

# A new proof of Zilber's relative trichotomy conjecture

Dmitry Sustretov  
Ben Gurion University  
sustreto@math.bgu.ac.il

April 23, 2014

**Zilber's relative trichotomy: statement**

Let  $M$  be an algebraic curve over an algebraically closed field  $k$ , and let  $X \subset T \times M^2$  be a family of distinct curves on the surface  $M^2$ ,  $\dim T \geq 2$ .

**Conjecture.** One can recover the field  $k$  starting from the data  $M(k), X(k) \subset (T \times M^2)(k)$ , moreover, one can do it in a definable way: the field is definable in the first-order structure  $(M, X)$ .

Proved by Rabinovich (1993) for  $M = \mathbb{P}^1$ ,  $X$  is allowed to be a family of constructible sets.

I will present the main ideas of the new proof (joint work with Assaf Hasson) which in particular has no restrictions on  $M$ .

In this talk I will assume that  $X_t$  is closed irreducible for  $t$  in an open dense subset of  $T$  (ensuring this is the first step of the proof). One can also without loss of generality assume that  $M$  is smooth.

## Weil's birational group laws

Let  $G$  be an algebraic variety and let  $m : G \times G \dashrightarrow G$  be a rational map such that

$$(x, y) \mapsto (x, m(x, y)) \text{ and } (x, y) \mapsto (m(x, y), y) \text{ are birational maps and} \\ m(x, m(y, z)) = m(m(x, y), z) \quad (\text{whenever it makes sense})$$

Then  $m$  is called a *birational group law*.

**Theorem (Weil)** Let  $m : G \times G \rightarrow G$  be a birational group law. Then there exists an algebraic group  $G'$  such that  $G'$  is birationally equivalent to  $G$  and such that the group law on  $G'$  pulls back to  $m$  under an isomorphism of dense open subsets of  $G$  and  $G'$ .

The work of Artin generalises this result to group schemes.

## Correspondences and compositions

Let  $X, Y$  be two varieties or, more generally, schemes. In this talk we will call a closed subscheme  $Z$  of  $X \times Y$  a *correspondence* from  $X$  to  $Y$  if it projects surjectively on  $X$  and  $Y$ . Notation:  $\alpha : X \dashrightarrow Y$ ,  $\Gamma(\alpha) = Z$ .

If  $U \subset X(k)$  then  $\alpha(U) = p_Y \circ p_X^{-1}(U)$ . Similarly, if  $X$  is proper, and  $\mathcal{L}$  is a coherent sheaf of  $\mathcal{O}_X$ -modules then  $\alpha(\mathcal{L}) = p_{Y*}p_X^*(\mathcal{L})$  is a coherent sheaf of  $\mathcal{O}_Y$ -modules.

Given two correspondences  $\alpha : X \dashrightarrow Y, \beta : Y \dashrightarrow Z$  one defines their composition  $\beta \circ \alpha : X \dashrightarrow Z$

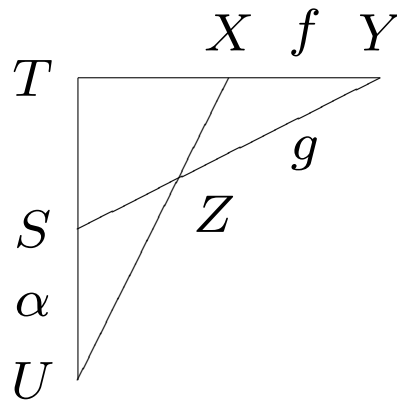
$$\Gamma(\beta \circ \alpha) = p_{XZ}(p_{XY}^{-1}(\Gamma(\alpha)) \cap p_{YZ}^{-1}(\Gamma(\beta)))$$

Similarly, for correspondences between proper schemes one considers pull-backs and pushforwards of sheaves of ideals defining their graphs, and scheme theoretic intersection

$$\mathcal{I}_{\Gamma(\beta \circ \alpha)} = p_{XZ*}(p_{XY}^*(\mathcal{I}_{\Gamma(\alpha)}) \otimes_{\mathcal{O}_{XYZ}} p_{YZ}^*(\mathcal{I}_{\Gamma(\beta)}))$$

## Hrushovski's group configuration

Hrushovski's theorem allows to recover a group law, in fact, even a group acting on a one-dimensional variety, from a collection of correspondences. One usually depicts the data as follows:



