Non locally modular reducts of ACF

Dmitry Sustretov
Hebrew University

Neostability theory, Oaxaca

sustretov@ma.huji.ac.il

July 13, 2015

Non locally modular strongly minimal sets

Let M be a strongly minimal set. Then model theoretic algebraic closure acl : $\mathcal{P}(M) \to \mathcal{P}(M)$ defines a pregeometry.

Zilber have conjectured that M can be understood up to bi-interpretability by studying the pregeometry acl. He isolated three cases: locally modular trivial, locally modular non-trivial, and non locally modular, with two latter giving rise to an interpretable algebraic structure. The hardest case is the last one.

Conjecture (Zilber): a non locally modular strongly minimal set interprets an algebraically closed field. (refuted by Hrushovski'91)

Non local modularity is equivalent to existence of a two-dimensional *pseudo-plane*: $X \subset S \times T$, where S is of Morley degree 1, $\dim S = \dim T = 2$, X_t is strongly minimal for $t \in T$ generic, and $\dim Cb(\text{tp}(x/t)) = 2$ where x is a generic element of X_t for $t \in T$ generic. X, T, S may live in imaginary sorts. One might as well assume $S = M^2$.

Restricted trichotomy

Theorem (Rabinovich'91). Let K be an algebraically closed field. Consider the structure $M = (K, \ldots)$ where all basic predicates are definable in K and such that M is non locally modular. Then M interprets an algebraically closed field.

A posteriori, this field is (definably) isomorphic to K.

Conjecture (Zilber). Let Z be a definable set in K and let M be a strongly minimal non locally modular structure $M = (Z, \ldots)$ such that all basic predicates are definable subsets of Z. Then M interprets a field.

In a joint work with Assaf Hasson we settle this question when $\dim Z = 1$. Note that Rabinovich's theorem only settles it for $Z = \mathbb{A}^1$ (actually for Z rational curve, with a bit of work). It makes no difference (and is convenient for geometric applications) to consider an algebraic variety Z instead, with basic relations definable in the full Zariski language on Z (closed subsets of Cartesian powers Z^n).

Slopes

From now on we use M to denote a curve over an algebraically closed field k, and X to denote a pseudoplane $X \subset M^2 \times T$. We will use the same letter to denote the reduct.

If $M = \mathbb{A}^1$ and $Z \subset M^2$ is a curve defined by an equation $y = f(x)$ with $f(0) = 0$ then the (first order) slope of Z at $(0,0)$ is defined to be $f'(0)$. If Z is defined by $h(x,y) = 0$ then the slope at $(0,0)$ is defined to be $\frac{\frac{dh}{dx}(0,0)}{\frac{dh}{dy}(0,0)}$ (provided that the denominator is non-zero).

If we worked analytically then for M arbitrary, a curve $Z \subset M^2$ and a smooth $Q \in Z$ we could have chosen an isomorphism of a neighbourhood of Q in M^2 with a neighbourhood of $(0,0)$ in $\mathbb{A}^2$ (this amounts to choosing local coordinates). For arbitrary base field k one works with formal neighbourhoods of points in M^2.

I would like to gloss over the formal definition of a slope here, mentioning only that higher-order slopes can be defined for arbitrary M and k, and Z étale over M with respect to projection on first coordinate (think truncated Taylor expansion of f in the first example), and that an n-th order slope naturally takes values in the ring of endomorphisms of $k[x]/(x^{n+1})$. In particular for $n = 1$ this ring is just the base field. We denote the n-th order slope of a curve Z at a point Q as $\tau_Q^{(n)}(Z)$.

Composition and addition

If we treat curves and more generally 1-dimensional definable sets $Z \subset M^2$ as multi-valued functions (correspondences) then it is natural to consider compositions. Given $Z_1, Z_2 \subset M^2$ define

$$Z_2 \circ Z_1 = \{(x, z) \mid (x, y) \in Z_1, (y, z) \in Z_2\}$$

Suppose $(Q_1, Q_2) \in Z_1$ and $(Q_2, Q_3) \in Z_2$ for some $Q_1, Q_2, Q_3 \in M$ then $(Q_1, Q_3) \in Z_2 \circ Z_1$.

Lemma. $\tau^{(n)}_{(Q_1,Q_3)}(Z_2 \circ Z_1) = \tau^{(n)}_{(Q_1,Q_2)}(Z_1) \circ \tau^{(n)}_{(Q_2,Q_3)}(Z_2)$ for all $n > 0$.

