Control Theorems for Abelian varieties over Global Function Fields of Characteristic $p$

Ki-Seng Tan

January, 21, 2008
This talk is about a function field version of Mazur’s control theorems for abelian varieties over $\mathbb{Z}_p^d$-extensions

(”Rational points of abelian varieties with values in towers of number fields”, Invent. Math. 18(1972), 183-266;


Let $A$ be an abelian variety over a field $K$ of characteristic $p$. We regard $A$ as a sheaf for the flat topology on $K$. And for each positive integer $m$, we use $A[p^m]$ to denote the kernel of the multiplication by $p^m$ on $A$, while as usual we use $A[p^m]$ to denote the $p^m$-torsion points on $A$. 
Suppose that $K$ is a global function field. The $p^m$-Selmer group $\text{Sel}_{p^m}(K)$ is defined as the kernel of the composite

$$H^1(K, A[p^m]) \longrightarrow H^1(K, A) \xrightarrow{\text{loc}} \bigoplus_v H^1(K_v, A),$$

where $\text{loc}$ is the localization map and in the direct sum $v$ runs through all places of $K$.

The $p^\infty$-Selmer group $\text{Sel}_{p^\infty}(K)$ is defined as the direct limit of $\text{Sel}_{p^m}(K)$.

**Theorem. 1** Let $A$ be an abelian variety over a global field $K$ of characteristic $p$. Suppose $L/K$ is a $\mathbb{Z}_p^d$-extension unramified outside a finite set $S$ of places of $K$. And assume that $A$ has good, ordinary reduction at each place $v \in S$. Then for all finite intermediate extensions $L'/K$ of $L/K$, the orders of the kernels and co-kernels of the restriction maps

$$\text{Sel}_{p^\infty}(K) \longrightarrow \text{Sel}_{p^\infty}(L')^{\text{Gal}(L'/K)}$$
are bounded.


**Application Iwasawa theory:** For an extension $L/K$ satisfying the conditions in the theorem, define $\text{Sel}_{p^\infty}(L)$ as the direct limit of $\text{Sel}_{p^\infty}(L')$ for $L'$ runs through all intermediate fields of $L/K$ and denote $\Gamma = \text{Gal}(L/K)$. By Nakayama’s Lemma, it follows from the theorem that the Pontryagin dual

$$X_L := \text{Hom}(\text{Sel}_{p^\infty}(L), \mathbb{Q}_p/\mathbb{Z}_p)$$

is a finitely generated module of the Iwasawa algebra $\Lambda_\Gamma := \mathbb{Z}_p[[\Gamma]]$.

The case where $A/K$ is a non-isotrivial elliptic curve has been studied by A. Bandini and I. Longhi, in “Control theorems for elliptic curves over function fields” (manuscript 2006. Available online at http://arxiv.org/abs/math/0604249).
The local control theorem:

**Theorem. 2** Assume that $A$ is an abelian variety over a local field $K = \mathbb{F}_q((T))$ so that the reduction $\overline{A}$ of $A$ is an ordinary abelian variety. If $L/K$ is a $\mathbb{Z}_p^d$-extension, then

$$|H^1(L/K, A(L))| \leq |\overline{A}(\mathbb{F}_q)_p|^{d+1},$$

here $\overline{A}(\mathbb{F}_q)_p$ denotes the $p$-Sylow subgroup of $\overline{A}(\mathbb{F}_q)$.

Theorem 2 $\implies$ Theorem 1,

by more or less standard arguments using the following: (1) the Hochschild-Serre spectral sequence, (2) the fact that $A(L)_p := A[p^\infty]$ is unramified over $K$, (3) the boundedness of

$$H^i(L'/K, A(L')_p), \quad i = 1, 2.$$

The rest of this talk is devoted to proving Theorem 2.
Assume that $K = \mathbb{F}_q((t))$.

For each $n$, denote $K^{(1/p^n)} = \mathbb{F}_q((t^{1/p^n}))$ which is the unique purely inseparable extension over $K$ of degree $p^n$.

Use $\bar{K}$ to denote the separable closure of $K$ and write $G_K = \text{Gal}(\bar{K}/K)$. And simply write $\bar{K}^{(1/p^n)} = \overline{K^{(1/p^n)}}$.

