How to represent a number field in a concise way?

$\mathbb{K}$ number field of degree n, discriminant $d_{\mathbb{K}}$

$\delta_{\mathbb{K}} = |d_{\mathbb{K}}|^{1/n}$ the root discriminant

$T = \{ \tau : \mathbb{K} \hookrightarrow \mathbb{C} \}$

$\mathcal{O}_{\mathbb{K}}$ ring of integers

if $\alpha \in \mathbb{K}$ let $\|\alpha\| = \max_{\tau \in T} |\tau(\alpha)|$

Most natural possibility: pick a primitive α in $\mathcal{O}_{\mathbb{K}}$ with small norm and give the minimal polynomial

$$F(x) = \prod_{\tau \in T} (x - \tau(\alpha))$$

$$= x^n - f_1 x^{n-1} + \dots + f_n$$

$$|f_i| \leq \binom{n}{i} \|\alpha\|^i$$

Size $\log \prod_{i=1}^{n} (|\delta_i| + 2)$ is proportional to $n^2 \times \log \|d\|$ that is $n \times \log |d_{\mathbb{K}}|$

$\longrightarrow$ very redundant.

Another natural possibility is to choose a basis $\omega_1, \omega_2, \dots, \omega_n$ of $\mathcal{O}_{\mathbb{K}}$ and give the multiplication tensor

$$\omega_i \omega_j = \sum a_{i,j}^{k} \omega_k$$

$\longrightarrow n^3$ integers of size $\log \max_{1 \leq i \leq n} \|\omega_i\|$

Nice and natural but even more redundant.

A variation on the previous model is to provide

$$T_R(\omega_i \omega_j \omega_k) \in \mathbb{Z}$$

More symmetric, still redundant.

Ellenberg and Venkatesh 2003 $\rightarrow$ can reduce the redundancy.

Take $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathcal{O}_{\mathbb{K}}$

r small and $\|\alpha_i\|$ small

Take a basis of $\mathcal{O}_{\mathbb{K}}$

$$\omega_i = \prod_{\ell=1}^{r} \alpha_\ell^{e_{i,\ell}} = \vec{\alpha}^{\vec{e}_i}$$

with $\vec{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_r)$ and

$\vec{e_i} = (e_1, e_2, \dots, e_r)$

$$\omega_i \omega_j \omega_k = \vec{\alpha}^{\vec{e_i} + \vec{e_j} + \vec{e_k}}$$

Choose r elements $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathcal{O}_{\mathbb{K}}$

Choose $\Sigma \subset \mathbb{N}^r$

Collect $T_R\left(\vec{\alpha}^{\vec{e}}\right)$ for $\vec{e} \in \Sigma$.

Size is $\exp\left(C \cdot \sqrt{\log n}\right) \times \log d_{\mathbb{K}}$

- Variant of the minimal polynomial model is to pick $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathcal{O}_{\mathbb{K}}$ that generate an order $\mathcal{O}$ in $\mathbb{K}$.

Give a generating set for the ideal of relations between the α_i.

$$0 \to I \to \mathbb{Z}[x_1, \dots, x_r] \twoheadrightarrow \mathcal{O} \to 0$$
$$x_i \mapsto \alpha_i$$

$$0 \to I \times \mathbb{Q} \to \mathbb{Q}[x_1, \dots, x_r] \to \mathbb{K} \to 0$$

$$P : \operatorname{Spec} \mathbb{K} \hookrightarrow \mathbb{A}^r_{\mathbb{Q}}$$

$$P \otimes \mathbb{C} = \sum_{\tau \in T} P_\tau$$

where $P_\tau = \left(\tau(\alpha_i)\right)_{1 \leq i \leq r}$.

Used in integer factoring algorithms and for computing discrete logarithms.

$*$ Very natural also

give complex or p-adic approximations of $\alpha_1, \dots, \alpha_r$ in G_K with enough accuracy to characterize them.

$\longrightarrow$ recover I from these approximations via lattice reduction (PARI-GP algdep).

$*$ Variant give approximations of all $\tau(\alpha_i)$ for $1 \leq i \leq r$ and $\tau \in T$.

All these methods require two ingredients

* Some knowledge about small elements in $G_{\mathbb{K}}$

* Small relations between this small elements.

