Geometric interpretation of quadratic Chabauty. Bas Edixhoven.

Séminaire Variétés Rationnelles, 2018/10/19, Paris IHP, 50th birthday P. Gille.
(Joint work with Guido Lido.) Still quite preliminary, no example worked out yet, nothing really written yet (well: notes of Oberwolfach lecture)
Goal: to replace p-adic Hodge theory, p-adic heights, p-adic and/(integration)/geom. by "old fashioned" (1980's) algebraic geometry $/\mathbb{Z}$ and over $\mathbb{Z}/p^2\mathbb{Z}$, not to reprove finiteness statements but to find $C(\mathbb{Q})$ for specific C.
Note: we are re-interpreting the work of Balakrishnan, Dogra, Müller, Tuitman and Vonk. Hopefully, computations become easier, and we clarify what quadr. Chabauty "is".

Let $C/\mathbb{Z}$ be a curve, proper, flat, regular, $C_{\mathbb{Q}}$ geom. connected, genus $g \geq 2$, $n \geq 1$ s.t. C smooth over $\mathbb{Z}[1/n]$.

$J :=$ Néron model $/\mathbb{Z}$ of $\mathrm{Pic}^0_{C_{\mathbb{Q}}/\mathbb{Q}}$, $J^\vee :=$ Néron model $/\mathbb{Z}$ of $J^\vee_{\mathbb{Q}}$, $\lambda : J \xrightarrow{\sim} J^\vee$.

$B_{\mathbb{Q}} :=$ Poincaré line bundle on $J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}}$, trivialised on $(\{0\} \times J^\vee_{\mathbb{Q}}) \cup (J_{\mathbb{Q}} \times \{0\})$.

$P_{\mathbb{Q}} :=$ Poincaré $\mathbb{G}_m$-torsor on $J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}}$: $P_{\mathbb{Q}} = \underline{\mathrm{Isom}}_{J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}}}(\mathcal{O}, B_{\mathbb{Q}})$.

$P_{\mathbb{Q}}$ is a bi-extension of $J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}}$ by $\mathbb{G}_m$: for S a $\mathbb{Q}$-scheme, $x_1, x_2 \in J_{\mathbb{Q}}(S)$, $y \in J^\vee_{\mathbb{Q}}(S)$: $(x_1 + x_2, y)^* B_{\mathbb{Q}} = (x_1, y)^* B_{\mathbb{Q}} \otimes_{\mathcal{O}_S} (x_2, y)^* B_{\mathbb{Q}}$, canonical isom from the thm. of the square/cube.
This gives $(x_1 + x_2, y)^* P_{\mathbb{Q}} \longleftarrow (x_1, y)^* P_{\mathbb{Q}} \times_S (x_2, y)^* P_{\mathbb{Q}}$

$$\begin{array}{cccccc} P_{\mathbb{Q}} & z_1 & z_2 & & z_1 +_1 z_2 \\ \downarrow & \downarrow & \downarrow & \rightsquigarrow & \downarrow \\ J_{\mathbb{Q}} \times J^\vee_{\mathbb{Q}} & (x_1, y) & (x_2, y) & & (x_1 + x_2, y) =: (x_1, y) +_1 (x_2, y). \end{array}$$

And of course the same for the other coordinate.
These $+_1$ and $+_2$ commute when it makes sense.

Extension over $\mathbb{Z}$. $J^0 \hookrightarrow J \twoheadrightarrow \Phi$, with J^0 fibrewise connected component of 0 of J, Φ finite skyscraper groupscheme supported on $\mathrm{Spec}(\mathbb{Z}/n\mathbb{Z})$. Then $P_{\mathbb{Q}}$ extends uniquely to $P \to J \times J^{\vee 0}$ as biextension by $\mathbb{G}_m$. (obstruction is Grothendieck's pairing $\Phi \times \Phi^{\vee} \to \mathbb{Q}/\mathbb{Z}$)
(Ref: L. Moret-Bailly's "Métriques permises".) ("Pinceaux de var. ab." (SGA 7))

Assume: we have $b \in C_{\mathbb{Q}}(\mathbb{Q})$ $(= C(\mathbb{Z}) = C^{sm}(\mathbb{Z}))$.

