Brief superficial remarks on Shinichi Mochizuki's Interuniversal Teichmueller Theory (IUTT), version 3 (27/12/2015)

Minhyong Kim

1. Arithmetic elliptic curves in general position (AECGP): a height inequality in an ideal case

Let F be a number field, E an elliptic curve over F, and l a rational prime. Assume that E has split semi-stable reduction at the set S of primes of bad reduction. Thus, for each $v \in S$, there is a Tate parametrisation

$$\mathbb{G}_m/q_v^{\mathbb{Z}} \simeq E_v$$

and a $G_v = \mathrm{Gal}(\bar{F}_v/F_v)-$equivariant exact sequence

$$0 \longrightarrow \, < q_v^{1/l} > \, \longrightarrow E[l] \longrightarrow \mathbb{Z}/l \longrightarrow 0.$$

Assume the existence of a cyclic subgroup $A \subset E[l]$ of order l defined over F which is equal to the $< q_v^{1/l} >$ for all $v \in S$. Let $E' = E/A$.

Denote by $h(\cdot)$ and $\Delta(\cdot)$ the Faltings height function and the norm of the minimal discriminant function on elliptic curves. There is a constant C that depends only on ϵ such that

$$\log \Delta \leq (12+\epsilon)h + C.$$

By the computations in Faltings's 'Finiteness Theorems' paper, we have

$$h(E') \leq h(E) + 2\log l$$

and by a more elementary computation, $\Delta(E') = \Delta(E)^l$. Thus,

$$l \log \Delta(E) = \log \Delta(E') \leq (12+\epsilon)h(E') + C \leq (12+\epsilon)h(E) + (12+\epsilon)2\log l + C.$$

Denote by $B = \prod_{v \in F_\infty} B_v$ a product of compact domains with open interiors in $\prod_{v \in F_\infty} \mathbb{A}^1(K_v)$, where F_∞ denotes the set of Archimedean places. Denote by $\mathcal{C}_B$ the set of elliptic curves E as above whose j-invariants are in B. Then for all $E \in \mathcal{C}_B$, we have

$$(12+\epsilon)h(E) \leq \log \Delta(E) + C',$$

with C' depending on F and ϵ. Thus, for $E \in \mathcal{C}_B$, we get

$$(12+\epsilon)lh(E) - lC' \leq (12+\epsilon)h(E) + (12+\epsilon)2\log l + C,$$

or

$$h(E) \leq \frac{1}{(12+\epsilon)(l-1)}(C + lC') + \frac{2\log l}{l-1}.$$

From this, we deduce bounds on the height and log discriminant of the elliptic curves in $\mathcal{C}_B$. This is not quite Szpiro's inequality, but hints at an approach to it in realistic cases.

In the AECGP paper, it is shown that Szpiro's inequality for the curves in $\mathcal{C}_B$ will imply it in general. It is also shown that it suffices to prove it for E such that E minus the origin e is a curve of strict Belyi type.

Correction (27/12/2015): Mochizuki has pointed out to me that an elliptic curve minus the origin is automatically strictly of Belyi type. It seems I was rather confused about the definition.

Whatever this means, the anabelian consequence is that the ground field can be algorithmically constructed from the augmented etale fundamental group

$$\pi_1(E \setminus \{e\}) \longrightarrow \mathrm{Gal}(\bar{F}/F).$$

This sort of statement is also true over local fields with the tempered fundamental group in place of the profinite π_1. The precise formulation of 'algorithmic construction' appears to be rather delicate. The model case to keep in mind is the construction of the function field $k(X)^\times$ of a curve X over a finite field from its absolute Galois group. Here, one first expresses all the multiplicative groups of local fields $k(X)_v^\times$ as subgroups of the abelianisation of the decomposition groups. The unit subroups can also be expressed as inertia subgroups. Then, $k(X)^\times$ itself can be expressed as the subgroup of the ideles given as the kernel of the reciprocity map. The difficult part of course is to recover the additive structure. However, it's clear that the set $k(X) = \kappa(X)^\times \cup \{0\}$ itself has a description purely in terms of the group. What Mochizuki does is express F and F_v similarly using just the data of the augmented π_1. One should think of such results as having the same spirit as the construction of a field from a projective geometry over it.