Suppose that M is an algebraic group. Then correspondences can be "added":

$$Z_1 + Z_2 = \{(x, y_1 * y_2) \mid (x, y_1) \in Z_1, (x, y_2) \in Z_2\}$$

where $*$ denotes the group law on M.

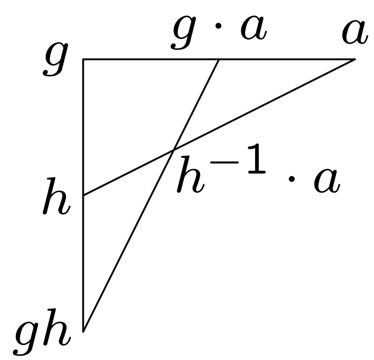
Lemma. $\tau^{(n)}_{(Q_1,Q_2+Q_3)}(Z_1 + Z_2) = \tau^{(n)}_{(Q_1,Q_2)}(Z_1) + \tau^{(n)}_{(Q_1,Q_3)}(Z_2)$ for all $n > 0$.

Neither of these operations are group laws for arbitrary correspondences, but there are natural "inverses".

Group configuration

Let G be a definable connected group of dimension n acting definably on a strongly minimal set. Let g, h be independent generic elements of G and let a be a generic element of A.

In the diagram



all vertices are pairwise independent, $\dim g = \dim h = \dim gh = n$, $\dim a = \dim g \cdot a = \dim h^{-1} \cdot a = 1$, all triples of tuples on the same line are of dimension $n + 1$, except for the vertical one: $\dim(\{g, h, gh\} = 2n$.

Theorem (Hrushovski). The vertices of a diagram of tuples satisfying the conditions mentioned above are inter-algebraic with the vertices of a diagram associated to a definable group action.

Finding enough slopes

A recurring step in applications of the group configuration theorem will be to find a point $Q \in M^2$ such that there are infinitely many distinct slopes of curves incident to Q.

Argument by contradiction: suppose there are only finitely many values a slope can take at each point $Q \in M^2$. Then for almost all $Q \in M^2$, formal Taylor expansions $f \in k[[x]]$ of any curve of the pseudoplane incident to Q must satisfy one of finitely many ODEs of the form

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

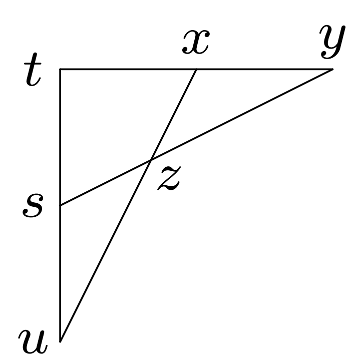
In characteristic 0, each such equation has a unique solution with zero constant term, therefore there are finitely many curves incident to a generic point in M^2. But in the pseudoplane there is a one-dimensional family of such curves, a contradiction. So there is a Q with the desired property, and one can modify the pseudoplane such that Q lies on the diagonal of $M^2 = M \times M$.

In characteristic p we might have curves like ones defined by an equation $y = x + (g(x))^p$ which have the same slope no matter what g is, so this argument doesn't work (more on it later).

One-dimensional group

We construct a one-dimensional group configuration under the assumption that for generic t, X_t is a pure-dimensional curve, i.e. has no 0-dimensional components (more on it later). Let Q be the point on the diagonal of M^2 such that incident curves have many slopes, as on the previous slide. Let T^Q be the definable set such that $Q \in X_t$ iff $t \in T^Q$. Let t, s, y be independent generic elements of T^Q. Let u, x, y be elements of T^Q such that

$$\begin{aligned}\tau_Q(X_u) &= \tau_Q(X_s)\tau_Q(X_t)\\ \tau_Q(X_x) &= \tau_Q(X_t)\tau_Q(X_y)\\ \tau_Q(X_z) &= \tau_Q(X_s)^{-1}\tau_Q(X_y)\end{aligned}$$



Lemma. In the reduct, u is algebraic over t, s; x is algebraic over t, y; z is algebraic over s, y; u is algebraic over x, z.

The main technical lemma

Let $Y \subset M^2 \times A, Z \subset M^2 \times B$ be some families of pure-dimensional curves flat over A, B respectively, and assume that generic curves Y_a, Z_b are incident to and intersect transversely at Q. Let N be the number of intersections $\#(Y_a \cap Z_b)$ without counting multiplicities for (a, b) independent and generic.