Then $j_b : C^{sm} \to J$, $P \mapsto [P-b]$. That gives:

$$\begin{tikzcd}
 & \ker_{\mathrm{Pic}} \arrow[r, "\sim"] \arrow[d, hook] & \ker_{NS} \arrow[d, hook] \\
J^{\vee}_{\mathbb{Q}} = \mathrm{Pic}^0_{J_{\mathbb{Q}}/\mathbb{Q}} \arrow[r, hook] \arrow[d, "\wr", "-\lambda^{-1} = j_b^*"'] & \mathrm{Pic}_{J_{\mathbb{Q}}/\mathbb{Q}} \arrow[r, two heads] \arrow[d, "j_b^*"'] & NS_{J_{\mathbb{Q}}/\mathbb{Q}} \arrow[d, "j_b^*"'] \\
J_{\mathbb{Q}} \arrow[r, hook] & \mathrm{Pic}_{C_{\mathbb{Q}}/\mathbb{Q}} \arrow[r, two heads, "\deg"] & (\mathbb{Z})_{\mathbb{Q}}
\end{tikzcd}$$

Note: $NS_{J_{\mathbb{Q}}/\mathbb{Q}}(\mathbb{Q}) = \mathrm{End}(J_{\mathbb{Q}})^+ \longrightarrow \mathbb{Z}$ via trace on $H_1(J(\mathbb{C}), \mathbb{Z})$.
free $\mathbb{Z}$-module, $\rho :=$ rank.

So: $\ker\left(j_b^* : \mathrm{Pic}(J_{\mathbb{Q}}) \to \mathrm{Pic}(C_{\mathbb{Q}})\right)$ is free $\mathbb{Z}$-mod. rank $\rho - 1$; let $\mathcal{L}_1, \ldots, \mathcal{L}_{\rho-1}$ be a basis, each $\mathcal{L}_i$ rigidified at 0.

Now we relate this to $P_{\mathbb{Q}}$. For all $\mathcal{L}$ inv. $\mathcal{O}$-module on $J_{\mathbb{Q}}$ we have $\varphi_{\mathcal{L}} : J_{\mathbb{Q}} \to J^{\vee}_{\mathbb{Q}}$, $x \mapsto (tr_x^* \mathcal{L}) \otimes \mathcal{L}^{-1}$, and

$$\mathcal{L}^{\otimes 2} = \underbrace{\mathcal{L} \otimes (-id)^* \mathcal{L}^{-1}}_{c \,\in\, J^{\vee}_{\mathbb{Q}}(\mathbb{Q})} \otimes \underbrace{\mathcal{L} \otimes (-id)^* \mathcal{L}}_{\cong\, (id, \varphi_{\mathcal{L}})^* B_{\mathbb{Q}}} = (id, f_{\mathcal{L}})^* B_{\mathbb{Q}} \quad \text{with} \quad f_{\mathcal{L}} = tr_c \circ \varphi_{\mathcal{L}}.$$

unique up to $\mathbb{Q}^{\times}$.

$$\begin{tikzcd}
 & P'_{\mathbb{Q}} \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & P_{\mathbb{Q}}^{\rho-1} \arrow[d] \\
C_{\mathbb{Q}} \arrow[ur, dashed, "\tilde{j}_b"] \arrow[r, "j_b"'] & J_{\mathbb{Q}} \arrow[r, "{(id, f_{\mathcal{L}_1}, \ldots, f_{\mathcal{L}_{\rho-1}})}"'] & J_{\mathbb{Q}} \times J_{\mathbb{Q}}^{\vee, \rho-1}
\end{tikzcd}$$

$\mathbb{G}_m^{\rho-1}$-torsor, biextension.

$\forall i$, f_{χ_i} extends uniquely to $f_{\chi_i} : J \longrightarrow J^\vee$.

Let $m :=$ l.c.m. of the exponents of the $\Phi(\overline{\mathbb{F}}_p)$, $p | n$.

Then $m \cdot f_{\chi_i} : J \longrightarrow J^{\vee,0}$, and $(\mathrm{id}, m\cdot f_{\chi_i})^* B_{\mathbb{Q}} = \chi_i^{\otimes 2m}$: trivial on $C_{\mathbb{Q}}$.

