# Short models of global fields

Jean-Marc Couveignes

# SHORT MODELS OF GLOBAL FIELDS

JEAN-MARC COUVEIGNES

ABSTRACT. We construct compact descriptions of function fields and number fields.

## CONTENTS



Given a field of scalars $K$ and an indeterminate $x$, a natural way to describe a function field $K(C)/K(x)$ over $K(x)$ with degree $n$ and genus $g$ is to choose a primitive element in it and to give its minimal polynomial. This is a polynomial in $K(x)[y]$ and even in $K[x,y]$ once we have cleared denominators. It has degree $n$ in $y$ and its degree in $x$ cannot be expected to be significantly smaller than the genus $g$ of the curve $C$ in general. So this plane model involves about $ng$ coefficients while the dimension of the underlying modular problem is rather linear in $n+g$. Indeed a plane model of a general curve of genus $g$ tends to have singularities and tells more about these singularities than about the function field itself. Another more natural possibility to

*Date*: November 5, 2020.

represent a function field $K(C)/K(x)$ is to consider the canonical model of the curve $C$ and express $x$ as a rational fraction of the holomorphic differentials. Even Petri's description of the ideal of canonical curves [3, Chapter III, §3] however involves a number of parameters that is quadratic in the genus $g$.

Similarly, a natural way to describe a number field $\mathbf{K}/\mathbf{Q}$ of degree $n$ and root discriminant $\delta_{\mathbf{K}}$ is to choose a primitive element in it and give its minimal polynomial. This is a polynomial in $\mathbf{Q}[x]$ and even in $\mathbf{Z}[x]$ once we have cleared denominators. It has degree $n$ in $x$ and its height cannot be expected to be significantly smaller than the absolute value of the discriminant $|d_{\mathbf{K}}| = \delta_{\mathbf{K}}^n$ in general. So this model has bit size of order $n \times \log |d_{\mathbf{K}}|$ while the logarithm of the number of number fields of degree $n$ and discriminant bounded by $D$ in absolute value is conjectured [7, 12], and even proven for $n \leqslant 5$ [9, 5, 6], to be bounded by $\log D$ plus a function of $n$ alone. The reason for this discrepancy is that the quotient ring of $\mathbf{Z}[x]$ by a unitary irreducible polynomial tends to be highly singular and provides more information than the mere isomorphism class of the corresponding number field.

In this text we construct two families of natural models for a function field of genus $g$ and degree $n$ over $K(x)$ where $K$ is a field of cardinality $q$. These models involve a number of coefficients in $K$ of order $n(\log n)^3(g/n+1+\log_q n)$ and $n(\log n)^2(g/n+1+\log_q n)$ respectively. In case $q = +\infty$ we set $\log_q n = 0$ in these formulae. The first model is obtained by picking few functions $(\kappa_j)_{1\leqslant j\leqslant r}$ of small degree in $K(C)$ and finding enough relations with small degree between them to produce local equations for an affine model of $C$. The second model is obtained from the first one by providing long enough formal series expansions of the $\kappa_j$ to be able to recover the equations. This second model is unambiguous: we can recover the full ideal of relations from these formal expansions, not just local equations. It is also a bit smaller. It consists of a finite $0$-dimentional affine $K$-scheme (a finite set in a finite $K$-algebra) that pins down a model of $C$.

Using (not so) parallel constructions in number theory we propose two families of models for a number field, having bit size of order $n(\log n)^3(\log \delta_K + \log n)$ and $n(\log n)^2(\log \delta_K + \log n)$ respectively. The first model, which was already presented in [8], is obtained by picking few small integers $(\kappa_j)_{1\leqslant j\leqslant r}$ in $\mathbf{K}$ and finding enough relations with small degree and small height between them to produce local equations for an affine model of $\operatorname{Spec}\mathbf{K}$. The second model is obtained from the first one by picking a small unramified prime $p$ an providing long enough $p$-adic approximations of the $\kappa_j$ to characterize the number field. Again this second model is unambiguous and a bit smaller. It consists of a finite $0$-dimentional affine scheme (a finite set in a finite algebra) that pins down a model of $\operatorname{Spec}\mathbf{K}$.

In this text, the notation $\mathcal{Q}$ stands for a positive absolute constant. Any sentence containing this symbol becomes true if the symbol is replaced in every occurrence by some large enough real number.

## 1. Definitions and main statements

We recall notation about function fields and number fields. We then define two ways of specifying a function field $K(C)$. We can provide local equations for a $0$-dimentional variety over the rational field $K(x)$ such that the function field $K(C)$ is the residue field of this variety.

We can also provide formal expansions for the coordinates of some formal point on the former model. We state the existence of small models of either kind for any function field $K(C)/K(x)$. We similarly define two ways of specifying a number field $\mathbf{K}$. One option is to provide local equations for a 0-dimentional variety over $\mathbf{Q}$ such that the number field $\mathbf{K}$ is the residue field of this variety. Another option is to provide $p$-adic expansions for the coordinates of some $p$-infinitesimal point on the former model, with enough accuracy to recover the equations. We state the existence of small models of either kind for any number field $\mathbf{K}$.

1.1. **Function fields.** Let $K$ be a field. Let $q$ be the cardinality of $K$. If $q$ is finite we write $\log_q$ for the logarithm function with base $q$. If $q = +\infty$ then $\log_q$ is the constant zero function. Let $\mathbf{P}^1_K = \operatorname{Proj} K[x_0, x_1]$ be the projective line over $K$. Let $x = x_1/x_0$ and let $\mathbf{A}^1_K = \operatorname{Spec} K[x]$ be the affine line over $K$. We call $\infty$ the point $(0, 1)$ on $\mathbf{P}^1_K$ with projective coordinate $x_0 = 0$. Let $C$ be a smooth absolutely integral projective curve over $K$. Let $f : C \to \mathbf{P}^1$ be a finite separable map and let $K(C)/K(x)$ be the corresponding regular field extension. In this paper we shall call such an extension a **function field**. We shall denote $n$ the degree of $f$ and $g$ the genus of $C$.

1.2. **Function fields as incomplete intersections.** Let $K(C)/K(x)$ be a function field as in Section 1.1. Let $r \geqslant 1$, $d_x \geqslant 1$ and $d_y \geqslant 1$ be integers. Let $y_1, \ldots, y_r$ be indeterminates. Let $E_1$, $E_2, \ldots, E_r$ be polynomials in $K[x][y_1, \ldots, y_r]$ with total degree $\leqslant d_y$ in the $y_j$ and with degree $\leqslant d_x$ in $x$. Let $\mathcal{I} \to \mathbf{A}^1 = \operatorname{Spec} K[x]$ be the $K[x]$-scheme with equations

$$E_1 = E_2 = \cdots = E_r = 0 \text{ and } \det\left(\partial E_i/\partial y_j\right)_{1 \leqslant i,\, j \leqslant r} \neq 0.$$

We assume that the generic fiber $\mathcal{I} \otimes K(x) \to \operatorname{Spec} K(x)$ has an irreducible component isomorphic to $\operatorname{Spec} K(C) \to \operatorname{Spec} K(x)$. We call $\mathcal{C} \to \mathbf{A}^1 = \operatorname{Spec} K[x]$ the Zariski closure of this component in $\mathcal{I}$. We say that $\mathcal{C} \to \mathbf{A}^1$ is an **incomplete intersection model** of the function field in dimension $r$ and degrees $(d_x, d_y)$.

1.3. **Interpolant of an infinitesimal point.** Let $r \geqslant 1$, $m \geqslant 1$, $d_x \geqslant 1$ and $d_y \geqslant 1$ be integers. Let $K$ be a field. Let $L \supset K$ be a finite separable field extension and let $l$ be its degree. Let $\lambda$ be a primitive element in $L$. Let $S \supset L$ be a finite separable field extension and let $s$ be its degree. Let $t$ be an indeterminate. Let $b_1^m, \ldots, b_r^m$ be $r$ elements in $S[[t]]/t^m$. Let

$$a^\infty = \lambda + t \in S[[t]] \quad \text{and} \quad a^m = a^\infty \bmod t^m \in S[[t]]/t^m.$$

Let $x, y_1, \ldots, y_r$ be $r + 1$ indeterminates. Let

$$\beta^m : K[x][y_1, \ldots, y_r] \to S[[t]]/t^m$$

be the morphism of $K$-algebras that maps $x$ onto $a^m$ and $y_j$ onto $b_j^m$ for $1 \leqslant j \leqslant r$. We assume that $\beta^m$ is surjective. We denote by $b^m$ the corresponding $S[[t]]/t^m$ point on $\mathbf{A}^{r+1}$.