Thus, the algebraic closure of $K$ equals

$$\bar{K}^{(1/p^\infty)} := \bigcup_{n=1}^{\infty} \bar{K}^{(1/p^n)}.$$ 

The Frobenius substitution

$$\text{Frob}_{p^n} : K^{(1/p^n)} \longrightarrow K, \quad x \mapsto x^{p^n},$$

is an isomorphism. And we use it to identify $G_{K^{(1/p^n)}}$, for $n = 1, \ldots, \infty$, with $G_K$. 
We have the following useful illustration:

\[ \bar{K} \hookrightarrow \bar{K}(1/p) \hookrightarrow \bar{K}(1/p^n) \hookrightarrow \bar{K}(1/p^\infty) \]

\[ \begin{array}{c|c|c|c|c}
| G_K & | G_K & | G_K & | G_K \\
K & K(1/p) & K(1/p^n) & K(1/p^\infty) \\
\end{array} \]

§ Some facts about ordinary abelian varieties.

Assume that \( K \) is a field of characteristic \( p \) and \( A/K \) is an abelian variety of dimension \( g \). Over the algebraic closure of \( K \), the étale part of the group scheme \( A[p] \) is of the form \( (\mathbb{Z}/p\mathbb{Z})^{g-r} \) for some non-negative integer \( r \).

\( A/K \) is ordinary if and only if

\[ r = 0. \]

In this case, the multiplication by \( p \) on \( A \), is decomposed as:

\[ [p] = V \circ F, \]

where \( V \) is...
where $F : A \to A^{(p)}$ is the Frobenius isogeny and $V : A^{(p)} \to A$ is separable.

For the rest of this talk, $K$ is a local field and $\bar{A}$, the reduction of $A$, is an ordinary abelian variety.

**(a)** The étale part of $\bar{A}[p]$ equals $(\mathbb{Z}/p\mathbb{Z})^g$, and so is that of $A[p]$. The reduction map gives rise to an isomorphism

$$A[p^m] \simeq \bar{A}[p^m] \simeq (\mathbb{Z}/p^m\mathbb{Z})^g.$$  

Therefore, $A/K$ is also ordinary.

**(b)** If $L$ is a local field containing $K$ and $P$ is a point in $A(L)$, then all the $p^m$-division points of $P$ are contained in $A(\bar{L}(1/p^m))$. In particular, the $p^m$-torsion points $A[p^m] \subset A(\bar{K}(1/p^m))$. 
(c) Suppose $L/K$ is a Galois extension and $I \subset \text{Gal}(L/K)$ is the inertia group. If $\sigma \in I$ and $Q \in A(L)_p$, then (a) says that $\sigma Q - Q = 0$. Therefore, $A(L)_p$ is unramified over $K$, in the sense that every point in $A(L)_p$ is rational over the maximal unramified sub-extension of $L/K$.

(d) Let $A^1(L)$ denote the subgroup of $A(L)$ consisting of points with trivial reduction. Then $A^1(L)$ is a torsion free $\mathbb{Z}_p$-module.

(e) For each $P \in A^1(L)$ there is a unique $P' \in A^1(L^{(1/p^m)})$ such that $p^m P' = P$, and vice versa. In other words, we have

$$A^1(L) = p^m A^1(L^{(1/p^m)}). \quad (1)$$

To see this, let $Q \in A(\bar{L}^{(1/p^m)})$ be a $p^m$-division point of $P \in A^1(L)$. Since the reduction $\bar{Q}$ is contained in $\bar{A}[p^m]$, there is
a point \( R \in A[p^m] \subset A(\bar{L}(1/p^m)) \) such that \( P' := Q - R \in A^1(\bar{L}(1/p^m)) \). Obviously, \( P' \) is also a \( p^m \)-division point of \( P \), and for \( \sigma \in G_L \), we have

\[
\sigma P' - P' \in A[p^m] \cap A^1(\bar{L}(1/p^m)) = \{0\}.
\]

(f) For a local field \( L \) finite over \( K \), we use \( \mathbb{F}_L \) to denote its constant field. And we also regard \( \mathbb{F}_L \) as the residue field of \( L \). One easily deduces from (a) and (e) that

\[
A(L(1/p^\infty)) = A^1(L(1/p^\infty)) \times A(L(1/p^\infty))_{tor}
\]

and the reduction map sends \( A(L(1/p^\infty))_{tor} \) bijectively onto \( \bar{A}(\mathbb{F}_L) \). Furthermore, this bijection respects the action of \( \text{Aut}_K(L) \). In view of this, the \( G_K \)-modules \( A(\bar{K}(1/p^\infty))_{tor} \) and \( \bar{A}(\mathbb{F}_q) \), are isomorphic under the reduction map.

\[\text{Tate's local duality Theorem}\]
Let $B$ denote the dual abelian variety to $A$ over $K$. Since $B$ is isogenous to $A$, it also has ordinary reduction.