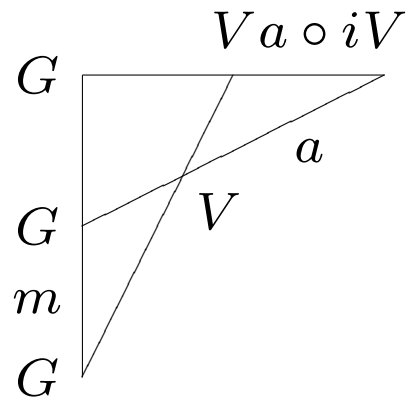
where  $f : T \times X \dashrightarrow Y$ ,  $g : S \times Z \dashrightarrow Y$ ,  $\alpha : X \times Y \dashrightarrow Z$  are correspondences, finite-to-finite at generic points. The line  $U - Z - X$  corresponds to the requirement that

$$\cup_{u \in \alpha(t,s)} \Gamma(g_s \circ f_t^{-1})$$

has an irreducible component that is a graph of a finite-to-finite correspondence  $h_u$  for generic  $u \in U$ .

## Hrushovski's group configuration, continued

If  $G$  is a group with the group law  $m : G \times G \rightarrow G$  and inverse  $i : G \rightarrow G$ , and  $a : G \times V \rightarrow V$  is faithful group action then one has a naturally associated configuration



**Theorem (Hrushovski).** Given a group configuration as on the previous slide,  $\dim S = \dim T = \dim U = 1$  there exists a (definable) group  $G$ , a definable set  $V$ , and a generically finite-to-finite correspondence  $\eta$

$$\begin{array}{ccc} & \Gamma(\eta) & \\ p_1 \swarrow & & \searrow p_2 \\ X \times Y \times Z \times S \times T \times U & & G^3 \times V^3 \end{array}$$

such that  $p_1^{-1}(\Gamma(\alpha)) = p_2^{-1}(\Gamma(\alpha'))$  share an irreducible component, for all respective correspondences  $\alpha$  and  $\alpha'$  in two configurations.

## Endomorphisms of fat points

The scheme of the form  $P_n = \text{Spec } k[x]/(x^{n+1})$  is called a *fat point*. Recall that  $\text{Hom}(P_1, X) \cong TX(k)$ .

One easily sees that  $\text{Aut}(P_1) = \mathbb{G}_m(k)$ ,  $\text{Aut}(P_2) = \mathbb{G}_a \rtimes \mathbb{G}_m(k)$ ; in general,  $\text{Aut}(P_n)$  is some unipotent linear group.

If the graph of a correspondence  $\alpha : X \dashrightarrow Y$  contains a point  $P$ , and the projection  $p_X$  is étale in a neighbourhood of  $P$  then by choosing closed embeddings  $P_1 \rightarrow M$  such that  $P_1 \times P_1 \rightarrow M^2$  maps the closed point to  $P$  and restricting  $\Gamma(\alpha)$  to  $P_1 \times P_1$  we get a graph of an endomorphism  $\tau_\alpha : P_1 \rightarrow P_1$ . We call  $\tau_\alpha$  an endomorphism of  $P_1$  associated to  $\alpha$  (at  $P$ ).

**Proposition.** Let  $\alpha, \beta : M \dashrightarrow M$  be two correspondences such that  $P \in \Gamma(\alpha), \Gamma(\beta)$  for  $P \in \Delta$ , where  $\Delta$  is the diagonal of  $M^2$ . Then

$$\tau_{\beta \circ \alpha} = \tau_\beta \circ \tau_\alpha$$

## Finding a one-dimensional subfamily

There exists a point  $P$  such that curves passing through  $P$  induce infinitely many distinct associated endomorphisms of  $P_1$ .

Indeed, suppose the contrary. Then there exists a function  $\varphi : M^2 \rightarrow \text{End}(P_1)$  such that for any point  $Q$  every curve  $X_t$  that passes through  $Q$  (except finitely many) has associated endomorphism  $\varphi(Q)$ . Then each  $X_t$  expanded into formal series  $y \in k[[x]]$  around some  $Q \in M^2$ , satisfies the equation

$$y' = f(x, y)$$

for some formal series  $f \in k[[x, y]]$ . But this ordinary differential equation has a unique solution with zero constant term (in char. 0), contradiction.

With some work one can actually find such a point on the diagonal  $P \in \Delta \subset M^2$ . We further denote as  $X^P$  the family of curves that pass through  $P$ , and it's parameter space as  $T^P$ .



## Defining “tangency”

Let  $X \rightarrow T, Y \rightarrow S$  be two families of curves in  $M^2$  that both pass through a point  $P$ .

**Fact.** The length of the structure sheaf of the scheme-theoretic intersection of  $Y_s$  and  $X_t$  as an  $\mathcal{O}_{M^2}$ -module is constant for  $(t, s)$  in a dense open subset of  $T \times S$ . Same for the number of irreducible components of the module.