Let $J_{d_x,d_y}$ be the ideal of $K[x][y_1, \ldots, y_r]$ generated by all polynomials in $\operatorname{Ker} \beta^m$ having total degree $\leqslant d_y$ in $y_1, \ldots, y_r$ and degree $\leqslant d_x$ in $x$. We say that a point

$$b^\infty = (a^\infty, b_1^\infty, \ldots, b_r^\infty) \in (S[[t]])^{r+1}$$

is the **interpolant** of $b^m$ in degrees $(d_x, d_y)$ if

(1) $b_j^\infty \bmod t^m = b_j^m$ for every $1 \leqslant j \leqslant r$,
(2) all polynomials in $J_{d_x,d_y}$ vanish at $b^\infty$,

(3) and $b^\infty$ is **unique** with the two above properties.

1.4. **Short models of function fields.** We shall prove that both incomplete intersections and interpolants provide short descriptions of function fields.

**Theorem 1** (Function fields as small incomplete intersections)**.** *The exists an absolute constant $\mathcal{Q}$ such that the following is true. Let $K$ be a field and let $K(C)/K(x)$ be a function field of genus $g \geqslant 2$ and degree $n$ as in Section 1.1. Let $q$ be the, possibly infinite, cardinality of $K$. Call $r$ the smallest positive integer such that*

$$\binom{2r}{r} \geqslant n(r+1).$$

*Let $h$ be smallest non-negative integer such that*

$$q^{h+1} > nr(r+1).$$

*Let*

$$\nu = 2 + \left\lceil \frac{2(g-1)}{n} \right\rceil \quad \text{and} \quad d_x = r(h+\nu) \quad \text{and} \quad d_y = r.$$

*There exists an incomplete intersection model of $K(C)/K(x)$ in dimension $r$ and degrees $(d_x, d_y)$. The total number of $K$-coefficients in this model is*

$$\leqslant \mathcal{Q}(\log n)^3(g + n(1+\log_q n)).$$

The meaning of this theorem is that we have a short description of $K(C)/K(x)$ as a quotient of a finite algebra : the smooth zero-dimensional part of a complete intersection of small degree in a projective space of small dimension. In particular the number of affine parameters required to decribe the incomplete intersection is almost linear in $g+n$. There remains a little uncertainty concerning which irreducible component of the complete intersection is of interest to us. One way of removing this uncertainty if to specify a geometric point on the targeted component. We then realize that giving enough such geometric points (counting multiplicities) enables us to reconstruct the equations. This leads us to the next theorem.

**Theorem 2** (Function fields from interpolants)**.** *The exists an absolute constant $\mathcal{Q}$ such that the following is true. Let $K$ be a field and let $K(C)/K(x)$ be a function field of genus $g \geqslant 2$ and degree $n$ as in Section 1.1. Let $q$ be the, possibly infinite, cardinality of $K$. Let $r$, $h$, $\nu$, $d_x$ and $d_y$ be as in Theorem 1. Let*

$$\rho = d_x + r(\nu + h).$$

*There exist integers $l$, $s$, $m$ and finite separable field extensions $L/K$ and $S/L$ of respective degrees $l$ and $s$, and an element $\lambda$ in $K$ such that $L = K(\lambda)$, and a point*

$$b^m = (\lambda + t \bmod t^m, b_1^m, \ldots, b_r^m) \in (S[[t]]/t^m)^{r+1}$$

*such that $b^m$ has an interpolant*

$$b^\infty = (\lambda + t, b_1^\infty, \ldots, b_r^\infty) \in (S[[t]])^{r+1}$$

*in degrees $(d_x, d_y)$. And there is an isomorphism of $K$-algebras from*

$$K(\lambda + t, b_1^\infty, \ldots, b_r^\infty) \subset S[[t]]$$

*onto $K(C) \supset K(x)$ that sends $\lambda + t$ onto $x$. Further*

$$1 \leqslant l \leqslant \mathcal{O}(1 + \log_q(1 + g/n) + \log_q n) \quad \textit{and} \quad 1 \leqslant s \leqslant n,$$

*and $m$ is the smallest positive integer such that $mls > n\rho$, and*

$$rmls \leqslant \mathcal{Q}(\log n)^2 \left(n(1 + \log_q n) + g\right).$$

The meaning of this theorem is that a model of the function field can be recovered from short formal expansions of a few functions in it. The function field is recovered from $r$ formal expansions of length $m$ having coefficients in an extension of degree $ls$ of $K$. This involves $rmls$ coefficients in $K$. So the number of parameters in this model is bounded by $\mathcal{Q}(\log n)^2 \left(n(1 + \log_q n) + g\right)$.

1.5. **Number fields.** By a number field we mean a finite field extension $\mathbf{K}/\mathbf{Q}$ of the rational field. We denote by $n$ the degree of this extension and by $\mathbf{O}$ the ring of integers of $\mathbf{K}$. We denote by $(\rho_i)_{1\leqslant i\leqslant r}$ the $r$ real embeddings of $\mathbf{K}$ and by $(\sigma_j, \bar{\sigma}_j)_{1\leqslant j\leqslant s}$ the $2s$ complex embeddings of $\mathbf{K}$. We also denote by $(\tau_k)_{1\leqslant k\leqslant n}$ the $n = r + 2s$ embeddings of $\mathbf{K}$. We let

$$\mathbf{K}_\mathbf{R} = \mathbf{K} \otimes_\mathbf{Q} \mathbf{R} = \mathbf{R}^r \times \mathbf{C}^s$$

be the Minkowski space. We follow the presentation in [14, Chapitre 1, §5]. An element $x$ of $\mathbf{K}_\mathbf{R}$ can be given by $r$ real components $(x_\rho)_\rho$ and $s$ complex components $(x_\sigma)_\sigma$. So we write $x = ((x_\rho)_\rho, (x_\sigma)_\sigma)$. For such an $x$ in $\mathbf{K}_\mathbf{R}$ we denote by $\|x\|$ the maximum of the absolute values of its $r + s$ components. The canonical metric on $\mathbf{K}_\mathbf{R}$ is defined by

$$< x, y >= \sum_{1\leqslant i\leqslant r} x_i y_i + \sum_{1\leqslant j\leqslant s} x_j \bar{y}_j + \bar{x}_j y_j.$$

The corresponding Haar measure is said to be canonical also. The canonical measure of the convex body $\{x, \|x\| \leqslant 1\}$ is

$$2^r (2\pi)^s \geqslant 2^n.$$

The map $a \mapsto a \otimes 1$ injects $\mathbf{K}$ and $\mathbf{O}$ into $\mathbf{K}_\mathbf{R}$. For every non-zero $x$ in $\mathbf{O}$ we have

$$\|x\| \geqslant 1.$$

Let $(\alpha_i)_{1\leqslant i\leqslant n}$ be any $\mathbf{Z}$-basis of $\mathbf{O}$. Set $A = (\tau_j(\alpha_i))_{1\leqslant i,j\leqslant n}$. The product $A\bar{A}^t$ is the Gram matrix $B = (< \alpha_i, \alpha_j >)_{1\leqslant i,j\leqslant n}$ of the canonical form in the basis $(\alpha_i)_i$. This is a real symmetric positive matrix. The volume of $\mathbf{O}$ according to the canonical Haar measure is

$$v_\mathbf{O} = \sqrt{\det(B)} = |\det(A)|.$$

We let

$$d_\mathbf{K} = \det(AA^t)$$

be the discriminant of $\mathbf{K}$ and we denote by

$$\delta_\mathbf{K} = |d_\mathbf{K}|^{\frac{1}{n}}$$

the root discriminant. The square of the volume of $\mathbf{O}$ is $|d_\mathbf{K}|$.