Small elements in $\mathcal{O}_{\mathbb{K}}$

$$\mathbb{M} = \mathbb{K} \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^r \oplus \mathbb{C}^s \qquad r + 2s = n$$

Scalar product $\langle x, y \rangle = \sum_{1 \leq i \leq r} x_i y_i + \sum_{1 \leq j \leq s} x_j \overline{y_j} + \overline{x_j} y_j$

$\mathcal{O}_{\mathbb{K}} \hookrightarrow \mathbb{M}$ is a euclidean lattice

$$\operatorname{cov}(\mathcal{O}_{\mathbb{K}}) = \sqrt{|d_{\mathbb{K}}|} = \delta_{\mathbb{K}}^{n/2}$$

$$\|x\| = \max\left(\max_{1 \leq i \leq r} |x_i| , \max_{1 \leq j \leq s} |x_j| \right)$$

$$\mathcal{E} := \{ x , \|x\| < 1 \}$$

$$\mathcal{E} \cap \mathcal{O}_{\mathbb{K}} = \{0\}$$

$\mathcal{E}$ open, convex, bounded, symmétric.

Minkowski theorem : there exist $\omega_1, \dots, \omega_n$ in $\mathcal{O}_{\mathbb{K}}$ that are linearly independant and

$$\prod_{i=1}^{n} \|\omega_i\| \leq \frac{2^n}{\mathrm{vol}(\mathcal{C})} \times \mathrm{cov}(\mathcal{O}_{\mathbb{K}})$$

$$= \frac{2^n}{2^r \times (2\pi)^s} \times \delta_{\mathbb{K}}^{n/2} \leq \delta_{\mathbb{K}}^{n/2}$$

if $\|\omega_1\| \leq \|\omega_2\| \leq \dots \leq \|\omega\|_n$ then

$$\|\omega_i\| \leq \delta_{\mathbb{K}}^{\frac{n}{2(n+1-i)}}$$

$\|\omega_1\| \leq \delta_{\mathbb{K}}^{1/2}$ ... $\|\omega_n\| \leq \delta_{\mathbb{K}}^{n/2}$

Stop halfway: $\quad m := \left\lceil \frac{n+1}{2} \right\rceil$

$\|w_i\| \leq \delta_{\mathbb{K}} \quad$ for $1 \leq i \leq m$

$\mathcal{O}_{\mathbb{K}}$ has a ring structure that is compatible with the norm

$\mathcal{O}_{\mathbb{K}}$ is integral

The products $\omega_i \omega_j$ for $1 \leq i \leq j \leq m$ generate a $\mathbb{Z}$-module of rank n.

Otherwise there exists $f : \mathcal{O}_{\mathbb{K}} \longrightarrow \mathbb{Z}$ such that $f(\omega_i \omega_j) = 0$ for $1 \leq i \leq j \leq m$.

Set $\varphi_i : \mathcal{O}_{\mathbb{K}} \longrightarrow \mathbb{Z}$

$\qquad\qquad x \longmapsto f(\omega_i x)$

$\mathbb{Z}\varphi_1 \oplus \mathbb{Z}\varphi_2 \oplus \cdots \oplus \mathbb{Z}\varphi_m$ is orthogonal to $\mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_m$

$m \quad + \quad m \quad > n$

$(\omega_i \omega_j)_{1 \leq i,j \leq m}$ generate a $\mathbb{Z}$-module of rank n and $\|\omega_i\| \leq \delta_{\mathbb{K}}$ for $i \leq m$

$$\|\omega_i \omega_j\| \leq \|\omega_i\| \times \|\omega_j\| \leq \delta_{\mathbb{K}}^2$$

We deduce the existence of n linearly independant integers $(\varpi_i)_{1 \leq i \leq n}$ such that

$$\|\varpi_i\| \leq_1 \delta_{\mathbb{K}}^{2}$$

Remark: the first occurence of such a result is in 2017 Bhargava, Shankar, Taniguchi, Thorne, Tsimerman, Zhao.

Small equations

There are many small integers in $\mathbb{K}$.