Lemma. For all $(a, b) \in A \times B$, if $\tau_Q^{(1)}(Y_a) = \tau_Q^{(1)}(Z_b)$ then $\#(Y_a \cap Z_b) < N$.

Outline of the proof: this statement is really about the family I of scheme-theoretic intersections of Y_a and Z_b. We restrict to $U \subset A \times B$ over which I is quasi-finite, and with enough assumptions we can show that I is flat over U. The basic situation is when it is also finite over U, otherwise reduce using Zariski Main Theorem. Then the number of intersections with multiplicities is constant, and the number of intersections is lower semicontinuous on U. Throw out the component of I corresponding to Q. The rest is still flat. Therefore, every time the number of reduced points in the fibre of I drops due to Y_a and Z_b becoming tangent at Q, it cannot be compensated by some other points becoming non-tangent, by lower semicontinuity.

Finding enough slopes, positive characteristic

There are two ways to deal with non-uniqueness of solutions to ODEs in positive characteristic: construct a better behaved pseudo-plane (I) or work with higher-order slopes (II).

I. Mimicking the char. 0 argument, one picks a point Q with infinitely many curves incident to it and having the following property. Consider Taylor expansion of all curves incident to Q in some local coordinate system. There is the smallest n such that the coefficient next to x^{p^n} in the Taylor expansion takes infinitely many values.

As one composes curves, truncated Taylor expansions compose. More remarkably, powers of Frobenius add up even if negative. So for example if the truncated Taylor expansion of X_t is of the form $(g(x))^{p^n}$ then $X_t^{-1} \circ X_t$ has the truncated Taylor expansion of the form $g^{-1}(g(x))$ where g^{-1} is the compositional inverse of g in the ring of endomorphisms of $k[x]/(x^{p^n+1})$.

II. Find a point Q such that the slopes of curves incident to Q almost coincide with a one-dimensional subgroup of $\mathrm{Aut}(k[x]/x^n)$ for some n (works in char. 0 as well). One might need to modify the pseudoplane by composing curves with their inverses.

Two-dimensional group

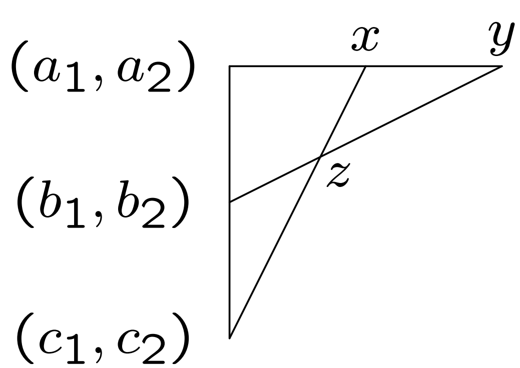
If M interprets a one-dimensional group, then the induced structure on this group is also non-locally modular.

Theorem (Marker-Pillay). Let $(\mathbb{C}, +, \ldots)$ be a non locally modular reduct of the field of complex numbers. Then it interprets an algebraically closed field.

We generalise this statement to an arbitrary field ($char > 0$ included) and arbitrary one-dimensional algebraic group.

Abusing notation slightly, the configuration must satisfy

$$\begin{aligned}
\tau(c_1) &= \tau(a_1)\tau(b_1) \\
\tau(c_2) &= \tau(a_1)\tau(b_2) + \tau(a_2) \\
\tau(x) &= \tau(a_1)\tau(y) + \tau(a_2) \\
\tau(z) &= \tau(b_1)^{-1}(\tau(y) - \tau(b_2))
\end{aligned}$$



(fine print: need to check that the group configuration corresponds to a faithful group action)

Last steps

Theorem (Cherlin, Hrushovski) Let G be a definable group of Morley rank 2 acting faithfully on a strongly minimal set A, then there exists a definable field structure on A and G is the group of affine transformations $\mathbb{G}_a(A) \rtimes \mathbb{G}_m(A)$ of the affine line over A.

Since in our case G and A are definable in an algebraically closest field, one can also come up with a direct proof of this statement.

I have glossed over the reduction to the pure-dimensional pseudoplane, this is the last and a non-trivial step of the proof.

Draft of the write-up of the proof is available from my webpage:
`http://www.ma.huji.ac.il/~sustretov/`

Prospects

- strongly minimal reducts of definable sets in ACVF (partial results due to Kowalski and Randriambololona)

- the methods should extend to higher-dimensional M

- applications along the lines of Bogomolov-Korotiaev-Tschinkel