1.6. **Number fields as incomplete intersections.** Let $\mathbf{K}/\mathbf{Q}$ be a number field. Let $r \geqslant 1$, $d \geqslant 1$, and $H \geqslant 1$ be integers. Let $E_1$, $E_2$, …, $E_r$ be $r$ polynomials of total degree $\leqslant d$ in $\mathbf{Z}[x_1, \ldots, x_r]$ all having coefficients bounded in absolute value by $H$. Let $\mathcal{I}$ be the $\mathbf{Z}$-scheme with equations

$$E_1 = E_2 = \cdots = E_r = 0 \text{ and } \det\left(\partial E_i/\partial x_j\right)_{1\leqslant i,j\leqslant r} \neq 0.$$

We assume that $\mathcal{I} \otimes \mathbf{Q} \to \operatorname{Spec} \mathbf{Q}$ contains $\operatorname{Spec} \mathbf{K}$ as one of its irreducible components. We call $\mathcal{C} \to \operatorname{Spec} \mathbf{Z}$ the Zariski closure of this component in $\mathcal{I}$. This is the spectrum of some order in $\mathbf{K}$. We say that $\mathcal{C} \to \operatorname{Spec} \mathbf{Z}$ is an **incomplete intersection model** of $\mathbf{K}/\mathbf{Q}$ in dimension $r$, degree $d$ and height $H$.

1.7. **Interpolant of a $p$-infinitesimal point.** Let $p$ be a prime integer. We fix some algebraic closure of $\mathbf{Q}_p$ and call $\mathbf{Q}_p^{\mathrm{nr}}$ the maximal unramified extension in it. For every power $q = p^f$ of $p$ we call $\mathbf{Q}_q$ the unique subextension of $\mathbf{Q}_p^{\mathrm{nr}}/\mathbf{Q}_p$ of degree $f$ and $\mathbf{Z}_q$ its ring of integers. Let $r \geqslant 1$, $s \geqslant 1$, $m \geqslant 1$, $d \geqslant 1$ and $H \geqslant 1$ be integers. Let $b_1^m$, …, $b_r^m$ be $r$ elements in $\mathbf{Z}_{p^s}/p^m$. Let $x_1$, …, $x_r$ be $r$ indeterminates. Let

$$\beta^m : \mathbf{Z}[x_1, \ldots, x_r] \to \mathbf{Z}_{p^s}/p^m$$

be the ring homomorphism sending $x_j$ onto $b_j^m$ for $1 \leqslant j \leqslant r$. We assume that $\beta^m$ is surjective. We call $b^m = (b_1^m, \ldots, b_r^m)$ the corresponding point in $\mathbf{A}^r(\mathbf{Z}_{p^s}/p^m)$. Let $J_{H,d}$ be the ideal of $\mathbf{Z}[x_1, \ldots, x_r]$ generated by all polynomials in $\operatorname{Ker} \beta^m$ having total degree $\leqslant d$ and all their coefficients bounded by $H$ in absolute value. We say that a point

$$b^\infty = (b_1^\infty, \ldots, b_r^\infty) \in (\mathbf{Z}_{p^s})^r$$

is the **interpolant** of $b^m$ in degree $d$ and height $H$ if

(1) $b_j^\infty \bmod p^m = b_j^m$ for every $1 \leqslant j \leqslant r$,
(2) all polynomials in $J_{H,d}$ vanish at $b^\infty$,
(3) and $b^\infty$ is **unique** with the two above properties.

1.8. **Short models of number fields.** We shall prove that both incomplete intersections and interpolants provide short descriptions of number fields.

**Theorem 3** (Number fields have small incomplete intersection models)**.** *There exists a positive constant $\mathcal{Q}$ such that the following is true. Let $\mathbf{K}$ be a number field of degree $n \geqslant \mathcal{Q}$ and root discriminant $\delta_{\mathbf{K}}$. Let $r$ be the smallest positive integer such that*

$$\binom{2r}{r} \geqslant n(r+1).$$

*Set*

$$\ell = \binom{2r}{r} - n \text{ and } H = \ell^{\ell/2n} \times \binom{2r}{r}^{1/2} \left(n^2 r(r+1)\delta_{\mathbf{K}}^2\right)^r. \tag{1}$$

*Then $r \leqslant \mathcal{Q} \log n$ and*

$$\log H \leqslant \mathcal{Q} \log n (\log n + \log \delta_{\mathbf{K}})$$

*and $\mathbf{K}$ has an incomplete intersection model in dimension $r$, degree $d = r$ and height $H$. Further*

$$\binom{d+r}{r} = \binom{2r}{r} \leqslant \mathcal{Q} n \log n$$

*so that the total number of coefficients in the $r$ equations is $\leqslant \mathcal{Q}n(\log n)^2$.*

The meaning of Theorem 3 is that we have a short description of $\mathbf{K}/\mathbf{Q}$ as a quotient of a finite algebra associated with the smooth zero-dimensional part of a complete intersection of small degree and small height in a projective space of small dimension. The bit size of the model is $\leqslant \mathcal{Q}n(\log n)^3(\log \delta_K + \log n)$. Every factor in this estimate is awaited but the $(\log n)^3$. Another annoyance is the remaining little uncertainty about which irreducible component of the complete intersection is of interest to us. One way of removing this uncertainty if to specify a geometric point on the targeted component. We then realize that giving enough such geometric points (counting multiplicities) enables us to reconstruct the equations. This leads us to the next theorem.

**Theorem 4** (Number fields from interpolants)**.** *The exists an absolute constant $\mathcal{Q}$ such that the following is true. Let $\mathbf{K}$ be a number field of degree $n \geqslant \mathcal{Q}$ and root discriminant $\delta_{\mathbf{K}}$ over $\mathbf{Q}$. Let $r$ and $H$ be as in Theorem 3. There exist positive integers $s \leqslant n$, and $m$ and a prime integer*

$$p \leqslant \mathcal{Q}n(\log n)^2(\log n + \log \delta_{\mathbf{K}})$$

*and a point*

$$b^m = (b_1^m, \dots, b_r^m) \in (\mathbf{Z}_{p^s}/p^m)^r$$

*such that $b^m$ has an interpolant*

$$b^\infty = (b_1^\infty, \dots, b_r^\infty) \in (\mathbf{Z}_{p^s})^r$$

*in degree $r$ and height $H$. And the field*

$$\mathbf{Q}(b_1^\infty, \dots, b_r^\infty) \subset \mathbf{Q}_q$$

*is isomorphic to $\mathbf{K}$. And*

$$rms \log p \leqslant \mathcal{Q}n(\log n)^2 (\log n + \log \delta_{\mathbf{K}}) .$$

The meaning of this theorem is that a model of the number field can be recovered from a few short $p$-adic expansions of a few algebraic numbers in it. The number field is recovered from $s$, $m$, $p$ and by $r$ elements in $\mathbf{Z}_q/p^m\mathbf{Z}_q$ where $q = p^s$. Each of these $r \leqslant \mathcal{Q}\log n$ elements is a $q$-adic expansion of bit size $ms \log p$. So the bit size of this model is bounded by $\mathcal{Q}n(\log n)^2 (\log n + \log \delta_{\mathbf{K}})$.

## 2. Constructing models of function fields

In this section we prove Theorems 1 and 2. In Section 2.1 we recall the definition of the Maroni invariants and we bound them. In Section 2.2 we use a generic well-posedness theorem in multivariate Hermite interpolation due to Alexander and Hirschowitz in order to prove the existence of small affine models of function fields. In Section 2.3 we prove that formal expansions of coordinates at a smooth point in these models characterize the function field.