$j_b : C^{sm} \longrightarrow J$, $\quad j_b^* (\mathrm{id}, m_i \cdot f_{\chi_i})^* B$ is trivial, uniquely up to ± 1,

on each of the finitely many open $U \subset C^{sm}$ obtained by removing all but one irred. comp. of each of the reducible fibres of $C^{sm} \to \mathrm{Spec}(\mathbb{Z})$.

Note: every $P \in C(\mathbb{Q})$ extends uniquely to a $P \in U(\mathbb{Z})$ for a unique U.

For each such U we have:

$$\begin{tikzcd}
 & P'' \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & P^{\rho-1} \arrow[d] \\
U \arrow[ur, "\tilde{j}_b"] \arrow[r, "j_b"'] & J \arrow[r, "{(\mathrm{id},\, m f_{\chi_1}, \ldots,\, m f_{\chi_{\rho-1}})}"'] & J \times_{\mathbb{Z}} J^{\vee,0,\rho-1}
\end{tikzcd}$$

Note that $P''(\mathbb{Z}) \to J(\mathbb{Z})$ is a $(\pm 1)^{\rho-1}$-torsor.

Now we apply Chabauty's idea:

$$\begin{tikzcd}
U(\mathbb{Z}) \arrow[r, hook] \arrow[d, hook] & P''(\mathbb{Z}) \arrow[d, phantom, "\cap"] \\
 & \overline{P''(\mathbb{Z})} \arrow[d, phantom, "\cap"] \\
U(\mathbb{Z}_p) \arrow[r, hook, "\tilde{j}_b"'] & P''(\mathbb{Z}_p)
\end{tikzcd}$$

$U(\mathbb{Z}) \overset{\tilde{j}_b}{\hookrightarrow} \underbrace{\tilde{j}_b(U(\mathbb{Z}_p))}_{\substack{\text{1-dim.} \\ \text{p-adic manif.}}} \cap \overline{P''(\mathbb{Z})}$.

We hope that this is at most r-dimensional. $\dim P''(\mathbb{Z}_p) = g + \rho - 1$.

$r := \mathrm{rank}(J(\mathbb{Z}))$.

Chabauty's idea should work if $r < g + \rho - 1$.

The biextension structure of $P^{\rho-1}$ should help us to understand $\overline{P''(\mathbb{Z})} \subset P''(\mathbb{Z}_p)$.

(Without such a structure ~~the~~ it doesn't work:

$$\begin{array}{ccc}
\mathbb{A}^2_{\mathbb{Z}} - 0(\mathrm{Spec}\,\mathbb{Z}) \circlearrowleft GL_{2,\mathbb{Z}} & & SL_2(\mathbb{Z}) \\
\downarrow & & \cap \quad \text{dense.} \\
\mathbb{P}^1_{\mathbb{Z}} & & SL_2(\mathbb{Z}_p)
\end{array}$$

(note: aha, a rational variety!))

How can we parametrise $P''(\mathbb{Z})$?

Let $P_1, \ldots, P_r, \ldots P_s$ generate $J(\mathbb{Z})$, $Q_1, \ldots, Q_t$ generate $J^{\vee,0}(\mathbb{Z})$.
Recall: $m \cdot f_{\mathcal{L}_k} = m \cdot (tr_{c_k} \circ \varphi_{\mathcal{L}_k}) = tr_{m \cdot c_k} \circ m \cdot \varphi_{\mathcal{L}_k}$.

$\forall i, \forall k$, write $m \cdot \varphi_{\mathcal{L}_k}(P_i) = \sum_j a_{k,i,j} \cdot Q_j$,

$\forall k$, write $m \cdot c_k = \sum_j b_{k,j} Q_j$.

$\forall i,j$ let $R_{i,j} \in P(\mathbb{Z})$ over (P_i, Q_j) in $(J \times J^{\vee 0})(\mathbb{Z})$.

Then, $\forall n_1, \ldots, n_s \in \mathbb{Z}$, $\sum_i n_i P_i$ in $J(\mathbb{Z})$ is mapped to

$$\left(\sum_i n_i P_i, \left(\sum_j \left(b_{k,j} + \sum_i n_i a_{k,i,j}\right) Q_j \right)_{k=1}^{\rho-1} \right) \text{ in } (J \times J^{\vee,0,\rho-1})(\mathbb{Z}).$$

Over this, in $P^{\rho-1}(\mathbb{Z})$, we have:

$$\left({\sum_j}_2 \left(b_{k,j} + \sum_i n_i a_{k,i,j}\right) \cdot_2 \underbrace{\left({\sum_i}_1 n_i \cdot_1 R_{i,j} \right)}_{\text{over } \left(\sum n_i P_i,\, Q_j\right)} \right)_{k=1}^{\rho-1}$$

$\boxed{\text{Note that this is quadratic in the } n_i.}$

Idea to see the closure in $P''(\mathbb{Z}_p)$: think of the $n_i \in \mathbb{Z}_p$.