Let  $N$  be the number of intersections  $\#(X_t \cap X_s)$  (on the level of geometric points, without counting multiplicities) for  $(t, s)$  in a dense open subset of  $T \times S$

**Proposition.** If  $\tau_{X_t} = \tau_{Y_s}$  then  $\#(X_t \cap Y_s) < N$ , where  $\tau_{X_t} = \tau_{Y_s}$  are the associated endomorphisms of  $P_1$ .

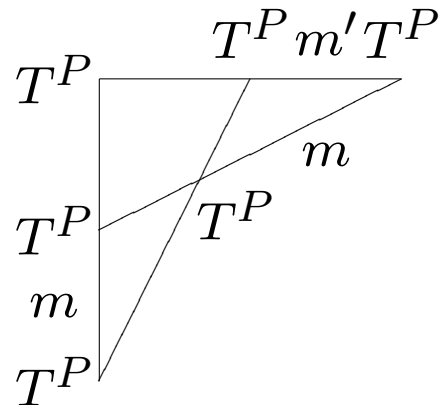
Notice that the opposite is not necessarily true. The relation  $\#(X_t \cap X_s) < N$  is thus possibly coarser than the relation  $\tau_{X_t} = \tau_{Y_s}$  and even if  $T = S$ , it might still be not transitive. However, it is definable in the structure  $(M, X)$  and it is enough to construct a group configuration.

## Building the group configuration

Let  $N$  be the number of intersections  $\#(X_t^P \circ X_s^P \cap X_u^P)$  for  $(t, s, u)$  in a dense open subset of  $T^3$ . Let  $m : T^P \times T^P \dashrightarrow T^P$  be the correspondence defined as follows:

$$\begin{aligned} \Gamma(m) &= \{ (t, s, u) \in (T^P)^3 \mid \#(X_t^P \circ X_s^P \cap X_u^P) < N \} \\ \Gamma(m') &= \{ (t, s, u) \in (T^P)^3 \mid \#(X_t^P \circ X_u^P \cap X_s^P) < N \} \end{aligned}$$

Consider the configuration



One checks that

$$\{ (u, z, x) \mid \tau_{X_x^P} = \tau_{X_z^P}^{-1} \circ \tau_{X_u^P} \} \subset \bigcup_{u \in \alpha(t, s)} \Gamma(m(s, -) \circ m(t, -))$$

Therefore,  $\Gamma(m)$ , which includes the lhs by the previous slide, intersects the rhs at a finite-to-finite correspondence, and the data satisfies the requirements of Hrushovski's theorem. There exists a definable one-dimensional group  $G$ .

## Reduct of an algebraic group: getting a field

The one-dimensional group that we have defined is in one-to-one correspondence with  $T^P$  and hence with  $M$ . We can therefore consider the image of the family  $X$  in  $G^2$  under the correspondence. There are other definable families of curves in  $G^2$ , and we can push them to  $G^2$  as well. A standard argument implies that there exists a family that does not consist of cosets of subgroups of  $G^2$ .

So our new setting is this: a one-dimensional algebraic group  $G$ , a definable set  $Z \subset G^2$  which is not a coset of a subgroup of  $G^2$ .

To complete the proof we need to define a field in the structure  $(G, \cdot, Z)$ . In fact, it suffices to define a two-dimensional group acting on a one-dimensional variety.

**Theorem** (*Cherlin, Hrushovski*) If  $G$  is a two-dimensional definable group (*in the setting of the conjecture*) acting on a definable one-dimensional set  $X$ , then  $G$  is definably isomorphic to  $(\mathbb{G}_a \rtimes \mathbb{G}_m)(K)$  for a definable field  $K$ .

That  $G$  is isomorphic to  $\mathbb{G}_a \rtimes \mathbb{G}_m$  can be directly observed for algebraic groups and varieties.

## Reduct of an algebraic group: getting a field, continued

We follow the same strategy as before: find a one-dimensional family of curves through the fixed point  $(0,0) \in G^2$  with infinitely many distinct associated endomorphisms of  $P_1$  and then define a group configuration.

This time we use two operations: composition of endomorphisms and their addition using group law.

$$Z + W := \{ (x, y) \in M^2 \mid y = y_1 + y_2, y_1 \in Z, y_2 \in W \}$$

**Lemma.** Let  $G$  be an algebraic group over a field  $k$ . Then there exists an exact sequence

$$1 \rightarrow \mathbb{G}_a^{\dim G}(k) \rightarrow G(P_1) \rightarrow G(k) \rightarrow 1$$

so the group law on  $T_0G$  is that of a vector group.