2.1. **Small degree functions.** Let $K$ be a field. Let $K(C)/K(x)$ be a function field as in Section 1.1. We call $C_{\mathrm{aff}}$ the affine part

$$C_{\mathrm{aff}} = f^{-1}(\mathbf{A}^1) \subset C$$

of $C$. The sheaf $f_\star\mathcal{O}_C$ is a rank $n$ locally free $\mathbf{P}^1$-module. Every such sheaf decomposes as a direct sum of invertible sheaves. So

$$f_\star\mathcal{O}_C = \bigoplus_{0\leqslant i\leqslant n-1} \mathcal{O}_{\mathbf{P}^1}(-a_i) \tag{2}$$

where $a_0 = 0$ and the remaining $a_i$ form a non decreasing sequence of strictly positive integers, called the scrollar invariants, or the Maroni invariants of the cover. We call $\mathcal{O}_i$ the $i$-th term on the right hand side of Equation (2). Let $\tilde{\omega}_i$ be a generator of $H^0(\mathbf{P}^1, \mathcal{O}_i \otimes \mathcal{O}_{\mathbf{P}^1}(a_i))$ and set

$$\omega_i = x_0^{-a_i}\tilde{\omega}_i.$$

This is a function on $C$, regular on $C_{\mathrm{aff}}$, and the maximum order of its poles above $\infty$ is $a_i$. The family $(\omega_i)_{0\leqslant i\leqslant d-1}$ is a $K[x]$ basis of

$$H^0(\mathbf{A}^1, f_\star(\mathcal{O}_C)) = K[C_{\mathrm{aff}}]$$

the integral closure of $K[x]$ in $K(C)$. The determinant sheaf

$$\det(f_\star\mathcal{O}_C) = \wedge^d f_\star\mathcal{O}_C$$

is isomorphic to $\mathcal{O}_{\mathbf{P}^1}(-a)$ where

$$a = \sum_{0\leqslant i\leqslant n-1} a_i = n + g - 1.$$

Because $f_\star\mathcal{O}_C$ is a sheaf of $\mathbf{P}^1$-algebras, there exists a multiplication tensor

$$m \in H^0(\mathbf{P}^1, \widehat{f_\star\mathcal{O}_C} \otimes \widehat{f_\star\mathcal{O}_C} \otimes f_\star\mathcal{O}_C).$$

For every triple $(i, j, k)$ of integers with $0 \leqslant i, j, k \leqslant n-1$, we call

$$m_{i,j}^k \in H^0(\mathbf{P}^1, \hat{\mathcal{O}}_i \otimes \hat{\mathcal{O}}_j \otimes \mathcal{O}_k)$$

the corresponding component of $m$. Since $m_{i,j}^k$ is a global section of a sheaf isomorphic to $\mathcal{O}_{\mathbf{P}^1}(a_i + a_j - a_k)$ we have

$$a_i + a_j \geqslant a_k \tag{3}$$

whenever $m_{i,j}^k$ is non-zero. We call $\mu_{i,j}^k \in K[x]$ the coefficients of the multiplication table of $K[C_{\mathrm{aff}}]$ in the basis $(\omega_0, \ldots, \omega_{n-1})$. We have

$$\omega_i\omega_j = \sum_k \mu_{i,j}^k \omega_k$$

and $\mu_{i,j}^k$ is a polynomial of degree $\leqslant a_i + a_j - a_k$. In particular $\mu_{i,j}^k$ is zero unless inequality (3) holds true.

There exists a permutation $\sigma$ of the set of integers in the interval $[1, n-2]$ such that, for every integer $i$ in this interval, the coefficient $\mu_{i,\sigma(i)}^{n-1}$ is non zero. Otherwise the determinant $\det(\mu_{i,j}^{n-1})_{1\leqslant i,j\leqslant n-2}$ would be zero and there would exist a function $\eta$ in the $K(x)$-vector space generated by $\omega_1, \omega_2, \ldots, \omega_{n-2}$ such that $\eta W \subset W$ where $W$ is the $K(x)$-vector space generated by $\omega_0 = 1, \omega_1, \ldots, \omega_{n-2}$. This would turn $W$ into a $K(x, \eta)$-vector space. But this is imposible

because the extension $K(x,\eta)/K(x)$ has degree at least two and the codimension of $W$ in $K(C)$ is 1. We deduce that $a_i + a_{\sigma(i)} \geqslant a_{n-1}$ for $1 \leqslant i \leqslant n-2$ and summing out we find

$$(n-2)a_{n-1} \leqslant 2 \sum_{1\leqslant i\leqslant n-2} a_i = 2(a - a_{n-1})$$

that is

$$a_{n-1} \leqslant \frac{2a}{n} = 2\left(1 + \frac{g-1}{n}\right). \tag{4}$$

This inequality and its proof are the function field analogue to [4][Theorem 3.1].

**Lemma 1.** *The Maroni invariants of a function field of degree $n$ and genus $g$ are bounded form above by*

$$\nu = 2 + \left\lceil \frac{2(g-1)}{n} \right\rceil$$

*the smallest integer bigger than or equal to $2 + 2(g-1)/n$.*

So the field extension $K(C)/K(x)$ has a basis made of functions in $K[C_{\mathrm{aff}}]$ with small degree.

2.2. **Small equations for function fields.** Having found small degree functions $(\omega_i)_{0\leqslant i\leqslant n-1}$ we now look for small degree relations between them. Let $r \geqslant 2$ and $h \geqslant 0$ be integers. For every pair of integers $(i,j)$ with $0 \leqslant i \leqslant n-1$ and $1 \leqslant j \leqslant r$ we let

$$u_{i,j}(x) \in K[x]_h$$

be a polynomial of degree $\leqslant h$ in $x$. For $1 \leqslant j \leqslant r$ we set

$$\kappa_j = \sum_{0\leqslant i\leqslant n-1} u_{i,j}\omega_i \in K[C_{\mathrm{aff}}].$$

The functions $\kappa_j$ have all their poles above $\infty$ and the order of these poles is bounded from above by $h + \nu$. We define a morphism of $K[x]$-algebras

$$\epsilon_{\mathrm{aff}} : K[x][y_1, \ldots, y_r] \to K[C_{\mathrm{aff}}]$$

by sending $y_j$ to $\kappa_j$ for $1 \leqslant j \leqslant r$. This results in a morphism

$$e_{\mathrm{aff}} \quad : \quad \begin{array}{ccc} C_{\mathrm{aff}} & \longrightarrow & \mathbf{A}^{r+1}_K = \operatorname{Spec} K[x][y_1,\ldots,y_r] \\ & {\scriptstyle f_{\mathrm{aff}}} \searrow \quad \swarrow & \\ & \mathbf{A}^1_K = \operatorname{Spec} K[x] & \end{array}$$

The image by $e_{\mathrm{aff}}$ of the cycle $[C_{\mathrm{aff}} \otimes_{f_{\mathrm{aff}}} K(x)]$ is a 0-cycle $P$ of degree $n$ on $\mathbf{A}^r_{K(x)}$. We let $I$ be the corresponding ideal of $K(x)[y_1,\ldots,y_r]$ and denote by $2P \subset \mathbf{A}^r_{K(x)}$ the subscheme associated with $I^2$. We denote by $\mathcal{C} \to \mathbf{A}^1$ the Zariski closure of $P/K(x)$ in $\mathbf{A}^{r+1}$. Let $d \geqslant 1$ be an integer such that

$$n(r+1) \leqslant \binom{d+r}{d}. \tag{5}$$

Let

$$V = K(x)[y_1,\ldots,y_r]_d$$

be the $K(x)$-vector space of polynomials having total degree $\leqslant d$ in the variables $y_1, \ldots, y_r$ and let $M$ be the basis of $V$ consisting of monomials. We say that $2P$ is **well poised** in degree $d$ if the restriction to $V$ of the quotient map

$$K(x)[y_1, \ldots, y_r] \to K(x)[y_1, \ldots, y_r]/I^2$$

is surjective. We let $\Omega$ be a separable closure of $K(x)$ and we call $T$ the set of $K(x)$-embeddings

$$\tau : K(C) \to \Omega.$$

There are $n$ such embeddings. For every $\tau$ in $T$ we call

$$P_\tau = (\tau(\kappa_j))_{1 \leqslant j \leqslant r} \in \mathbf{A}^r(\Omega)$$

the corresponding geometric point of $P$. The scheme $2P$ is well poised if and only if the matrix

$$\mathcal{M}_P^1 = [(m(P_\tau))_{\tau \in T, m \in M}, (\partial m/\partial y_1(P_\tau))_{\tau \in T, m \in M}, \ldots, (\partial m/\partial y_r(P_\tau))_{\tau \in T, m \in M}]$$

with $n(r+1)$ rows and $\binom{d+r}{d}$ columns has maximal rank $n(r+1)$. We note that $\mathcal{M}_P^1$ consists of $r+1$ blocks of size $n \times \binom{d+r}{d}$ piled vertically. It has maximal rank for a generic $P$ when $d \geqslant 5$, according to the theorem of Alexander and Hirschowitz [1, 2].