We will assume now that $E \setminus \{e\}$ is of strict Belyi type.

2. Simulation of the subgroup A.

Let K be the field extension of F generated by $E([l])$. We have to choose l a bit carefully, so that, for example, the image of $\mathrm{Gal}(K/F)$ in $\mathrm{Aut}(E[l])$ contains $SL_2(\mathbb{F}_l)$. Denoting by V_K and V_F the set of places of K and F, there is the restriction map $V_K \xrightarrow{r} V_F$. Denote by $\underline{V}$ a section of r satisfying certain conditions. Thus, we are choosing a place of K over each place of F. The main condition has to do with the set $\underline{V}_S$ of places of $\underline{V}$ lying above the bad primes S. For each $v \in \underline{V}_S$, we will continue to use the notation of the previous section for the Tate parametrization. We assume the existence of a subgroup $A \subset E[l]$ such that for $v \in \underline{V}_S$, A does indeed agree with the subgroup $< q_v^{1/l} >$. The existence of such a section $\underline{V}$ after choosing A first is guaranteed by the condition on the Galois action: Note that we are insisting on the consistency between the local and global subgroup not at all primes of bad reduction in K, but only those in $\underline{V}$. The main goal of the IUTT papers is to carry out the 'ideal' argument of section 1 using E_K and $\underline{V}$ in place of E and $\mathrm{Spec}(\mathcal{O}_F)$.

In order to get a feeling for how this might work, recall a formula of Szpiro that says

$$(1/12)\log\Delta(E_K) = -<e,e>,$$

where e is the origin on a regular minimal model of E. That is, $-h(E_K)$ is essentially the self-intersection number of the origin. Denote the isogeny from E to E' by f and the origin of a regular minimal model of E' by e'. Then

$$h(E') \sim -<e',e'>= -<f_*(e),e'>= -<e,f^*(e')>\sim -<e,\bar{A}> .$$

(We denote also by f an extension of f to the regular minimal model, which probably exists, even though I don't quite remember the relevant theorem.)
Here, I'm being a bit sloppy about the intersection contribution of $\bar{A}$, the closure of A, since some contracted divisors may get in the way. In any case to compute this intersection number, one could first compute the intersection between Ne and A for some multiple N and divide the result by N. But then, there will be a section θ of $\mathcal{O}(Ne)$, a theta function, which doesn't vanish on any of the points in A. Hence, we would get something like

$$-<e,\bar{A}>= (1/N)[\sum_{v \text{ finite}}(\sum_{x\in\bar{A}} -\log\|\theta(x)\|_v) + \sum_{v \text{ infinite}}(\sum_{x\in\bar{A}}\log\|\theta(x)\|_v)].$$

Thus, we need to examine the contributions $\sum_{x\in \bar{A}} \log \|\theta(x)\|_v$ for each v, which is probably dominated by the primes of bad reduction. (I'm not sure about how to bound the Archimedean contributions. This is possibly done by choosing θ having small Archimedean sup norm.) But notice that this is still a sum over *all* primes of bad reduction in K. At the $v \in \underline{V}_S$, the equality $A =< q_v^{1/l} >$ allows us to identify the values $\theta(x)$ with powers

$$q_v^{j^2/(2l)}, \quad 1 \leq j \leq (l-1)/2$$

of $q_v^{1/(2l)}$, at least after normalising θ carefully (and replacing it by an l-th root $\underline{\underline{\Theta}}$). If we had this behaviour at all the bad v, we would end up with a bound for $h(E_K)$ similar to that of the previous section, since we are repeating the same computation over a different field. However, this will be very rare, if at all possible (maybe for $l = 2$ and very special curves?).