Take r of them $\alpha_1, \dots, \alpha_r$.

$$0 \to I \to \mathbb{Z}[x_1, x_2, \dots, x_r] \to \mathcal{O} \to 0$$
$$x_i \longmapsto \alpha_i$$

$$0 \to I \cdot \mathbb{Q} \to \mathbb{Q}[x_1, \dots, x_r] \to \mathbb{K} \to 0$$

$$P: \quad \operatorname{Spec} \mathbb{K} \hookrightarrow \mathbb{A}^r_{\mathbb{Q}}$$

$$P \otimes_{\mathbb{Q}} \mathbb{C} = \sum_{\tau \in T} P_\tau \qquad P_\tau = (\tau(\alpha_i))_{1 \leq i \leq r}$$

dimention count:

$$\dim \mathbb{Q}[x_1, \dots, x_r]_{\leq d} = \binom{d+r}{r}$$

$$\text{if } \binom{d+r}{r} > n \text{ then } I_{\leq d} \neq \{0\}$$

if $d = r$ then $\binom{d+r}{r} = \binom{2r}{r} \sim 4^r$

if $d = r \gg \log n$ then we have

equations in degree d.

Do they generate I ?

Do they generate I/I^2 at least ?

$E_1, \dots, E_r$ in $I_{\leq d}$ such that

$$\det \left(\frac{\partial E_i}{\partial x_j} \right)_{1 \leq i,j \leq r} \notin I$$

We look for r hypersurfaces in $\mathbb{A}^r$ that cross transversally at $(P_\tau)_{\tau \in T}$.

The existence of r such hypersurfaces of degree $\leq d$ is granted if

$$\mathbb{Q}[x_1,\dots,x_r]_{\leq d} \twoheadrightarrow \mathbb{Q}[x_1,\dots,x_r]/I^2$$

$$\uparrow \qquad\qquad\qquad\qquad \uparrow$$

$$\dim = \binom{d+r}{r} \qquad\qquad \dim = n\times(r+1)$$

$$0 \to I/I^2 \to \mathbb{Q}[x_1,\dots,x_r]/I^2 \to \mathbb{K} \to 0$$

I/I^2 " sum of cotangent spaces at P_i

$\dim = nr$

$\dim = n$

We now assume $\underbrace{\binom{d+r}{r} \geq n(r+1)}$

Geometrically: the Hermite interpolation problem in degree $\leq d$ is well poised at

$$P = (P_\tau)_{\tau \in T}$$

Other phrasing: $2\underline{P}$ is well poised.

Matrix formulation:

$$M = \{\text{monomials of degree } \leq d \text{ in } x_1, \dots, x_r\}$$

$\left(m(P_\tau) \right)_{\tau \in T,\, m \in M}$ n lines and $\binom{d+r}{r}$ columns

$\left(\frac{\partial m}{\partial x_1}(P_\tau) \right)_{\tau \in T,\, m \in M}$ n lines and $\binom{d+r}{r}$ columns

$\left(\frac{\partial m}{\partial x_2}(P_\tau) \right)_{\tau \in T,\, m \in M}$ n lines and $\binom{d+r}{r}$ columns

$\vdots$

$\left(\frac{\partial m}{\partial x_r}(P_\tau) \right)_{\tau \in T,\, m \in M}$ n lines and $\binom{d+r}{r}$ columns

total of $n(r+1)$ lines and $\binom{d+r}{r}$ columns

Well poisedness $\Leftrightarrow$ maximal rank.

Theorem (Alexander & Hirschowitz, 1995)
if $d \geq 5$ a generic Hermite interpolation problem is well poised.

Fine! But are we generic?
Yes since we have a free system of small integers

$\omega_1, \omega_2, \dots, \omega_n$ we can set

$$\alpha_i = \sum u_{i,j} \omega_j \quad 1 \leq i \leq \ell \text{ and } 1 \leq j \leq n$$

with $u_{i,j} \in \mathbb{Z}$ small.

So we have small degree local equations

$E_1, E_2, \dots, E_n \in \mathbb{Z}[x_1, \dots, x_n]$

What about the height?

$$0 \to I_{\le d} \to \mathbb{Z}[x_1, \dots, x_r]_{\le d} \longrightarrow G$$

$$x_i \mapsto \alpha_i$$

free submodule of rank $\ell := \binom{d+r}{r} - n$

euclidean space with canonical form

We can bound the covolume of $I_{\le d}$ in terms of the $\|\alpha_1\|, \dots, \|\alpha_r\|$

Finally if $d = r$ is the smallest integer such that $\binom{2d}{d} \geq n(d+1)$ then $d \ll \log n$ and we find d equations of degree $\leq d$ and logarithmic height $\ll \log n \, (\log n + \log S_{\mathbb{K}})$.