The maximal minors of $\mathcal{M}_P^1$ are polynomials of degree $\leqslant dn(r+1)$ in each of the $u_{i,j}$ and one of them is not identically zero. The latter determinant cannot vanish on the cartesian product $(K[x]_h)^{nr}$ as soon as the cardinality of $K[x]_h$ is bigger than $dn(r+1)$. If $K$ is a finite field with cardinality $q$ this condition is granted as soon as

$$q^{h+1} > dn(r+1).$$

If $K$ is infinite we can afford $h = 0$. We will assume that $2P$ is well poised in degree $d$. So $P$ is well poised also and the map $e_{\text{aff}} \otimes K(x)$ is a closed immersion.

We look for small degree equations between the $(\kappa_j)_{1 \leqslant j \leqslant r}$. More precisely we look for polynomials in

$$\operatorname{Ker} \epsilon_{\text{aff}} \subset K[x][y_1, \ldots, y_r]$$

having total degree $\leqslant d$ in the $y_j$ and degree in $x$ as small as possible. We denote $K[x][y_1, \ldots, y_r]_d$ the $K[x]$-module of polynomials with total degree $\leqslant d$ in the $y_j$. This is a free $K[x]$-module of rank $\binom{d+r}{d}$. We define a morphism of $K[x]$-modules

$$K[x][y_1, \ldots, y_r] \to K[C_{\text{aff}}] \otimes x_0^{d(h+\nu)} = H^0(\mathbf{A}^1, f_\star \mathcal{O}_C \otimes_{\mathbf{P}^1} \mathcal{O}_{\mathbf{P}^1}(d(h+\nu)))$$

by sending $\prod_j y_j^{\gamma_j}$ to $x_0^{d(h+\nu)} \prod_j \kappa_j^{\gamma_j}$ for all exponents $(\gamma_1, \ldots, \gamma_r)$ with $\sum_j \gamma_j \leqslant d$. This morphism of $K[x]$-modules extends to a morphism of $\mathbf{P}^1$-modules

$$\epsilon_{\leqslant d} : \operatorname{Sym}^{\leqslant d} \mathcal{O}_{\mathbf{P}^1}^{\oplus r} \to f_\star \mathcal{O}_C \otimes_{\mathbf{P}^1} \mathcal{O}_{\mathbf{P}^1}(d(h+\nu))$$

that is generically surjective. The kernel of $\epsilon_{\leqslant d}$ is a locally free sheaf of rank

$$\ell = \binom{d+r}{d} - n.$$

The image of $\epsilon_{\leqslant d}$ is a locally free sheaf of rank $n$ and its determinant has degree

$$\deg \det \operatorname{Im} \epsilon_{\leqslant d} \leqslant \deg \det f_\star \mathcal{O}_C \otimes_{\mathbf{P}^1} \mathcal{O}_{\mathbf{P}^1}(d(h+\nu)) = -a + nd(h+\nu).$$

Since

$$\det \mathrm{Sym}^{\leqslant d} \mathcal{O}_{\mathbf{P}^1}^{\oplus r} \simeq \det \mathrm{Ker}\, \epsilon_{\leqslant d} \otimes_{\mathbf{P}^1} \det \mathrm{Im}\, \epsilon_{\leqslant d}$$

we deduce that

$$\deg \det \mathrm{Ker}\, \epsilon_{\leqslant d} \geqslant -n(h+\nu)d + a.$$

There exists $\ell$ non negative integers $(e_i)_{1\leqslant i\leqslant \ell}$ that form a non decreasing sequence and such that

$$\mathrm{Ker}\, \epsilon_{\leqslant a} \simeq \oplus_{1\leqslant i\leqslant \ell} \mathcal{O}_{\mathbf{P}^1}(-e_i).$$

More explicitly there exist $\ell$ polynomials $(E_i)_{1\leqslant i\leqslant \ell}$ in $K[x][y_1,\dots,y_r]_d$ such that the coefficients of $E_i$ are polynomials in $K[x]$ of degree $\leqslant e_i$ and

$$E_i(\kappa_1,\dots,\kappa_r) = 0.$$

Further

$$\sum_{1\leqslant i\leqslant \ell} e_i \leqslant n(h+\nu)d - a.$$

On the one hand

$$e_i \leqslant \lfloor \frac{n(h+\nu)d-a}{n} \rfloor \leqslant (h+\nu)d$$

for every $1 \leqslant i \leqslant \ell + 1 - n$. On the other hand the scheme $2P$ is well poised and the $\Omega$-vector space generated by the $E_i$ for $1 \leqslant i \leqslant \ell + 1 - n$ has codimension $n - 1 < n$ in $\mathrm{Ker}\, \epsilon_{\leqslant d} \otimes_{\mathbf{P}^1} \Omega$. So there exists at least one embedding $\tau \in T$ such that the $(\ell + 1 - n) \times r$ matrix

$$((\partial E_i/\partial y_j)(P_\tau))_{1\leqslant i\leqslant \ell+1-n,\, 1\leqslant j\leqslant r}$$

has maximal rank $r$. This means that there exist $r$ integers $1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant \ell + 1 - n$ such that the minor determinant

$$\Phi = \det\left((\partial E_{i_k}/\partial y_j)\right)_{1\leqslant k,\, j\leqslant r} \tag{6}$$

does not vanish at $P_\tau$ for some $\tau$ and thus for all $\tau$ by Galois action.

We now choose $d$, $r$, and $h$ depending on $g$, $n$, and $q$. We take $r = d$ and in order to grant the condition in Equation (5) we choose $r$ to be the smallest integer such that

$$\frac{1}{r+1}\binom{2r}{r} \geqslant n.$$

Since $\binom{2k}{k} \geqslant 2^k$ for every integer $k \geqslant 1$ we have

$$\frac{1}{k+1}\binom{2k}{k} \geqslant 2^{\frac{k}{2}}$$

for $k$ large enough. Further

$$\frac{1}{k+2}\binom{2k+2}{k+1} \leqslant \frac{1}{k+1}\binom{2k}{k} \times 4$$

for $k \geqslant 1$. We deduce that

$$\frac{1}{r+1}\binom{2r}{r} \leqslant 4n \quad \text{and} \quad r \leqslant \mathcal{Q}\log n. \tag{7}$$

If $K$ is infinite we set $h = 0$. If $K$ has $q$ elements we take $h$ to be the smallest integer such that

$$q^{h+1} > nr(r+1).$$

We check that

$$h \leqslant \mathcal{Q}(1+\log_q n). \tag{8}$$

We have

$$n+\ell = \binom{2r}{r} \leqslant 4n(r+1)$$

and

$$e_i \leqslant d(h+\nu) \leqslant \mathcal{Q}(\log n)(1+\log_q n + \frac{g}{n}) \tag{9}$$

for every $1 \leqslant i \leqslant \ell+1-n$. The number of $K$-coefficients in $E_i$ for each $1 \leqslant i \leqslant \ell+1-n$ is thus bounded from above by

$$\binom{2r}{r} \times (1+\max_{1\leqslant i\leqslant \ell+1-n} e_i) \leqslant \mathcal{Q}(\log n)^2(g+n(1+\log_q n)).$$

This finishes the proof of Theorem 1.

2.3. **Interpolants for function fields.** We set

$$d_x = (h+\nu)r$$

an upper bound for the degree in $x$ of the equations $E_{i_k}$. In order to prove Theorem 2 we look for a fiber of $f_{\text{aff}} : C_{\text{aff}} \to \mathbf{A}^1$ where the determinant $\Phi$ of Equation (6) does not vanish. Let $\Psi(x) \in K[x]$ be the product of all $\Phi(P_\tau)$ for $\tau \in T$. We bound the degree of $\Psi(x)$. First $\Phi$ has degree $\leqslant rd_x$ in $x$ and total degree $\leqslant r(r-1)$ in the $y_j$. Since the $\alpha_j$ have poles of order at most $\nu+h$ we deduce that the evaluation of $\Phi$ at $(\alpha_j)_{1\leqslant j\leqslant r}$ is a function in $K[C_{\text{aff}}]$ with poles of order $\leqslant (\nu+h)r(r-1)+rd_x$. The norm of this function is $\Psi(x)$ and its degree in $x$ is bounded from above by $n$ times $(\nu+h)r(r-1)+rd_x$. So

$$\deg\Psi \leqslant \mathcal{Q}n(\log n)^2(1+\log_q n+\frac{g}{n})$$

according to Equations (7), (9) and (8).

If $K$ is infinite there exist infinitely many unitary polynomials of degree one in $K[x]$ that are prime to $\Psi(x)$. If $K$ is finite with cardinality $q$ then we use the following lemma.