3. Estimating arithmetic degrees

To proceed from here, I will give one possible approach that is different from the IUTT papers, and which Mochizuki believes is doomed to failure. This is to try to recover the values $\log \|\theta(x)\|_v$ at the 'missing' v in terms of the values at $v \in \underline{V}_S$. For this, one would need various anabelian reconstruction theorems, including a π_1 description of the theta function. A theory of this sort is developed in the étale theta function paper. That is, a theta function as a section of a line bundle is essentially the 'Frobenioid' manifestation. (Recall that Frobenioids are categories of line bundles with sections parametrised by a base category of Galois type.) However, one can also look at a Kummer class

$$\kappa(\underline{\underline{\Theta}}) \in H^1(\pi_v, \hat{\mathbb{Z}}(1)),$$

where π_v is the tempered fundamental group of $(E \setminus \{e\}) \otimes K_v$ (or some subscheme, covering scheme, etc), and $\underline{\underline{\Theta}}$ is some carefully chosen l-th root of θ^{-1}. This is the étale theta function. One evaluates this class at the various $x \in A$ to get Kummer classes $x^*(k(\underline{\underline{\Theta}})) \in H^1(G_v, \hat{\mathbb{Z}}(1))$. According to the paper, these classes will be the Kummer classes of the values $\underline{\underline{\Theta}}(x) \in K_v^*$. One obtains thereby an anabelian description of these values (up to some harmless ambiguities).

Here is then a possible strategy: The

$$\pi_w \longrightarrow G_w$$

for $w \notin \underline{V}$ are isomorphic to such a pair

$$\pi_v \longrightarrow G_v$$

at $v \in \underline{V}$. So perhaps the sum

$$\sum_{w\in r^{-1}(V_F)} (\sum_{x\in\bar{A}} \log \|\underline{\underline{\Theta}}(x)\|_w)]$$

can be expressed in terms of the sum with fewer terms:

$$\sum_{v\in\underline{V}_S} (\sum_{x\in\bar{A}} \log \|\underline{\underline{\Theta}}(x)\|_v)]?$$

Since the anabelian construction of the K_w for $w \notin \underline{V}$ from the $\pi_v \longrightarrow G_v$ for $v \in \underline{V}_S$ has no reason to preserve the powers of $q^{1/(2l)}$ in a coherent manner, getting a bound out of this strategy will not be straightforward.

Correction: This is not right. If it's just a question of computing valuations, this can be done in an anabelian way. (Or a 'mono-anabelian' way.) That is, as Saidi points out to me, just from G_{K_v}, one can construct the multiplicative group K_v^* together with the valuation map $K_v^* \longrightarrow \mathbb{Z}$. Of course one gets the profinite completion of K_v^* and the units $O_{K_v}^* \subset \widehat{K_v^*}$ using class field theory. So one needs to construct the Frobenius element in

$$\widehat{K_v^*}/O_{K_v}^* \simeq G_{K_v}^{un}.$$

But one does this by constructing the Galois module $\hat{\mathbb{Z}}^{(p)}(1)$ of the inverse limit of roots of 1 prime to the residue characteristic p (which itself can be read off from the profinite group $O_{K_v}^*$) . This is, for example, the unique Galois module $\simeq \hat{\mathbb{Z}}^{(p)}$ such that

$$H^2(G_{K_v}, \hat{\mathbb{Z}}^{(p)}(1)) \simeq \hat{\mathbb{Z}}^{(p)}.$$

Then, the Frobenius element can be characterized by it's action on the quotients μ_n for n prime to p. So the problem must be elsewhere.

Correction (27/12/15): It seems the faliure of this strategy is simply that the Galois conjugation that takes π_w to π_v will not preserve the subgroup A.

However, my initial thought was that this is possibly where the 'controlled distortions', referred to often in the IUTT papers, need to be calculated. When this is all done, one might optimistically hope that a bound emerges rougher than the 'ideal' one, but sufficient for a version of Szpiro's inequality.