The total number of coefficients is

$$\leqslant d \times \binom{2d}{d} \ll n \times (\log n)^2$$

The total size of the local equations

is $\ll n (\log n)^3 \left(\log n + \log S_{\mathbb{K}} \right)$

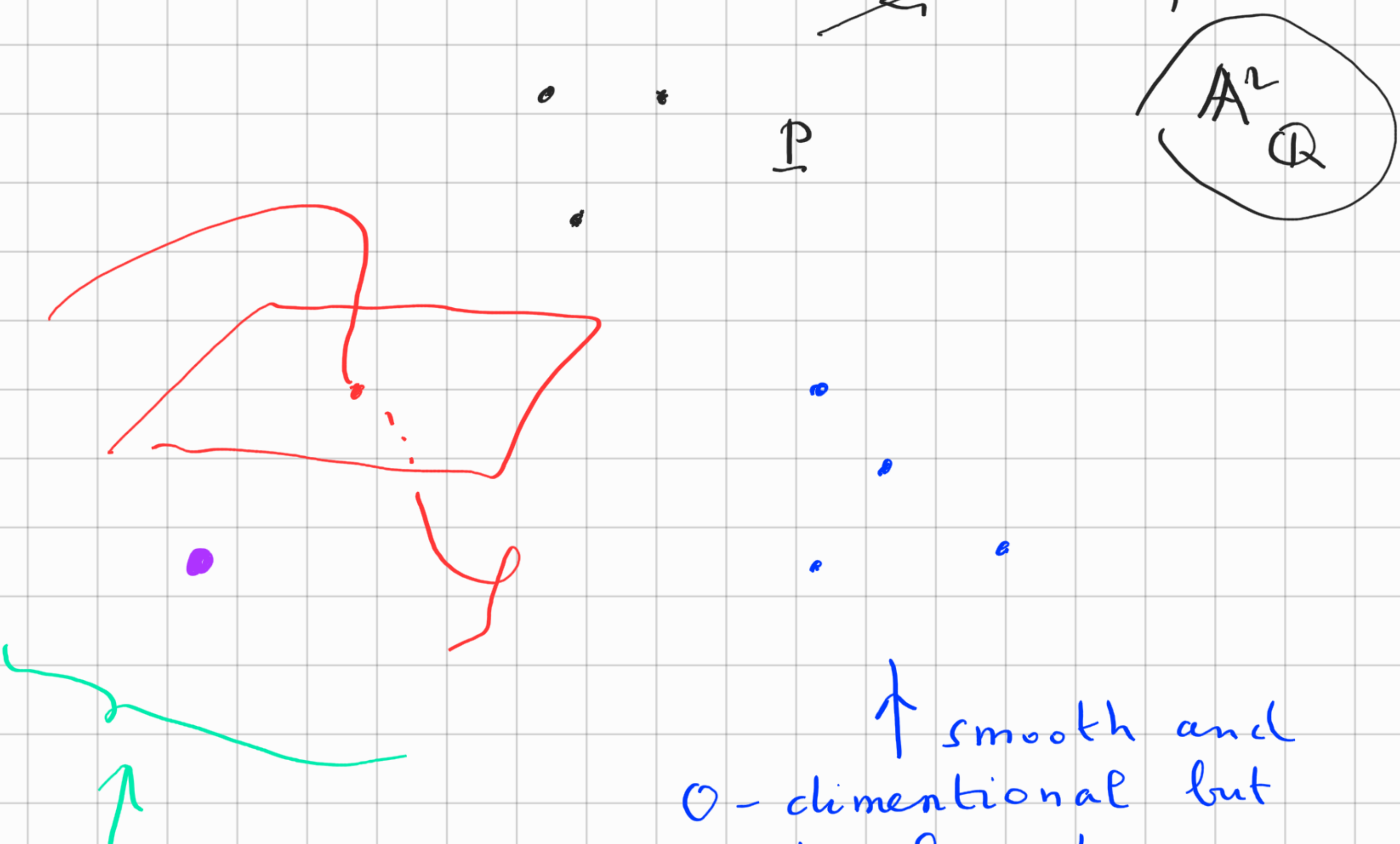
Objection : this is not a model of $\mathbb{K}$

Indeed let

$$J = (E_1, \cdots, E_r) < \mathbb{Q}[x_1, \cdots, x_r]$$

$$J \subsetneq I$$

relevant component



smooth and 0 - dimentional but not relevant.

not smooth or not zero dimentional.