**Lemma 2.** *Let $K$ be a finite field with $q$ elements. Let $\Psi(x) \in K[x]$ be a polynomial with degree $\deg\Psi \geqslant 1$. There exists an irreducible polynomial in $K[x]$ that is prime to $\Psi$ and has degree $\leqslant \log_q(\deg\Psi)+1$.*

For every integer $k \geqslant 1$ we set $\Pi_k(x) = x^{q^k}-x$. This is a separable polynomial in $K[x]$ and all its irreducible factors have degree dividing $k$. If $q^k > \deg\Psi$ then at least one of these irreducible factors is prime to $\Psi$. We take $k$ to be the smallest integer bigger than $\log_q \deg\Psi$. □

We apply Lemma 2 to our $\Psi(x)$ and find a unitary irreducible polynomial $F(x) \in K[x]$ that is prime to $\Psi(x)$ and has degree

$$l \leqslant \log_q(\deg\Psi)+1 \leqslant \mathcal{O}(1+\log_q(1+g/n)+\log_q n).$$

Let $\bar{K}$ be an algebraic closure of $K$. Let $\lambda \in \bar{K}$ be a root of $F$. Let $\sigma$ be a point in $C(\bar{K})$ such that $f(\sigma) = \lambda$. We set $L = K(\lambda)$ and $S = K(\sigma)$ the residual field at $\sigma$. Let $s$ be the degree of $S/L$. We set

$$\rho = d_x + r(\nu + h) \leqslant \mathcal{Q}(\log n)(1 + \log_q n + \frac{g}{n})$$

and let $m$ be the smallest positive integer such that $mls > n\rho$. We denote $b_1^\infty, \ldots, b_r^\infty$ the expansions of the functions of $\kappa_1, \ldots, \kappa_r$ at the point $\sigma$ in the local parameter $t = x - \lambda$. We set

$$b_j^m = b_j^\infty \bmod t^m \in S[[t]]/t^m$$

for every $1 \leqslant j \leqslant r$. The point

$$b^m = (\lambda + t \bmod t^m, b_1^m, \ldots, b_r^m)$$

in $\mathbf{A}^{r+1}(S[[t]]/t^m)$ has an interpolant in degrees $(d_x, d_y)$ and this interpolant is

$$b^\infty = (\lambda + t, b_1^\infty, \ldots, b_r^\infty).$$

Indeed let $E(x, y_1, \ldots, y_r)$ be a polynomial in $K[x][y_1, \ldots, y_r]$ with degree $\leqslant d_x$ in $x$ and with total degree $\leqslant d_y = r$ in the $y_j$. The polynomial $E$ induces a function in $K[C_{\text{aff}}]$ having at most $n$ poles with order $\leqslant d_x + r(\nu + h) = \rho$ each. If this function vanishes at $b^m$ then the divisor of its zeros has degree $mls > n\rho$. So $E$ induces the zero function on $C_{\text{aff}}$. Therefore it vanishes at $b^\infty$. Unicity follows from the existence of $r$ equations with degree $\leqslant d_x$ in $x$ and total degree $\leqslant d_y$ in the $y_j$ having a non-zero Jacobian determinant at $\sigma$. Since

$$\frac{n\rho}{ls} < m \leqslant \frac{n\rho}{ls} + 1$$

we have $mls \leqslant n\rho + ls \leqslant \mathcal{Q}(\log n)(n(1 + \log_q n) + g)$ and $r \leqslant \mathcal{Q} \log n$. This finishes the proof of Theorem 2.

## 3. Constructing models of number fields

We prove Theorems 3 and 4. A natural counterpart to sheaves of modules over $\mathbf{P}^1$ in the context of number fields are euclidean lattices. Sections 3.1 and 3.2 summarize [8]. These sections realize the spectrum of some order of $\mathbf{K}$ as an irreducible component of a complete intersection in some affine space over $\mathbf{Z}$. Section 3.3 finds a smooth $\mathbf{F}_p$-point on this irreducible component and thickens it just enough to characterize the number field.

### 3.1. Small elements in number fields.

The ring of integers of a number field can be seen as a euclidean lattice. The existence of an integral domain structure which is compatible with the $L^\infty$-norm restricts the possibilities for the successive minima: they must all have the same order of magnitude.

**Lemma 3** (Number fields have small integers)**.** *The ring of integers* $\mathbf{O}$ *of a number field* $\mathbf{K}$ *with degree* $n$ *and root discriminant* $\delta_{\mathbf{K}}$ *contains* $n$ *linearly independant elements* $(\omega_i)_{1 \leqslant i \leqslant n}$ *over* $\mathbf{Z}$ *such that all the absolute values of all the* $\omega_i$ *are* $\leqslant \delta_{\mathbf{K}}^2$.

This is Proposition 1 in [8]. Bhargava, Shankar, Taniguchi, Thorne, Tsimerman, and ZhaoSee prove in [4][Theorem 3.1] a similar statement.

3.2. **Small equations for number fields.** Having found small integers $(\omega_i)_{0\leqslant i\leqslant n-1}$ we now look for relations between them with small degree and small height. Let $d \geqslant 5$ and $r \geqslant 1$ be two integers. We assume that

$$n(r+1) \leqslant \binom{d+r}{d}.$$

Let $M$ be the set of monomials of total degree $\leqslant d$ in the $r$ variables $x_1, \ldots, x_r$. We have

$$\mathbf{A}^r_{\mathbf{C}} = \operatorname{Spec} \mathbf{C}[x_1, \ldots, x_r] \subset \operatorname{Proj} \mathbf{C}[x_0, x_1, \ldots, x_r] = \mathbf{P}^r_{\mathbf{C}}.$$

Let $V_{\mathbf{C}}$ be the $\mathbf{C}$-linear space generated by $M$. We may associate to every element in $M$ the corresponding degree $d$ monomial in the $r+1$ variables $x_0, x_1, \ldots, x_r$. We thus identify $V_{\mathbf{C}}$ with $H^0(\mathcal{O}_{\mathbf{P}^r_{\mathbf{C}}}(d))$, the space of homogeneous polynomials of degree $d$. We call $T$ the set of all $n$ embeddings of $\mathbf{K}$ into $\mathbf{C}$. We let $(\omega_i)_{1\leqslant i\leqslant n}$ be $n$ linearly independant short elements in $\mathbf{O}$ as in Lemma 3. We pick $rn$ rational integers $(u_{i,j})_{1\leqslant i\leqslant n,\, 1\leqslant j\leqslant r}$ and we set

$$\kappa_j = \sum_{1\leqslant i\leqslant n} u_{i,j}\omega_i$$

for $1 \leqslant j \leqslant r$. For every $\tau \in T$ we consider the points

$$P_\tau = \Big(\sum_{1\leqslant i\leqslant n} u_{i,j}\tau(\omega_i)\Big)_{1\leqslant j\leqslant r} \in \mathbf{C}^r = \mathbf{A}^r(\mathbf{C}) \subset \mathbf{P}^r(\mathbf{C})$$

and call $P$ the union of these $n$ points. The maximal minors of the matrix

$$\mathcal{M}^1_P = \left[(m(P_\tau))_{\tau,\, m\in M}, (\partial m/\partial x_1(P_\tau))_{\tau,\, m\in M}, \ldots, (\partial m/\partial x_r(P_\tau))_{\tau,\, m\in M}\right]$$

are polynomials of degree $\leqslant dn(r+1)$ in each of the $u_{i,j}$ and one of them is not identically zero according to the theorem of Alexander and Hirschowitz [1, 2]. The latter determinant cannot vanish on the cartesian product $[0, dn(r+1)]^{nr}$. Thus there exist $nr$ rational integers $u_{i,j}$ in the range

$$[0, dn(r+1)]$$

such that the corresponding scheme $2P$ is well poised: it imposes $n(r+1)$ independent conditions on degree $d$ homogeneous polynomials. We assume that the $u_{i,j}$ meet these conditions. We look for polynomials with degree $\leqslant d$ and small integer coefficients vanishing at $P$. We denote by $V_{\mathbf{R}} = \mathbf{R}[x_1, \ldots, x_r]_d$ the $\mathbf{R}$-vector space of polynomials in $\mathbf{R}[x_1, \ldots, x_r]$ of degree $\leqslant d$. There is a unique $\mathbf{R}$-bilinear form on $V_{\mathbf{R}}$ that turns the set $M$ of monomials into an orthonormal basis. Let $V_{\mathbf{Z}} = \mathbf{Z}[x_1, \ldots, x_r]_d$. The lattice of relations with integer coefficients and degree $\leqslant d$ is a free $\mathbf{Z}$-module $\mathcal{L} \subset V_{\mathbf{Z}}$ of rank