However, Mochizuki assures me that the papers proceed by

> *completely forgetting about the $v \notin \underline{V}$.*

What is developed rather is a version of the intersection theory and arithmetic degree argument using *only the primes in $\underline{V}$*. This is one of the senses in which scheme theory has been dismantled. It is not hard to imagine that a version of the ideal argument exists, provided such a degree theory exists. The IUTT papers develop such a theory. However, Mochizuki has emphasised that the degree doesn't apply to a general arithmetic divisor. Rather, it is only the degree of specific arithmetic divisors of interest, mostly the $\Sigma_{v\in\underline{V}_S} \log \|\underline{\underline{\Theta}}(x)\|_v$, that are computed (in a suitable sense).

I lack the understanding to say much more at the moment. However, it might be worthwhile still to convey my superficial intuition surrounding a few more ingredients, bearing in mind that much of what I write now is guesswork. From a certain point of view, the main obstruction to developing a degree theory for divisors supported on $\underline{V}$ is that the group K_S^* of numbers in K that are units outside of S is not closed under addition[1]. So one needs to develop some formalism to overcome this. The key tool here is the log map

$$\log_v : \bar{K}_v^* \longrightarrow \bar{K}_v,$$

which Mochizuki views as 'mixing up' addition and multiplication. The vertical portion of his 'log-theta lattice' contains an infinite sequence of such maps (ignoring many subtleties even about the precise domain and range of the log map, which make up the 'log shells' of the IUTT papers)

$$\xrightarrow{\log_v} \bar{K}_v \xrightarrow{\log_v} \bar{K}_v \xrightarrow{\log_v} \bar{K}_v \xrightarrow{\log_v}$$

on which the log map itself acts as an endomorphism (repreatedly emphasised to be an analogue of the Frobenius map). In some sense that I don't understand, one passes then to a quotient of this sequence modulo the log endomorphism, and thereby ends up with an object where addition and multiplication are identified. I think the way this is actually carried out is by constructing log-equivariant versions of the objects of interest, especially arithmetic divisors. That is, we are here

[1] Incidentally, this kind of non-additive property is also well-known in usual Arakelov theory, whereby the set of global sections in the Arakelov sense do not form a group.

employing the stack-theoretic convention that when a group Gr acts on a space Sp, Gr-equivariant objects on Sp amount to the same kind of objects on the stack Sp/Gr.

The equivariant construction is one of the many sources of the indeterminacies that need to be estimated. Another main difficulty is to deal with the discrepancy between the image of K inside $\prod_{v\in\underline{V}} K_v$ and the image after taking the log. After these difficulties are dealt with, my impression is that one ends up therefore with something like a 'degree map with indeterminacies,' (the 'procession normalised mono-analytic log volume') which however can be precisely controlled. The inequality between the arithmetic degree of

$$\log \underline{\underline{q}} = (\log(q_v^{1/(2l)}))_v$$

and the possible arithmetic degrees of the log-equivariant

$$\log \underline{\underline{\Theta}}(x) = (\log \|\underline{\underline{\Theta}}(x)\|_v)_v$$

is the main concern of IUTT III, and is analysed using the interaction between the vertical log direction and the horizontal theta direction of the two-dimensional lattice. The theta direction, by the way, is a sophisticated version of the evaluation map on theta functions.

Mohamed Saidi has stressed to me that the inquality in IUTT III is not Szpiro's inequality per se. Rather, what is proved is the slightly curious statement that whenever a constant C_Θ satisfies

$$-|\log \underline{\underline{\Theta}}| \leq C_\Theta |\log \underline{\underline{q}}|,$$

then $C_\Theta \geq -1$. Then, in IUTT IV, a specific C_Θ, involving $h(E)$, the discriminant of the field, and various other simple numbers, is shown to satisfy this inequality. For that specific choice, $C_\Theta \geq -1$ is Szpiro's inequality.