[\overline{C}]_0$ (resp. $\mathbb{F}_q[\overline{C}]_\infty$) be the integral closure of $\mathbb{F}_q[x]$ (resp. $\mathbb{F}_q[1/x]$) inside $\mathbb{F}_q(\overline{C})$.

Theorem (Hess)

Let k be a field and $k(C)$ a degree d function field. There exist unique negative integers $r_1 \geq r_2 \geq \ldots \geq r_{d-1}$ for which there is a basis $1, \alpha_1, \ldots, \alpha_{d-1}$ of $k[C]_0$ over $k[x]$ such that $1, x^{r_1}\alpha_1, \ldots, x^{r_{d-1}}\alpha_{d-1}$ is a basis of $k[C]_\infty$ over $k[1/x]$.

Compare with Minkowski reduced bases. We call $e_i = -r_i - 2$ the *Maroni invariants* of $\overline{C}$ with respect to $\overline{\varphi}$. A corresponding basis is called a *reduced basis*.

Reduced bases

Let $\mathbb{F}_q[\overline{C}]_0$ (resp. $\mathbb{F}_q[\overline{C}]_\infty$) be the integral closure of $\mathbb{F}_q[x]$ (resp. $\mathbb{F}_q[1/x]$) inside $\mathbb{F}_q(\overline{C})$.

Theorem (Hess)

Let k be a field and $k(C)$ a degree d function field. There exist unique negative integers $r_1 \geq r_2 \geq \ldots \geq r_{d-1}$ for which there is a basis $1, \alpha_1, \ldots, \alpha_{d-1}$ of $k[C]_0$ over $k[x]$ such that $1, x^{r_1}\alpha_1, \ldots, x^{r_{d-1}}\alpha_{d-1}$ is a basis of $k[C]_\infty$ over $k[1/x]$.

Compare with Minkowski reduced bases. We call $e_i = -r_i - 2$ the *Maroni invariants* of $\overline{C}$ with respect to $\overline{\varphi}$. A corresponding basis is called a *reduced basis*. We have

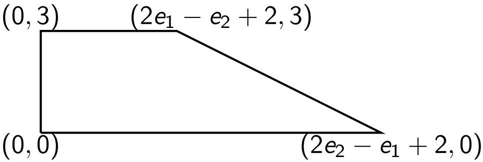
- $-1 \leq e_1 \leq ... \leq e_{d-1} \leq \frac{2g-2}{d}$,
- $e_1 + ... + e_{d-1} = g - d + 1$.

Liftable models in degree $d = 3$

There is a model of $\overline{C}$ of the form

$$\overline{f}_3(x)y^3 + \overline{f}_2(x)y^2z + \overline{f}_1(x)yz^2 + \overline{f}_0(x)z^3 = 0$$

inside $\mathbb{A}^1 \times \mathbb{P}^1$ with Newton polygon ($z = 1$)

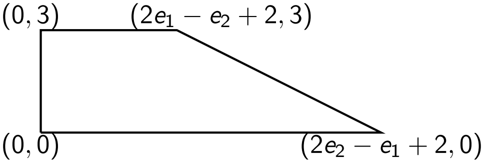


Liftable models in degree $d = 3$

There is a model of $\overline{C}$ of the form

$$\overline{f}_3(x)y^3 + \overline{f}_2(x)y^2z + \overline{f}_1(x)yz^2 + \overline{f}_0(x)z^3 = 0$$

inside $\mathbb{A}^1 \times \mathbb{P}^1$ with Newton polygon $(z = 1)$



Such a model can be lifted naively to $\mathcal{O}_K$. How to compute this explicitly?

The Delone–Faddeev correspondence

A *cubic ring* R over $\mathbb{F}_q[x]$ is an $\mathbb{F}_q[x]$-algebra, free of rank 3 as an $\mathbb{F}_q[x]$-module.

The Delone–Faddeev correspondence

A *cubic ring* R over $\mathbb{F}_q[x]$ is an $\mathbb{F}_q[x]$-algebra, free of rank 3 as an $\mathbb{F}_q[x]$-module.

Theorem (Delone, Faddeev)

There is a canonical bijection between cubic rings R over $\mathbb{F}_q[x]$, up to isomorphism, and binary cubic forms over $\mathbb{F}_q[x]$, up to an action of $\mathrm{GL}_2(\mathbb{F}_q[x])$.

- Change of basis of the ring R corresponds to the action of GL_2.

The Delone–Faddeev correspondence

A *cubic ring* R over $\mathbb{F}_q[x]$ is an $\mathbb{F}_q[x]$-algebra, free of rank 3 as an $\mathbb{F}_q[x]$-module.

Theorem (Delone, Faddeev)

There is a canonical bijection between cubic rings R over $\mathbb{F}_q[x]$, up to isomorphism, and binary cubic forms over $\mathbb{F}_q[x]$, up to an action of $\mathrm{GL}_2(\mathbb{F}_q[x])$.

- Change of basis of the ring R corresponds to the action of GL_2.
- The bijection is very explicit and can be done on a computer.