How can we recover P and I from J ?

We can get rid of the non smooth and 0-dimentional locus by inverting the Jacobian determinant.

We are left with a 0-dimensional smooth variety of degree $\leq \deg E_1 \times \deg E_2 \times \cdots \times \deg E_r$
$$\leq d^d \ll n^{\log \log n}$$

Bezout theorem in the proper case.

In general : make a deformation to reduce to the proper case. When deforming the isolated points remain isolated. So the number of isolated point is maximal in the generic case.

There remains some ambiguity since we are interested in one component among $n^{\log\log n}$.

We are left with an étale algebra of degree $\leqslant n^{\log\log n}$ over $\mathbb{Q}$ of which $\mathbb{K}$ is a quotient.

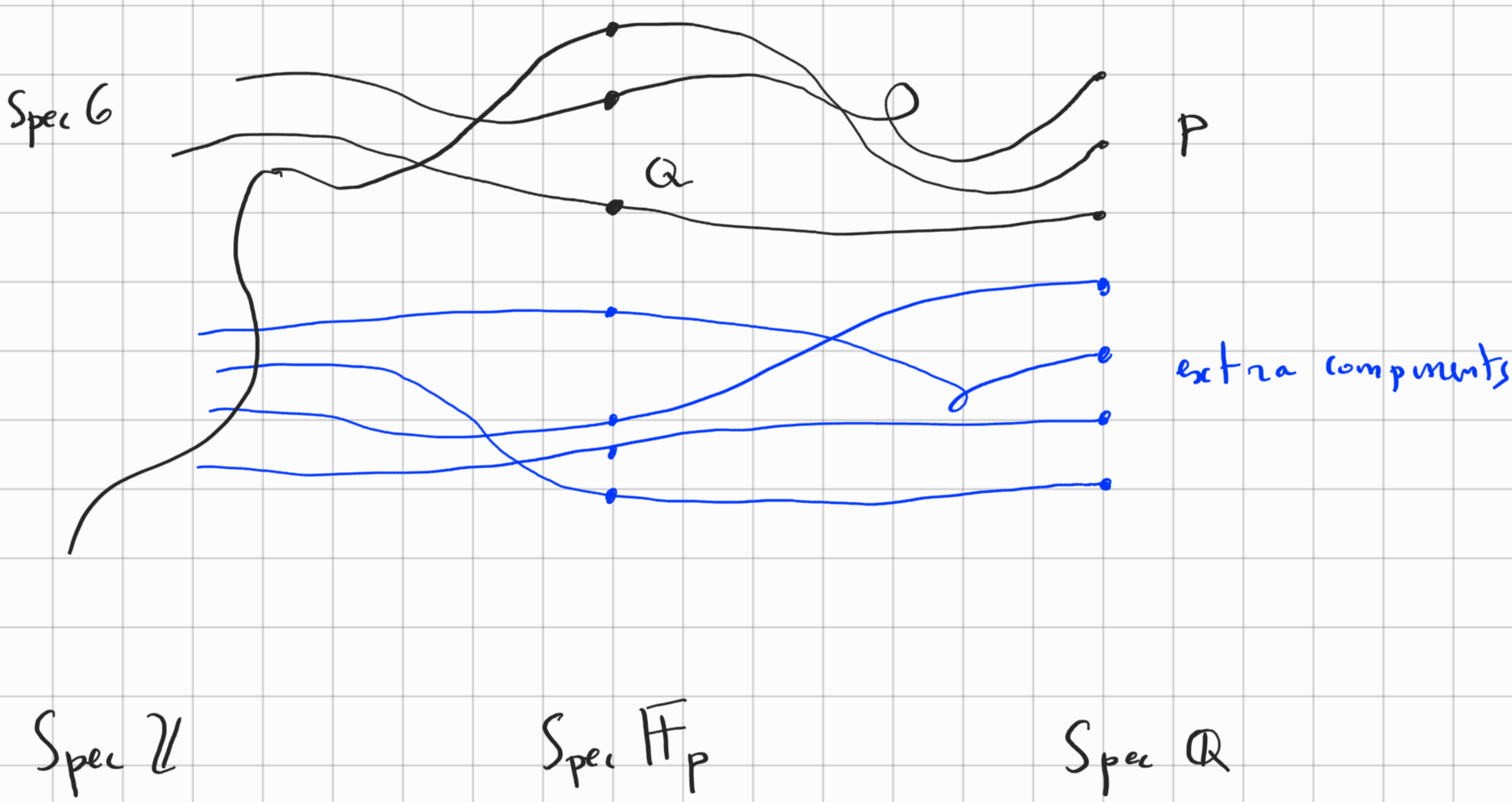
We may pin down the interesting irreducible component by giving a geometric point on it.