$$\ell = \binom{d+r}{d} - n.$$

We set $L = \mathcal{L} \otimes_{\mathbf{Q}} \mathbf{R}$ the underlying $\mathbf{R}$-vector space and $L^\perp$ its orthogonal complement in $V_{\mathbf{R}}$. We denote by $\mathcal{L}^\perp$ the intersection $\mathcal{L}^\perp = L^\perp \cap V_{\mathbf{Z}}$. Since $V_{\mathbf{Z}}$ is unimodular, $\mathcal{L}$ and $\mathcal{L}^\perp$ have the same volume. See [13, Corollary 1.3.5.]. We denote by $\hat{\mathbf{O}} = \operatorname{Hom}(\mathbf{O}, \mathbf{Z})$ the dual of $\mathbf{O}$, the ring of integers of $\mathbf{K}$, as a $\mathbf{Z}$-module. The evaluation map at $(x_1, \ldots, x_r) = (\kappa_1, \ldots, \kappa_r)$ is denoted

$$\epsilon_{\mathbf{Z},d} : \mathbf{Z}[x_1, \ldots, x_r]_d \to \mathbf{O}.$$

We observe that $\mathcal{L}^\perp$ contains the image of $\hat{\mathbf{O}}$ by the transpose map

$$\hat{\epsilon}_{\mathbf{Z},d} : \hat{\mathbf{O}} \to \mathbf{Z}[x_1, \dots, x_r]_d$$

where we have identified $\mathbf{Z}[x_1, \dots, x_r]_d$ with its dual thanks to the canonical bilinear form. So the volume of $\mathcal{L}$ is bounded from above by the volume of $\hat{\epsilon}_{\mathbf{Z},d}(\hat{\mathbf{O}})$. We consider the matrix

$$\mathcal{M}_P^0 = [(m(P_\tau))_{\tau, m \in M}]$$

of the map $\epsilon_{\mathbf{C},d} = \epsilon_{\mathbf{Z},d} \otimes_{\mathbf{Z}} \mathbf{C}$ in the canonical bases. If we prefer to use an integral basis of $\mathbf{O}$ on the right we should multiply $\mathcal{M}_P^0$ on the left by the inverse $T$ of the matrix of a basis of $\mathbf{O}$ in the canonical basis. We deduce that the square of the volume of $\hat{\epsilon}_{\mathbf{Z},d}(\hat{\mathbf{O}})$ is the determinant of $T\mathcal{M}_P^0(\mathcal{M}_P^0)^t T^t$. Since $T\mathcal{M}_P^0$ has real coefficients we have

$$\det(T\mathcal{M}_P^0(\mathcal{M}_P^0)^t T^t) = \det\left(T\mathcal{M}_P^0\left(\overline{\mathcal{M}_P^0}\right)^t \bar{T}^t\right) = \det\left(\mathcal{M}_P^0\left(\overline{\mathcal{M}_P^0}\right)^t\right)/|d_{\mathbf{K}}|.$$

So the square of the volume of the lattice of relations is bounded by the determinant of the hermitian positive definite matrix $\mathcal{M}_P^0\left(\overline{\mathcal{M}_P^0}\right)^t$. We will use several times the following lemma.

**Lemma 4.** *If $E(x_1, \dots, x_r) \in \mathbf{Z}[x_1, \dots, x_r]$ is a polynomial with degree $\leqslant d_E$ and height $H_E$ then for every embedding $\tau$ the evaluation of $E$ at $P_\tau$ is bounded in absolute value by*

$$H_E\left(n^2 d(r+1)\delta_{\mathbf{K}}^2\right)^{d_E}\binom{d_E + r}{r}.$$

The coefficients $u_{i,j}$ are bounded by $dn(r+1)$. All the absolute values of the $\omega_i$ are bounded by $\delta_{\mathbf{K}}^2$. So the terms in $E$ are bounded from above by

$$H_E\left(n^2 d(r+1)\delta_{\mathbf{K}}^2\right)^{d_E}$$

and there are at most $\binom{d_E+r}{r}$ of them. □

Recall that the coefficients in $\mathcal{M}_P^0$ are degree $\leqslant d$ monomials in the $\kappa_j$. We deduce from Lemma 4 that they are bounded from above by

$$\left(n^2 d(r+1)\delta_{\mathbf{K}}^2\right)^d.$$

The coefficients in $\mathcal{M}_P^0\left(\overline{\mathcal{M}_P^0}\right)^t$ are bounded from above by

$$\mathfrak{D} = \binom{d+r}{d}\left(n^2 d(r+1)\delta_{\mathbf{K}}^2\right)^{2d}.$$

The matrix $\mathcal{M}_P^0\left(\overline{\mathcal{M}_P^0}\right)^t$ being hermitian positive definite, its determinant is bounded from above by the product of the diagonal terms. We deduce that the volume of the lattice $\mathcal{L}$ of relations is bounded from above by $\mathfrak{D}^{n/2}$. Recall that the dimension of $\mathcal{L}$ is

$$\ell = \binom{d+r}{d} - n.$$

For any $x$ in $V_{\mathbf{R}}$ we denote by $\|x\|$ the $\ell_2$-norm in the monomial basis. The volume of the sphere $\{x \in L, \|x\| \leqslant 1\}$ is $\geqslant 2^\ell \ell^{-\ell/2}$. Applying Minkowski's second theorem [17, Lecture III,

§4, Theorem 16] to the gauge function $x \mapsto ||x||$ we find that $\mathcal{L}$ contains $\ell$ linearly independant elements $E_1, E_2, \ldots, E_\ell$ such that

$$\prod_{1 \leqslant i \leqslant \ell} ||E_i|| \leqslant \ell^{\ell/2} \mathfrak{D}^{n/2}.$$

We assume that the sequence $i \mapsto ||E_i||$ is non-decreasing and deduce that

$$||E_i|| \leqslant \ell^{\frac{\ell}{2(\ell+1-i)}} \mathfrak{D}^{\frac{n}{2(\ell+1-i)}}$$

for every $1 \leqslant i \leqslant \ell$. We forget the last $n-1$ equations. On the one hand

$$||E_i|| \leqslant H(\mathbf{K}, d, r)$$

for every $1 \leqslant i \leqslant \ell + 1 - n$, where

$$H(\mathbf{K}, d, r) = \ell^{\ell/2n} \mathfrak{D}^{1/2} = \ell^{\ell/2n} \times \binom{d+r}{d}^{1/2} \left(n^2 d(r+1) \delta_{\mathbf{K}}^2\right)^d. \tag{10}$$

On the other hand the scheme $2P$ is well poised and the $\mathbf{C}$-vector space generated by the $E_i$ for $1 \leqslant i \leqslant \ell + 1 - n$ has codimension $n - 1 < n$ in $L \otimes_{\mathbf{R}} \mathbf{C}$. So there exists at least one embedding $\tau$ such that the $(\ell + 1 - n) \times r$ matrix

$$((\partial E_i / \partial x_j)(P_\tau))_{1 \leqslant i \leqslant \ell+1-n,\, 1 \leqslant j \leqslant r}$$

has maximal rank $r$. There exist $r$ integers $1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant \ell + 1 - n$ such that the value at $P_\tau$ of the minor determinant

$$\Phi = \det\left((\partial E_{i_k} / \partial x_j)\right)_{1 \leqslant k,\, j \leqslant r} \tag{11}$$

is non-zero for some $\tau$ and thus for all $\tau$ by Galois action.