Lifting in degree $d = 3$

- Consider the cubic ring $\mathbb{F}_q[\overline{C}]_0$ over $\mathbb{F}_q[x]$.

Lifting in degree $d = 3$

- Consider the cubic ring $\mathbb{F}_q[\overline{C}]_0$ over $\mathbb{F}_q[x]$.
- Apply the Delone–Faddeev correspondence to $\mathbb{F}_q[\overline{C}]_0$ together with a reduced basis to obtain a binary cubic form $\overline{f}(x; y, z)$.

Lifting in degree $d = 3$

- Consider the cubic ring $\mathbb{F}_q[\overline{C}]_0$ over $\mathbb{F}_q[x]$.
- Apply the Delone–Faddeev correspondence to $\mathbb{F}_q[\overline{C}]_0$ together with a reduced basis to obtain a binary cubic form $\overline{f}(x; y, z)$.
- $\overline{f}(x; y, z) = 0$ defines a model of $\overline{C}$.

Lifting in degree $d = 3$

- Consider the cubic ring $\mathbb{F}_q[\overline{C}]_0$ over $\mathbb{F}_q[x]$.
- Apply the Delone–Faddeev correspondence to $\mathbb{F}_q[\overline{C}]_0$ together with a reduced basis to obtain a binary cubic form $\overline{f}(x; y, z)$.
- $\overline{f}(x; y, z) = 0$ defines a model of $\overline{C}$.
- This polynomial can be lifted to $\mathcal{O}_K$ naively.

Lifting in degree $d = 3$

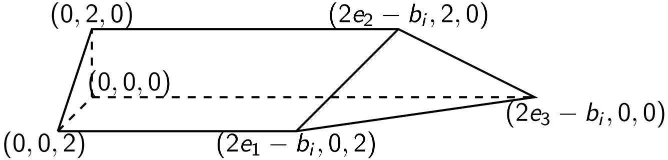
- Consider the cubic ring $\mathbb{F}_q[\overline{C}]_0$ over $\mathbb{F}_q[x]$.
- Apply the Delone–Faddeev correspondence to $\mathbb{F}_q[\overline{C}]_0$ together with a reduced basis to obtain a binary cubic form $\overline{f}(x; y, z)$.
- $\overline{f}(x; y, z) = 0$ defines a model of $\overline{C}$.
- This polynomial can be lifted to $\mathcal{O}_K$ naively.
- All of this can be done algorithmically, and we have implemented this in Magma.

Liftable models in degree $d = 4$

There is a model of $\overline{C}$ in $\mathbb{A}^1 \times \mathbb{P}^2$ defined as a complete intersection by

$$\overline{Q}_1(x; y_1, y_2, y_3) = \overline{Q}_2(x; y_1, y_2, y_3) = 0,$$

where $\overline{Q}_i$ has Newton polytope ($y_3 = 1$)

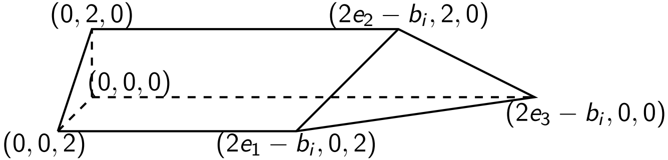


Liftable models in degree $d = 4$

There is a model of $\overline{C}$ in $\mathbb{A}^1 \times \mathbb{P}^2$ defined as a complete intersection by

$$\overline{Q}_1(x; y_1, y_2, y_3) = \overline{Q}_2(x; y_1, y_2, y_3) = 0,$$

where $\overline{Q}_i$ has Newton polytope ($y_3 = 1$)



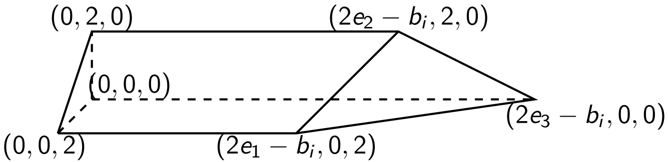
Here $b_1 \leq b_2$ are certain integers satisfying $b_1 + b_2 = g - 5$.

Liftable models in degree $d = 4$

There is a model of $\overline{C}$ in $\mathbb{A}^1 \times \mathbb{P}^2$ defined as a complete intersection by

$$\overline{Q}_1(x; y_1, y_2, y_3) = \overline{Q}_2(x; y_1, y_2, y_3) = 0,$$

where $\overline{Q}_i$ has Newton polytope ($y_3 = 1$)



Here $b_1 \leq b_2$ are certain integers satisfying $b_1 + b_2 = g - 5$. Such a model is naively liftable to $\mathcal{O}_K$. How do we compute it?

The Bhargava correspondence

Theorem (Bhargava)

There is a canonical bijection between pairs (R, S) *where* R *is a quartic ring over* $\mathbb{F}_q[x]$ *and* S *is a cubic resolvent of* R*, up to isomorphism, and pairs* (Q_1, Q_2) *of ternary quadratic forms over* $\mathbb{F}_q[x]$*, up to an action of* $\mathrm{GL}_3(\mathbb{F}_q[x]) \times \mathrm{GL}_2(\mathbb{F}_q[x])$.

