Moret-Bailly's theorem

Statement of the theorem.

We are going to sketch Moret-Bailly's proof of a theorem that is a version of a general class of theorems that goes by the name of Rumely's local-global principle.

Theorem (Moret-Bailly). *Let $\mathcal{M}$ be a geometrically irreducible variety over $\mathbb{Q}$. Let S_1 and S_2 be disjoint sets of places of $\mathbb{Q}$, with $\infty \in S_1$. Suppose for all $v \in S_1$, $w \in S_2$, $\mathcal{M}(\mathbb{Q}_v) \neq \emptyset$, $\mathcal{M}(\mathbb{Q}_w^{unr}) \neq \emptyset$. Then there is a finite Galois extension $F/\mathbb{Q}$ in which every place in S_1 splits completely and every place in S_2 is unramified, such that $\mathcal{M}(F) \neq \emptyset$.*

Moreover, if for all $w \in S_2$ there is a $Gal(\mathbb{Q}_w^{unr}/\mathbb{Q}_w)$-invariant open subset Ω_w of the w-adic manifold $\mathcal{M}(\mathbb{Q}_w^{unr})$ such that $\Omega_w \neq \emptyset$, then we can assume that $\mathcal{M}(F)$ contains a point x, for F a field as above, such that $x \in \Omega_w$ for all $w \in S_2$.

The second part of the theorem was important in the proof contained in the articles [CHT], [T], [HST], because it allowed us to keep track of the place of multiplicative reduction, but it appears to be unnecessary if one doesn't worry about this condition, thus it will be ignored.

Moret-Bailly's theorem is much stronger: he shows the existence of a point x that is *integral* at all places of $\mathbb{Q}$ but those in $S_1 \cup S_2$, plus (at least) one more, chosen arbitrarily. This may be useful in some applications. The theorem also applies to general number fields and to function fields of curves over finite fields.

Let $S = S_1 \cup S_2$, R the ring of S'-integers of $\mathbb{Q}$, where S' is any set of places strictly containing S, $B = Spec(R)$. Here are some simple reductions:

(1) The condition that $F/\mathbb{Q}$ be Galois is superfluous, one can always replace F by its Galois closure over $\mathbb{Q}$. Thus it does not need to be verified separately.

(2) As mentioned, the theorem is valid over any number field. Existence of local points over unramified extensions of $\mathbb{Q}_w$ means existence of local points over split extensions of K_w, after passing to an appropriate finite extension $K/\mathbb{Q}$. Thus we can assume $S = S_1$.

(3) Using Bertini's theorem and an argument of cutting by hypersurface sections, Moret-Bailly reduces the proof to the case where $\mathcal{M}$ is a curve. In the main applications, $\mathcal{M}$ will always be a curve, thus we may assume $\dim \mathcal{M} = 1$. Note however that one also needs to solve this problem simultaneously for several $\mathcal{M}_j$, which means that one needs to find an F that works for $\prod_j \mathcal{M}_j$, thus the reduction is in fact necessary.

(4) It is not asserted that $\mathcal{M}$ is projective, and this will not in fact be the case in the applications. Thus we may assume $\mathcal{M}$ to be an affine curve which extends to a projective curve $\bar{f} : \bar{\mathcal{M}} \to B$. Moreover, by shrinking $\mathcal{M}$ we may assume $f : \mathcal{M} \to B$ to be smooth and surjective, hence $\mathcal{M}$ is a regular (two-dimensional) scheme; we may normalize and assume $\bar{\mathcal{M}}$ to be normal.

We let $Z = \bar{\mathcal{M}} - \mathcal{M}$, of dimension ≤ 1, containing no fibers of $\bar{f}$; we give Z the reduced subscheme structure, and let g be the genus of $\bar{\mathcal{M}}_\eta$, $z = deg(Z_\eta)$, and we can always assume $z > 0$ (by adding a point if necessary). Since we don't care about integrality, we can shrink B so that $\bar{\mathcal{M}}$ is regular, the fibers of $\bar{f}$ are geometrically integral, Z is regular and finite, flat, and surjective over B (see [MB] for the justification).

For any integer $d > 0$, let $\mathcal{M}^{(d)}$ be the d-th symmetric power of $\mathcal{M}$

$$\mathcal{M}^{(d)} = \mathcal{M}^d / \mathfrak{S}_d$$

(fiber product over B). Let $U_d \subset \mathcal{M}^{(d)}$ be the complement of the diagonals. Since $\mathcal{M}$ is smooth over B, there is a functorial bijection for any B-scheme T identifying $\mathcal{M}^{(d)}(T)$ with the set of effective Cartier divisors $D \subset \mathcal{M}_T$, finite, flat, and of degree d over S; $U_d(T)$ correspond to étale Cartier divisors (no multiplicities).