In order to prove Theorem 3 we specialize the values of the parameters $r$ and $d$. We take $d = r$. It is evident that $\binom{2r}{r} \geqslant 2^r$ so

$$\frac{1}{r+1}\binom{2r}{r} \geqslant 2^{\frac{r}{2}}$$

for $r$ large enough. Further

$$\frac{1}{r+2}\binom{2r+2}{r+1} \leqslant \frac{1}{r+1}\binom{2r}{r} \times 4.$$

We choose $r$ to be the smallest positive integer such that $n(r+1) \leqslant \binom{2r}{r}$. We have

$$n(r+1) \leqslant \binom{2r}{r} \leqslant 4n(r+1) \text{ and } r \leqslant 3 \log n \tag{12}$$

for $n$ large enough. We deduce that $\ell = \binom{2r}{r} - n \leqslant 4n(r+1) \leqslant \mathcal{Q} n \log n$. So

$$\ell^{\ell/2n} \leqslant n^{\mathcal{Q} \log n}.$$

From Equation (12) we deduce that $\binom{2r}{r} \leqslant \mathcal{Q} n \log n$. Also $n^2 d(r+1) \leqslant \mathcal{Q} n^2 \log^2 n$ and

$$\left(n^2 d(r+1)\right)^d \leqslant n^{\mathcal{Q} \log n}. \tag{13}$$

So the coefficients of equations $E_i$ are bounded in absolute value by

$$H(\mathbf{K}, r, r) \leqslant (n \delta_{\mathbf{K}})^{\mathcal{Q} \log n}. \tag{14}$$

This proves Theorem 3.

3.3. **Interpolants for number fields.** In order to prove Theorem 4 we first look for a prime integer $p$ such that the value at $P_\tau$ of the determinant $\Phi$ of Equation (11) is prime to $p$. Let $\Psi \in \mathbf{Z}$ be the product of all $\Phi(P_\tau)$ for all embeddings $\tau$. We first bound $\Psi$ in absolute value. For every $1 \leqslant k,\, j \leqslant r$ the polynomial

$$\partial E_{i_k}/\partial x_j \in \mathbf{Z}[x_1, \ldots, x_r]$$

has total degree $\leqslant r$ and height $\leqslant rH(\mathbf{K}, r, r)$. Using Lemma 4, Equation (14) and Equation (13) we deduce that the evaluation of $\partial E_{i_k}/\partial x_j$ at $P_\tau$ is bounded in absolute value by

$$G = \left(n^2 r(r+1)\delta_{\mathbf{K}}^2\right)^r rH(\mathbf{K}, r, r)\binom{2r}{r} \leqslant (n\delta_{\mathbf{K}})^{\mathcal{Q}\log n} \tag{15}$$

We deduce that

$$|\Phi(P_\tau)| \leqslant G^r r! \leqslant (n\delta_{\mathbf{K}})^{\mathcal{Q}(\log n)^2} \quad \text{and} \quad |\Psi| \leqslant (n^n |d_{\mathbf{K}}|)^{\mathcal{Q}(\log n)^2}.$$

Using an estimate [18, Chapter I §2.6, Corollary 10.1] for the Tchebychev function $\theta$ we deduce that there exists a prime

$$p \leqslant \mathcal{Q} n(\log n + \log \delta_{\mathbf{K}})(\log n)^2$$

that does not divide $\Psi$.

The ring $\mathbf{Z}[\kappa_1, \ldots, \kappa_r]$ is an order in $\mathbf{K}$ which is unramified at $p$. Let $\mathfrak{q}$ be a place above $p$. Let $s$ be the degree of inertia at $\mathfrak{q}$. We set $q = p^s$ and we fix an isomorphism between $\mathbf{Z}_q$ and the completion of $\mathbf{Z}[\kappa_1, \ldots, \kappa_r]$ at $\mathfrak{q}$. We call $b_1^\infty, \ldots, b_r^\infty$ the images of $\kappa_1, \ldots, \kappa_r$ by this bijection. We let $m$ be the smallest positive integer such that $q^m = p^{ms}$ is bigger than $G^n$ where $G$ is given in Equation (15). We check that

$$ms \log p \leqslant n \log G + s \log p \leqslant n(\log G + \log p) \leqslant \mathcal{Q} n \log n(\log n + \log \delta_{\mathbf{K}}).$$

We set $b_j^m = b_j^\infty \bmod p^m \in \mathbf{Z}_q/p^m$ for every $1 \leqslant j \leqslant r$. The point

$$b^m = (b_1^m, \ldots, b_r^m)$$

has an interpolant in degree $d = r$ and height $H(\mathbf{K}, r, r)$ and this interpolant is $b^\infty$. Indeed let $E(x_1, \ldots, x_r)$ be a polynomial vanishing at $b^m$ and with total degree $\leqslant r$ and height $\leqslant H(\mathbf{K}, r, r)$. The evaluation of $E$ at $P_\tau$ is bounded from above by $G$ according to Lemma 4. Its norm is thus an integer bounded in absolute value by $G^n$ and divisible by $p^{ms} > G^n$. So $E$ vanishes at $P_\tau$ and at $b^\infty$ just as well. Unicity follows from the existence of $r$ equations with degree $\leqslant r$ and heigth $\leqslant H(\mathbf{K}, r, r)$ having a non-zero Jacobian determinant modulo $\mathfrak{q}$. This finishes the proof of Theorem 4.

## 4. Conclusion

We have constructed short models of two kinds for a global field: as an irreducible component of some complete intersection or as an interpolant of a finite affine scheme. Theorems 1 and 2 on the one hand and Theorems 3 and 4 on the other hand present evident similitudes. The awaited factor $g + n(1 + \log_q n)$ in the geometric situation has counterpart $n(\log n + \log \delta_{\mathbf{K}})$ in the arithmetic situation. The not so welcome factor $(\log n)^3$ or $(\log n)^2$ is the same in either cases. The methods are parallel to some extent. Interpolation plays a crucial role on either sides,

especially the theorem of Alexander and Hirschowitz. We do not use the geometric equivalent of Minkowski space however although it exists, see [16]. The reason is that basic arguments about vector bundles over $\mathbf{P}^1$ suffice for our purpose. Another difference is that in the arithmetic case our constructions are consistent with the best known bounds for the number of number fields of given degree and bounded discriminant [8, 15, 11]. In the geometric situation however, cohomological methods produce much better estimates [10], but no effective construction.

## REFERENCES


[1] J. Alexander. Singularités imposables en position générale à une hypersurface projective. *Compositio Math.*, 68(3):305–354, 1988.

[2] J. Alexander and A. Hirschowitz. Polynomial interpolation in several variables. *J. Algebraic Geom.*, 4(2):201–222, 1995.

[3] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves. Vol. I*, volume 267 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1985.

[4] M. Bhargava, A. Shankar, T. Taniguchi, F. Thome, J. Tsimerman, and Y. Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *ArXiv e-prints*, January 2017.

[5] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2):1031–1063, 2005.

[6] Manjul Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3):1559–1591, 2010.

[7] Henri Cohen, Francisco Diaz y Diaz, and Michel Olivier. Counting discriminants of number fields. *J. Théor. Nombres Bordeaux*, 18(3):573–593, 2006.

[8] Jean-Marc Couveignes. Enumerating number fields. *Ann. of Math. (2)*, 192(2):487–497, 2020.

[9] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[10] A. Johan de Jong and Nicholas M. Katz. Counting the number of curves over a finite field. *unpublished*, 2000.

[11] Jungin Lee. Upper bound on the number of extensions of a given number field. *ArXiv e-prints*, October 2020.

[12] Gunter Malle. On the distribution of Galois groups. II. *Experiment. Math.*, 13(2):129–135, 2004.

[13] Jacques Martinet. *Perfect lattices in Euclidean spaces*, volume 327 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 2003.

[14] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1999.

[15] Robert J. Lemke Oliver and Frank Thorne. Upper bounds on number fields of given degree and bounded discriminant. *ArXiv e-prints*, May 2020.

[16] Michael Rosen. A geometric proof of Hermite's theorem in function fields. *J. Théor. Nombres Bordeaux*, 29(3):799–813, 2017.

[17] Carl Ludwig Siegel. *Lectures on the geometry of numbers*. Springer-Verlag, Berlin, 1989.

[18] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 46 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1995. Translated from the second French edition (1995) by C. B. Thomas.



JEAN-MARC COUVEIGNES, UNIV. BORDEAUX, CNRS, BORDEAUX-INP, IMB, UMR 5251, F-33400 TALENCE, FRANCE.

JEAN-MARC COUVEIGNES, INRIA, F-33400 TALENCE, FRANCE.
*Email address*: Jean-Marc.Couveignes@u-bordeaux.fr