The Bhargava correspondence

Theorem (Bhargava)

There is a canonical bijection between pairs (R, S) where R is a quartic ring over $\mathbb{F}_q[x]$ and S is a cubic resolvent of R, up to isomorphism, and pairs (Q_1, Q_2) of ternary quadratic forms over $\mathbb{F}_q[x]$, up to an action of $\mathrm{GL}_3(\mathbb{F}_q[x]) \times \mathrm{GL}_2(\mathbb{F}_q[x])$.

- Change of basis of R (resp. S) corresponds to action of GL_3 (resp. GL_2).

The Bhargava correspondence

Theorem (Bhargava)

There is a canonical bijection between pairs (R, S) where R is a quartic ring over $\mathbb{F}_q[x]$ and S is a cubic resolvent of R, up to isomorphism, and pairs (Q_1, Q_2) of ternary quadratic forms over $\mathbb{F}_q[x]$, up to an action of $\mathrm{GL}_3(\mathbb{F}_q[x]) \times \mathrm{GL}_2(\mathbb{F}_q[x])$.

- Change of basis of R (resp. S) corresponds to action of GL_3 (resp. GL_2).
- The cubic resolvent of $\mathbb{F}_q[\overline{C}]_0$ is of the form $\mathbb{F}_q[\overline{C}']_0$ for some cubic function field $\mathbb{F}_q(\overline{C}')/\mathbb{F}_q(x)$.

Lifting in degree $d = 4$

- Consider the ring $\mathbb{F}_q[\overline{C}]_0$ and its resolvent S over $\mathbb{F}_q[x]$.

Lifting in degree $d = 4$

- Consider the ring $\mathbb{F}_q[\overline{C}]_0$ and its resolvent S over $\mathbb{F}_q[x]$.
- Apply the Bhargava correspondence to $(\mathbb{F}_q[\overline{C}]_0, S)$ together with reduced bases for both to get two ternary quadratic forms $\overline{Q}_1, \overline{Q}_2$ over $\mathbb{F}_q[x]$.

Lifting in degree $d = 4$

- Consider the ring $\mathbb{F}_q[\overline{C}]_0$ and its resolvent S over $\mathbb{F}_q[x]$.
- Apply the Bhargava correspondence to $(\mathbb{F}_q[\overline{C}]_0, S)$ together with reduced bases for both to get two ternary quadratic forms $\overline{Q}_1, \overline{Q}_2$ over $\mathbb{F}_q[x]$.
- $\overline{Q}_1 = \overline{Q}_2 = 0$ defines a model of $\overline{C}$.

Lifting in degree $d = 4$

- Consider the ring $\mathbb{F}_q[\overline{C}]_0$ and its resolvent S over $\mathbb{F}_q[x]$.
- Apply the Bhargava correspondence to $(\mathbb{F}_q[\overline{C}]_0, S)$ together with reduced bases for both to get two ternary quadratic forms $\overline{Q}_1, \overline{Q}_2$ over $\mathbb{F}_q[x]$.
- $\overline{Q}_1 = \overline{Q}_2 = 0$ defines a model of $\overline{C}$.
- These polynomials can be lifted to $\mathcal{O}_K$ naively.

Lifting in degree $d = 4$

- Consider the ring $\mathbb{F}_q[\overline{C}]_0$ and its resolvent S over $\mathbb{F}_q[x]$.
- Apply the Bhargava correspondence to $(\mathbb{F}_q[\overline{C}]_0, S)$ together with reduced bases for both to get two ternary quadratic forms $\overline{Q}_1, \overline{Q}_2$ over $\mathbb{F}_q[x]$.
- $\overline{Q}_1 = \overline{Q}_2 = 0$ defines a model of $\overline{C}$.
- These polynomials can be lifted to $\mathcal{O}_K$ naively.
- All of this can be done algorithmically, and we have implemented it in Magma.

Closing remarks

- The case $d = 5$ is very similar to the case $d = 4$. This time relying on Bhargava's parametrization of quintic rings.

Closing remarks

- The case $d = 5$ is very similar to the case $d = 4$. This time relying on Bhargava's parametrization of quintic rings.
- Works well in practice, running time is dominated by Tuitman's algorithm.

Closing remarks

- The case $d = 5$ is very similar to the case $d = 4$. This time relying on Bhargava's parametrization of quintic rings.
- Works well in practice, running time is dominated by Tuitman's algorithm.
- $d \geq 7$ is impossible by the non-unirationality of the Hurwitz spaces $\mathcal{H}_{d,g}$. Degree $d = 6$ is not known.

Closing remarks

- The case $d = 5$ is very similar to the case $d = 4$. This time relying on Bhargava's parametrization of quintic rings.
- Works well in practice, running time is dominated by Tuitman's algorithm.
- $d \geq 7$ is impossible by the non-unirationality of the Hurwitz spaces $\mathcal{H}_{d,g}$. Degree $d = 6$ is not known.
- Computing these liftable models is possible over many fields, not just finite fields.