For $v \in S$, let $\Omega_v^{[d]} \subset U_d(\mathbb{Q}_v) \subset \mathcal{M}^{(d)}(\mathbb{Q}_v)$ be the set of divisors in $D \subset \mathcal{M}(\mathbb{Q}_v)$ that are effective of degree d, étale, and split over $\mathbb{Q}_v$.

Proposition. *For all $d \geq 0$, $\Omega_v^{[d]}$ is a non-empty open subset of $U_d(\mathbb{Q}_v)$.*

Proof. Since $X^d \to X^{(d)}$ is étale over U_d, it defines an open map on $\mathbb{Q}_v$-valued points. One can construct a point in $\Omega_v^{[d]}$ by taking d distinct points in $\mathcal{M}(\mathbb{Q}_v)$.

For any T as above, let $PG(\bar{\mathcal{M}}, Z)(T)$ denote the group of equivalence classes of pairs $(\mathcal{L}, \alpha)$ where $\mathcal{L}$ is an invertible sheaf on $\bar{\mathcal{M}}_S$ and $\alpha : \mathcal{O}_{Z_S} \xrightarrow{\sim} \mathcal{L}_{Z_S}$ a trivialization over Z_S. The group structure is given by tensor product of invertible sheaves. Let $PG_d \subset PG$ be the subgroup of degree d. Then PG_0 is the generalized Jacobian (relative to the trivialization at Z. There is an exact sequence of sheaves:

$$1 \to (\mathbb{G}_m)_B \to (\pi_Z)_*(\mathbb{G}_m)_Z \to PG(\bar{\mathcal{M}}, Z) \to Pic_{\bar{\mathcal{M}}/B} \to 1.$$

Thus $PG(C\bar{M}, Z)$ is an extension of Pic by a torus, Pic_0 is the Jacobian of $\bar{\mathcal{M}}$, $Pic/Pic_0 = \mathbb{Z}_B$.

Any Cartier divisor $D \in \mathcal{M}^{(d)}(T)$ defines a class $cl^Z(D) \in PG_d(\bar{\mathcal{M}}, Z)$, the trivialization along Z being given by the canonical map $\mathcal{O}_{\bar{\mathcal{M}}} \to \mathcal{O}_{\bar{\mathcal{M}}}(D)$ which is an isomorphism outside D, and in particular along Z. There is thus a B-morphism

$$\phi_d : \mathcal{M}^{(d)} \to PG_d(\bar{\mathcal{M}}, Z)$$

analogous to the usual map from the symmetric power of a complete smooth curve to its Jacobian. For d sufficiently large, one knows that the latter map is a projective space bundle, the projective space over an invertible sheaf $\mathcal{L}$ being the projectivization of the space of sections of a sufficiently ample twist of $\mathcal{L}$, the set of zeroes of a given section defining a point in the symmetric power. In this relative generalized situation, the result is

Lemma. *Suppose $d \geq 2g + z - 1$. Then ϕ_d is a locally trivial fibration in affine spaces of dimension $d + 1 - g - z$*

More precisely, for any T, set

$$\Gamma(\bar{\mathcal{M}}_T, \mathcal{L}, \alpha) = \{s \in H^0(\bar{\mathcal{M}}, \mathcal{L}) \mid s|_Z = \alpha\}.$$

This is an affine space and there is a bijection

$$\mathcal{M}^{(d)}(T) = \{ \text{ isomorphism classes of triples } (\mathcal{L}, \alpha, s)\}$$

where $(\mathcal{L}, \alpha) \in PG_d(\bar{\mathcal{M}}, Z)(T)$ and $s \in \Gamma(\bar{\mathcal{M}}_T, \mathcal{L}, \alpha)$. Here D on the left maps to the pair $(cl^Z(D), s_D)$, and $(\mathcal{L}, \alpha, s)$ maps to $div(s)$.

We are very close to having translated the initial problem into a problem of strong approximation in the affine space $A = \Gamma(\bar{\mathcal{M}}, \mathcal{L}, \alpha)$. We can view A as a principal homogeneous space under the projective R-module (which we can even take to be free) $M = H^0(\bar{\mathcal{M}}, \mathcal{L}(-Z))$, the difference between any two α being a section of $\mathcal{L}$ vanishing on Z.

Lemma. *Let S' be a set of places of $\mathbb{Q}$ strictly containing S, and let R be the ring of S'-integers. Under localization, the R-affine space A is dense in $\prod_{v \in S} A \otimes_R \mathbb{Q}_v$.*

If we ignored S'-integrality, this would be quite standard. We apply the lemma as follows (we write PG_d for $PG_d(\bar{\mathcal{M}}, Z)$:

Lemma. *Let $\mathcal{L}$ be an invertible sheaf on $\bar{\mathcal{M}}$ of degree $d \geq 2g + z - 1$. Let α be a trivialization of $\mathcal{L}$ over Z, hence $(\mathcal{L}, \alpha) \in PG_d(R)$. Suppose that for every $v \in S$, the corresponding point in $PG_d(\mathbb{Q}_v)$ belongs to $\phi_d(\Omega_v^{[d]})$.*

Then there is an $s \in A = \Gamma(\bar{\mathcal{M}}, \mathcal{L}, \alpha)$ such that $div(s)_v \in \Omega_v^{[d]}$ for all $v \in S$. Moreover, any irreducible component of $div(s)$ defines a point of $\mathcal{M}$ over a number field in which the places in S split completely.