Via the Poincaré biextension $W \rightarrow A \times B$, a point on $B$ is regarded as an element in $\text{Ext}(A, G_m)$, and hence a point $Q \in B(L)$ gives rise to an exact sequence of $G_L$-modules:

$$0 \rightarrow \bar{L}^* \rightarrow W_Q \rightarrow A(\bar{L}) \rightarrow 0.$$  

Using the induced long exact sequence:

$$\ldots \rightarrow H^1(L, A) \xrightarrow{\delta_Q} H^2(L, \bar{L}^*) \rightarrow \ldots,$$

one defines the local duality pairing of $Q$ and a class $\xi \in H^1(L, A)$ as

$$\langle \xi, Q \rangle_{A,B,L} := \text{inv}(\delta_Q(\xi)).$$

Here $\text{inv} : H^2(L, \bar{L}^*) \rightarrow \mathbb{Q}/\mathbb{Z}$ is the invariant of the Brauer group.
The pairing is compatible with isogenies. If \( \psi : A \to A' \) and \( \hat{\psi} : B' \to B \) are dual isogeny, then

\[
<, >_{A,B,L} : H^1(L, A) \times B(L) \to \mathbb{Q}/\mathbb{Z}
\]

\[
\downarrow \psi \quad \uparrow \hat{\psi}
\]

\[
<, >_{A',B',L} : H^1(L, A') \times B'(L) \to \mathbb{Q}/\mathbb{Z}.
\]

In particular, for \( Q' \in B^{(p)}(L) \) and \( \xi \in H^1(L, A) \), we have

\[
< \xi, \hat{F}(Q') >_{A,B,L} = < F(\xi), Q' >_{A^{(p)},B^{(p)},L}.
\]

Tate’s local duality theorem says that the local pairing is non-degenerated, and it identifies \( H^1(K, A) \) with the Pontryagin dual of \( B(L) \).

**Lemma. 3** Let \( i_* \) be the homomorphism from \( H^1(K, A) = H^1(G_K, A(\bar{K})) \) to \( H^1(G_K, A(\bar{K}^{1/p^\infty})) \) induced from the inclusion \( A(\bar{K}) \to A(\bar{K}^{1/p^\infty}) \). If \( i_*(\xi) = 0 \), then \( \xi \) annihilates \( B^1(K) \).
Kummer Theory

Over the field $\bar{K}^{(1/p^\infty)}$, we have the following exact sequence of $G_K$-modules:

$$0 \longrightarrow A[p^m] \xrightarrow{j} A(\bar{K}^{(1/p^\infty)}) \xrightarrow{[p^m]} A(\bar{K}^{(1/p^\infty)}) \longrightarrow 0.$$ 

We are allowed to replace $A[p^m]$ by $\bar{A}[p^m]$ ((f)).

And by taking the direct limit over $m$ for the induced Kummer sequence, we get the following exact sequence:

$$0 \longrightarrow A(K^{(1/p^\infty)}) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\text{H}^1(G_K, \bar{A}[p^\infty])} \text{H}^1(G_K, A(K^{(1/p^\infty)})) \xrightarrow{j^*} 0 \leftarrow \text{H}^1(G_K, A(K^{(1/p^\infty)}))_p,$$

Equations (1) implies

$$A(K^{(1/p^\infty)}) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p = 0.$$  (2)
Let \( k_* = j_*^{-1} \circ i_* : H^1(K, A)_p \rightarrow H^1(G_K, \bar{A}[p^\infty]) \).

By Lemma 3,

\[
\ker(k_*) \subset \hat{B}(\mathbb{F}_q) \quad (3)
\]

We have \(|\hat{B}(\mathbb{F}_q)| = |\bar{B}(\mathbb{F}_q)| = |\bar{A}(\mathbb{F}_q)|\).

**Lemma. 4** Suppose \( L/K \) is a \( \mathbb{Z}_p \)-extension, then for every finite intermediate extension \( L'/K \subset L/K \) we have

\[
|H^1(L'/K, \bar{A}(\mathbb{F}_{L'})_p)| \leq |\bar{A}(\mathbb{F}_K)_p|^d.
\]

\( \S \) The proof of Lemma 3

Let \( L/K \) be a finite extension. We first consider of the map

\[
H^1(G_L, A(\bar{L})) \xrightarrow{i_1^*} H^1(G_L, A(\bar{L}^{(1/p)}))
\]
induced from $A(\bar{L}) \xrightarrow{i_1} A(\bar{L}(1/p))$. Next, we show that if $i_1^*(\xi)$ annihilates $B^1(L(1/p))$, then $\xi$ annihilates $B^1(L)$.