Therefore,  $\text{End}(P_1)$  has a structure of a ring (actually a field  $\cong k$ ), composition of curves inducing multiplication on  $\text{End}(P_1)$  and group law of  $G$  inducing addition.

**Reduct of an algebraic group: finding a one-dimensional family**

We consider the one-dimensional family of shifts of the definable curve  $Z \subset G^2$

$$X_t := Z - t, t \in T^0 = Z$$

One ensures that the associated endomorphisms of  $P_1$  are distinct.

$G = \mathbb{G}_a$  **and**  $G = \mathbb{G}_m$ . Passing to formal power series the condition that associated endomorphisms are constant in  $t$  amounts to a differential equation

$$y' = a \quad (\text{for } \mathbb{G}_a) \qquad \frac{y'}{y} = \frac{a}{x} \quad (\text{for } \mathbb{G}_m)$$

for some  $a \in k$ . Solving these equations we get that  $Z$  is a coset.

$G$  — **elliptic curve**. Suppose to the contrary that the  $T_t Z$  is constant as a subspace of  $T_0 G^2$ . Then  $TZ$  is trivial, hence  $Z$  is an elliptic curve, hence a coset of a subgroup of  $G \times G$ .

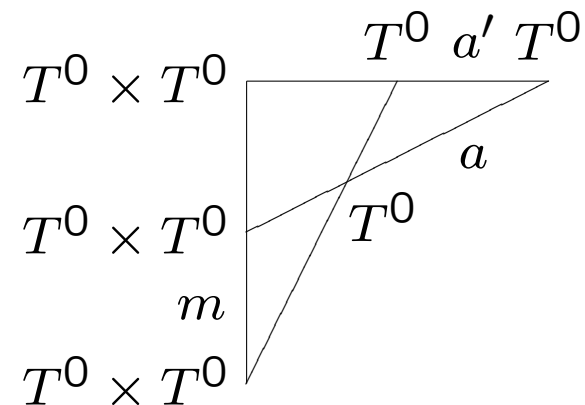
## Reduct of an algebraic group: two-dimensional group configuration

Define

$$\begin{aligned} \Gamma(m) &= \{ (t_1, t_2), (s_1, s_2), (u_1, u_2) \in (T^0 \times T^0)^3 \mid \\ &\quad \#(X_{t_1} \circ X_{s_1} \cap X_{u_1}) < N_1 \text{ and} \\ &\quad \#(X_{t_1} \circ X_{s_2} + X_{t_2} \cap X_{u_2}) < N_2 \} \\ \Gamma(a) &= \{ ((t_1, t_2), x, y) \in (T^0)^3 \mid \#(X_{t_1} \circ X_x + X_{t_2} \cap X_y) < K \} \\ \Gamma(a') &= \{ ((t_1, t_2), x, y) \in (T^0)^3 \mid \#(X_{t_1} \circ X_y + X_{t_2} \cap X_x) < K \} \end{aligned}$$

where  $N_1$ ,  $N_2$ ,  $K$  are numbers of intersections of generic elements of respective families of curves.

Consider the configuration



There are certain additional requirements for two-dimensional group configuration which are satisfied but I wish not to mention them here.

**Remarks on characteristic  $p$** 

Caveat: ODEs don't have unique solutions any more. Given

$$y' = f(x, y)$$

the solutions with zero constant term are a torsor under  $k[[x^p]]$ .

**Proposition.** There exists a point  $P$  and a one-dimensional family of curves  $X^P \rightarrow T^P$  such that one of the following holds

1. there are infinitely many endomorphisms of  $P_1$  associated to curves  $X_t^P$ ;
2. expansion of  $X_t^P$  into power series lies in  $k[[x]]^{p^n}$  for almost all  $t \in T^P$ ;
3. expansion of  $X_t^P$  into power series is of the form  $ax + (f_t)^{p^n}$  for almost all  $t \in T^P$ .

## Remarks on characteristic $p$ , continued

In the first case we can proceed as in char. 0.

In the second case, we consider the family of curves of the form  $X_{s_0}^{-1} \circ X_t$ , and there are infinitely many associated endomorphisms of  $P_1$ .

In the third case we consider the family of curves of the form  $X_{s_0}^{-1} \circ X_t$ , and there are infinitely many associated endomorphisms of  $P_{p^n}$ .

One encounters similar problems with the second group configuration. Due to non-uniqueness of solutions of respective ODEs it might be the case that we have a non-coset  $Z$  such that its shifts  $Z - t$  have constant associated endomorphism of  $P_1$ . However, using group operation and composition, it is always possible to construct a definable set that does not have this property.