The first statement is an immediate consequence of strong approximation for A, since by an earlier proposition, the set of $sinA \otimes_R \mathbb{Q}_v$ such that $div(s) \in \Omega_v^{[d]}$ is open. The second statement just follows from the definitions. Since this may seem like we are getting something for nothing, I remind you that the property of a divisor D being in $\Omega_v^{[d]}$ is just that it is a union of d distinct points of $\mathcal{M}$ all rational over $\mathbb{Q}_v$. So the trick is to find a pair $(\mathcal{L}, \alpha)$ with the given local property.

Proposition. *Let $\mathcal{L}_0$ be an ample line bundle on $\bar{\mathcal{M}}$ (i.e., of positive degree). Under the above hypotheses, there exists an integer $n \geq 1$ and a trivialization α of $\mathcal{L}_0^{\otimes n} \mid_Z$ such that the pair $(\mathcal{L}_0^{\otimes n}, \alpha)$ satisfies the local hypotheses of the last lemma.*

Proof. Let $d = deg(\mathcal{L}_0)$. After taking an appropriate tensor power, we may assume $d \geq 2g + z$ and $\mathcal{L}_0 \mid_Z \xrightarrow{\sim} \mathcal{O}_Z$ (the latter hypothesis has to do with triviality of the class group of Z, which can be assumed by shrinking B). Take a trivialization α_0 of $\mathcal{L}_0$ on Z. Then any trivialization of $\mathcal{L}_0^{\otimes n}$ on Z is of the form $\lambda \cdot \alpha_0^{\otimes n}$ for some invertible function λ on Z. Set

$$\mathbb{Q}_S = \prod_{v \in S} \mathbb{Q}_v; \; G = PG_0(\mathbb{Q}_S)/Im(\Gamma(Z, \mathcal{O}_Z^{\times}),$$

the latter with the quotient topology on the S-adic topological group

Main Lemma. *The topological group G is quasi-compact; in particular, for any $g \in G$, the sequence $(g^n, n = 1, 2, \dots)$ has the identity as accumulation point.*

The proof of this lemma is in two parts. Recall that PG_0 is a generalized Jacobian, an extension of an abelian variety by a torus. For the abelian variety part, this is a consequence of projectivity of abelian varieties. For the torus part, this is a consequence of the Dirichlet unit theorem (for S-units), where the existence of an extra place in S' is crucial.

Admitting this lemma, I conclude the proof. There is an additional non-trivial property of the $\Omega_v^{[d]})$, namely

$$\Omega_v^{[d]}) \cdot \Omega_v^{[d']}) \subset \Omega_v^{[d+d']})$$

provided $d' > 0$ and $d \geq 2g + z$, which (like the construction of the affine fibration) is a consequence of the Riemann-Roch theorem. We define $\Omega_S^{[d]} = \prod_{v \in S} \Omega_v^{[d]})$, so that, for all $m, n \geq 1$,

$$\Omega_S^{[nd]}) \cdot \Omega_S^{[md]}) \subset \Omega_S^{[(m+n)d]}).$$

Fix a point $q_0 \in \Omega_S^{[d]})$ and let $p_0 \in PG_d(\mathbb{Q}_\Sigma)$ be the class of $(\mathcal{L}_0, \alpha_0)$. Now $\Omega' = q_0^{-1} \cdot \Omega_S^{[d]})$ is a neighborhood of the identity in $PG_0(\mathbb{Q}_S)$. Applying the Main Lemma, we conclude that there exists $n \geq 1$ such that $(p_0 q_0^{-1})^n \in \Gamma(Z, \mathcal{O}_Z^\times) \cdot \Omega'$. In other words, there exists $\lambda \in \Gamma(Z, \mathcal{O}_Z^\times)$ such that $(p_0/q_0)^n \in \lambda q_0^{-1} \Omega'$, i.e.

$$\lambda^{-1} p_0^n \in q_0^{n-1} \cdot \Omega_S^{[d]}.$$

But $q_0 \in \Omega_\Sigma^{[d]}$ and by the multiplicative property recalled above, this implies that

$$\lambda^{-1} p_0^n \in \Omega_S^{[nd]}.$$

Letting $\alpha = \lambda \cdot \alpha_0^n$, we find that $(\mathcal{L}_0^n, \alpha)$ satisfies the conclusion of the Proposition.