The lemma is proved by inductively taking $L = K(1/p^m)$ for $m = 0, 1, ..., \infty$.

The ideal is to relate the map $i_1$ to some isogeny.

The Frobenius substitution $\text{Frob}_p$ induces an isomorphism of $G_L$-modules

$$\text{Frob}_p : A(\bar{L}(1/p)) \rightarrow A(p)(\bar{L}) \quad \text{with} \quad P \mapsto F(P).$$

Therefore,

$$A(\bar{L}) \xrightarrow{i_1} A(\bar{L}(1/p)) \quad \text{and the bottom right arrow induces} \quad H^1(G_L, A(\bar{L})) \xrightarrow{F^*} H^1(G_L, A(p)(\bar{L})).$$
• \( \iota_1^*(\xi) \) annihilates \( B^1(L^{(1/p)}) \) if and only if \( F^*(\xi) \) annihilates \( (B^p)^1(L^{(1/p)}) \).

Let \( \widehat{F} : B^p \longrightarrow B \) be the dual isogeny to \( F \).

• \( F^*(\xi) \) annihilates \( (B^p)^1(L^{(1/p)}) \) if and only if \( \xi \) annihilates \( \widehat{F}( (B^p)^1(L) ) \).

The kernel of \( \widehat{F} \), which is the dual of \( (\mu_p)^g \), is exactly the maximal etale subgroup of the group scheme \( B^p[p] \), where \( B^p[p] \) denotes the kernel of the multiplication by \( p \) on \( B^p \).

But, if we write \( [p]_B \), the multiplication by \( p \) on \( B \), as the composite \( V_B \circ F_B \), then the kernel of \( V_B \) also equals the maximal etale subgroup of \( B^p[p] \). Therefore,

\[
\widehat{F}( ((B^p)^1)(L) ) = V_B( ((B^p)^1)(L) ).
\]

Equality (1), for \( A = B \), says

\[
B^1(L) = pB^1(L^{(1/p)}) = V_B(F_B(B^1(L^{(1/p)}))).
\]
which is a subset of $V_B((B^{(p)})^1(L))$. Q.E.D.

§ The proof of Lemma 4

Let $L'_0$ be the maximal unramified extension of $K$ contained in $L'$. Write $G = \text{Gal}(L'/K)$, $H_0 = \text{Gal}(L'/L'_0)$, $M = \bar{A}(\mathbb{F}_{L'})_p$. We have $M = M^{H_0}$

Consider the inflation-restriction exact sequence:

$$
\begin{align*}
\text{H}^1(G/H_0, M) &\xrightarrow{\text{inf}} \text{H}^1(G, M) \\
&\downarrow \text{res} \\
\text{H}^1(H_0, M)^{G/H_0} &
\end{align*}
$$

We shall bound the orders of $\text{ker}(\text{res})$ and $\text{Im}(\text{res})$.

Since $G/H_0$ is cyclic, by computing the Herbrand quotient, one sees that

$$|\text{H}^1(G/H_0, M)| = |\bar{A}(\mathbb{F}_q)_p/\mathcal{N}|,$$

where $\mathcal{N}$ is the image of the norm map $N_{G/H_0} : M \rightarrow \bar{A}(\mathbb{F}_K)_p$. 
Also, since $M$ is fixed by the action of $H_0$, we have
\[
H^1(H_0, M)^{G/H_0} = \text{Hom}(H_0, \bar{A}(\mathbb{F}_q)_p).
\]
To proceed further, we choose a basis $e_1, ..., e_c$ of $G$, for some $c \leq d$, so that $e'_1 := p^m e_1, e_2, \ldots, e_c$, for some non-negative integer $m$, form a basis of $H_0$. The cocycle condition implies that if $\rho$ be a 1-cocycle representing a class in $H^1(G, M)$, then the value $\rho(e'_1)$ equals $N_{G/H_0}(\rho(e_1))$. And this implies that the image of $res$ must be contained in the subgroup
\[
\{ \phi \in \text{Hom}(H_0, \bar{A}(\mathbb{F}_q)_p) \mid \phi(e'_1) \in \mathcal{N} \},
\]
whose order is bounded by $|\bar{A}(\mathbb{F}_q)_p|^c \cdot |\mathcal{N}|$.
Q.E.D.