Structure of $P^{\rho-1}(\mathbb{Z}_p)$

$\mathbb{Z}_p^\times = \mathbb{F}_p^\times \times (1+p\mathbb{Z}_p)$ $\quad \mathbb{Z}_p^{\times,\rho-1}$-torsor $\qquad\qquad \mathbb{F}_p^{\times,\rho-1}$-torsor

$$\begin{tikzcd}
P^{\rho-1}(\mathbb{Z}_p) \arrow[r] \arrow[d] & P^{\rho-1}(\mathbb{F}_p) \arrow[d] & \ni z \arrow[d, mapsto] \\
J(\mathbb{Z}_p) \times J^{\vee,0,\rho-1}(\mathbb{Z}_p) \arrow[r] & J(\mathbb{F}_p) \times J^{\vee,0,\rho-1}(\mathbb{F}_p) & \ni (x,y)
\end{tikzcd}$$

$\circlearrowleft (1+p\mathbb{Z}_p)^{\rho-1}$-torsor.

$$P^{\rho-1}(\mathbb{Z}_p) = \coprod_{z \in P^{\rho-1}(\mathbb{F}_p)} P^{\rho-1}(\mathbb{Z}_p)_z$$

↑ residue polydisc.

$$\begin{tikzcd}
P^{\rho-1}(\mathbb{Z}_p)_z \arrow[d] \\
\underbrace{J(\mathbb{Z}_p)_x \times J^{\vee,0,\rho-1}(\mathbb{Z}_p)_y}
\end{tikzcd}$$

is a torsor under the free ($p>2$) $\mathbb{Z}_p$-module $J(\mathbb{Z}_p)_0 \times J^{\vee,0,\rho-1}(\mathbb{Z}_p)_0$.

A specific case Assume $r = g$, $\rho - 1 \geq 2$, $p > 2$, $p \nmid n$,
$P_1, \ldots, P_g$ a $\mathbb{Z}$-basis of $\ker(J(\mathbb{Z}) \to J(\mathbb{F}_p))$,
$Q_1, \ldots, Q_g$ a $\mathbb{Z}$-basis of $\ker(J^{\vee,0}(\mathbb{Z}) \to J^\vee(\mathbb{F}_p))$,
the images of $P_1, \ldots, P_g$ in $\ker(J(\mathbb{Z}/p^2\mathbb{Z}) \to J(\mathbb{F}_p))$ form an $\mathbb{F}_p$-basis,
and same for the $Q_1, \ldots, Q_g$.

Then, $\forall u \in U(\mathbb{F}_p)$ s.t. $\tilde{j}_b(u) \in P''(\mathbb{F}_p)$ is in the image of $P''(\mathbb{Z})$,
$\forall k \in \{1, \ldots, \rho - 1\}$,

$$\begin{tikzcd}
 & P''_{k} \arrow[r, "p_k"] \arrow[d] & P \arrow[d] \\
U \arrow[ur, "\tilde{j}_b"] \arrow[r, "j_b"'] & J \arrow[r, "{(\mathrm{id},\, m \cdot f_{\chi_k})}"'] & J \times J^{\vee 0}
\end{tikzcd}
\qquad
\begin{tikzcd}
 & P(\mathbb{Z}) \arrow[d] \\
U(\mathbb{Z}/p^2\mathbb{Z})_u \arrow[r, "p_k \circ \tilde{j}_b"'] & P(\mathbb{Z}/p^2\mathbb{Z})
\end{tikzcd}$$

res. at u

$(p_k \circ \tilde{j}_b)^{-1}$(image of $P(\mathbb{Z})$) is given
by a (at most) quadr. equation, on $T_{U_{\mathbb{F}_p}}(u)$, to which $\underline{\text{Hensel}}$ is applicable

unique p-adic lifts of simple zeros over $\mathbb{F}_p$.