Let $\Phi = \det \left(\frac{\partial E_i}{\partial x_j} \right)_{1 \le i, j \le n} \in \mathbb{Z}[x_1, \dots, x_n]$

The product $\prod_{\tau \in T} \Phi(P_\tau) = \mathrm{Norm}_{\mathbb{K}/\mathbb{Q}} (\Phi \bmod I)$

is a rational integer.

Let p a prime not dividing this integer.



$\mathcal{O}$ is unramified above p

Let $\mathfrak{P}$ be above p and Q the corresponding geometric point to

$$\mathbb{Z}[x_1, \dots, x_r] \longrightarrow \mathcal{O}/\mathfrak{P}$$
$$x_i \mapsto \alpha_i \bmod \mathfrak{P}$$

Q is specified by r elements in some finite field.

$\operatorname{Spec}\mathcal{O}$ is the unique irreducible component meeting Q.

We can take $p \leq K\, n\, x (\log n)^2 (\log n + \log \delta_{\mathbb{K}})$

So we get rid of the ambiguity at allmost no cost.

We may go a bit further and give the images of $\alpha_1, \alpha_2, \dots, \alpha_r$ in

$\mathcal{O}_{\mathbb{K}} / \mathfrak{P}^m \mathcal{O}_{\mathbb{K}}$.

$$0 \to I_m \to \mathbb{Z}[x_1, \dots, x_n] \to \mathcal{O}_{\mathbb{K}} / \mathfrak{p}^m \mathcal{O}_{\mathbb{K}} \to 0$$

Of course $\underset{\nwarrow\, 1 \dim}{I} \subset I_m \;\nwarrow 0 \dim$

let H and d be the height and degree of the local equations we found $E_1, E_2, \dots, E_n$.

Let $I_{m,d,H}$ be the ideal generated by all the polynomials in I_m having degree $\leq d$ and height $\leq H$.

If p^m is large enough then $I_{m,d,H}$ vanishes at $P = (\alpha_1, \alpha_2, \dots, \alpha_n)$ and contains n equations with non-zero Jacobian determinant.

From any such n equations we can Hensel lift the $\alpha_i \bmod \mathfrak{p}^m$ to the p-adic expansions of the α_i. The field $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$ is then isomorphic to $\mathbb{K}$.

So instead of giving local equations for a model of $\mathbb{K}$ we may give p-adic expansions of a few elements in $\mathcal{O}_{\mathbb{K}}$.

In the end we have at least 3 different ways of specifying a number field:

- Traces of elements $\vec{\alpha}^{\vec{e}} = \prod_{1 \leq i \leq r} \alpha_i^{e_i}$

where $\alpha_1, \alpha_2, \dots, \alpha_r$ are small elements in $\mathcal{O}_{\mathbb{K}}$ and $\vec{e} \in \Sigma \subset \mathbb{N}^r$

This is the original idea of Ellenberg and Venkatesh. It has been shown by Lemke Oliver and Thorne, using the Alexander-Hirschowitz theorem that the size of such a model is

$$\leqslant K\, n(\log n)^2 \log \delta_{\mathbb{K}} + \text{function of } n$$

- local equations $E_1, E_2, \dots, E_r$ in $\mathbb{Z}[x_1, \dots, x_r]_{\leq d}$.

The size of such a model is

$$\leq K\, n \times (\log n)^3 \left[\log \delta_{\mathbb{K}} + \log n \right]$$

- truncated p-adic expansions of r integers in $\mathbb{K}$.

The size of such a model is

$$\leq K\, n \times (\log n)^2 \left[\log \delta_{\mathbb{K}} + \log n \right]$$

$N_n(X) =$ # of nb fields with degree n and $|\mathrm{disc}| \leq X$

$$N_n(X) = X^{\cancel{K(\log n)^2}} \times n^{K n \cancel{(\log n)^2}}$$