Schanuel's Conjecture: Constructive Aspects

Angus Macintyre
a.macintyre@qmul.ac.uk

November 2016

Schanuel's Conjecture:Motivation and Formulation

The setting is the complex field $\mathbb{C}$, with central player the exponential function *exp*.

We all know the algebraic laws

1. $exp(0) = 1$
2. $exp(x + y) = exp(x).exp(y)$

and the less "algebraic"

1. $exp(\pi.i) = -1$.

What more do we know , of this kind?

Schanuel's Conjecture (*SC* for short) says that anything of this kind that is true follows from the preceding laws. It was formulated around 1960 by Steve Schanuel (1934-2014), in terms of two familiar notions of dependence between complex numbers. These notions are about dependence over the field $\mathbb{Q}$ of rational numbers.

1. Linear Independence over $\mathbb{Q}$, with associated notion of Linear Dimension $ldim_{\mathbb{Q}}$
2. Algebraic Independence over $\mathbb{Q}$, with associated notion of Transcendence Degree $td_{|Q}$

The first dimension is at least as big as the second.

The Conjecture says:

1. Let $\lambda_1, ...\lambda_n$ be complex numbers. Then

$$td_{\mathbb{Q}}(\lambda_1, ...\lambda_n, exp(\lambda_1), ...exp(\lambda_n)) \geq ldim_{\mathbb{Q}}(\lambda_1, ..., \lambda_n)$$

Recall that $\mathbb{Q}$ -linear relations translate into multiplicative relations between the corresponding exponentials (as we all know from working with roots of unity), and SC somehow says that this is the only way that we can create algebraic relations between exponentials, except for the use of Euler's identity.

Explanatory Power

1. e is transcendental. For take $n = 1$, $\lambda_1 = 1$. RHS is 1, and 1 contributes nothing to transcendence degree.
2. . Of course the previous result is proved unconditionally, but this one is not.Namely, e^e is transcendental.. For take $n = 2$, $\lambda_1 = 1$ and $\lambda_2 = e$. Then RHS is 2, but LHS involves e twice,as well as 1 so in fact we get that e and e^e are algebraically independent.
3. . π is transcendental. Best to prove $i.\pi$ transcendental. Take $n = 1$, and $\lambda_1 = i.\pi$. The RHS is 1, and LHS has a -1 from Euler,as well as π.
4. . Of course the previous result is proved unconditionally., but this one is not.Namely, π and e are algebraically independent.Take $n = 2$, $\lambda_1 = i.\pi$ and $\lambda_2 = 1$. The RHS is 2, since π is real, whereas LHS has $-$ by Euler, and 1 , so get algebraic independence of $i.\pi$ and e.

Unconditional results "provable" easily from SC

1. Hermite-Lindemann. Arbitrary n but the λ assumed algebraic.
2. $n = 1$, Gelfond-Schneider, transcendence of $exp(z)$ where z is $\beta.log(\alpha)$, with α an algberaic number distinct from 0 and 1, and β is an irrational algebraic number.
3. Baker's work on algebraic independence of logarithms of algebraic numbers .
4. . Nesterenko's result that π and $exp(\pi)$ are algebraically independent.

How hidden might a counterexample be?

It should be made clear that the evidence for SC is not great. The beauty of the conjecture is indisputable. One should note, too, that there are no examples in mathematical history where a number expected to be transcendental turns out not to be (though there are intriguing results in "Periods" by Konsevich and Zagier).

The numbers listed so far in this talk are very explicit,and in particular are all computable complex numbers. Thus the following Theorem is rather surprising.

Theorem

If there is a counterexample to SC, there is one in which the λ are computable.

This was proved by me in 2012, and a proof can be found in a long paper entitled "Turing meets Schanuel" in Proceedings of Manchester ASL Meeting 2012.

Exponential Algebra

Model theorists have been heavily involved for well over 25 years in the definability -theoretic content of SC where the quantification is over arbitrary complex numbers and not just over some fairly "explicit " arithmetical numbers. In particular they have been led to a systematic study of exponential fields, and the correct definition of exponential dependence (and thus of exponential-algebraic numbers).
One begins with some abstract algebra, of $E - rings$, that is, commutative unital rings R equipped with a map E from R to R satisfying $E(0) = 1$ and $E(x + y) = E(x).E(y)$.

Free Structures

These form an equational class, with classic examples the real and complex exponentials. There exist free $E-$*rings* on any set X. and indeed free $E-$*rings* in X over any $E-$*ring*. This is the analogy with ordinary algebra, but it does not help very much . The iteration of E causes much complication.It turns out that the free objects are best construed as iterated group algebras, and in this way considerable progress has been made. The free $E-$*rings* satisfy SC, and the free $E-$*rings* over $E-$*rings* satisfying SC also satisfy SC.Note that if this were not so over $\mathbb{R}$ or $\mathbb{C}$ then SC would obviously be false.

E-polynomials

One could define these in the usual boring syntactical way, but having the apparatus of free $E-$ *rings* we define them as elements of the free object over our given E-ring. But we sometimes pretend we are using syntactic definition. One has immediately issues

about zeros, say in $\mathbb{C}$ or $\mathbb{R}$ about such polynomials , even in one variable. In $\mathbb{R}$ they have only finitely many zeros , as Hardy proved. In $\mathbb{C}$ even the simplest may have infinitely many zeros, e.g

$f(z) = \sum \lambda_i E(\mu_i z)$ where the λ_i and μ_i are in $\mathbb{C}$ and the μ_i are distinct, and there are at least two μ_i.
Note too that

$E(z) = z$ has infinitely many zeros in $\mathbb{C}$ (did you all know this?).

Systems and Families of Systems

The basic objects of study, over an E-field $\mathbb{K}$, are finite systems

$$F_1(\bar{x}_1, ..., \bar{x}_n, E(\bar{x}_1), ..., E(\bar{x}_n), \tilde{w}_1, .., \tilde{w}_m) = 0,$$

$$...$$

$$F_k(\bar{x}_1, ..., \bar{x}_n, , E(\bar{x}_1), ..., E(\bar{x}_n), .., \tilde{w}_1, ..., \tilde{w}_m) = 0,$$

where each $F_j(\bar{X}, \bar{Y}, \tilde{W})$ is a polynomial over $\mathbb{Q}$. There is no gain in generality in allowing inequations as well.
Note that iterated exponentiation is avoided, at the cost (potentially very great!) of moving into higher dimensions.

The variables are of two kinds. The $\tilde{w}$'s are parameters, to be replaced by values $\tilde{a}$, thus yielding a system of equations over K in the unknown $\bar{X}$'s. The resulting system is written $\Sigma(\bar{X}, \tilde{a})$.
As $\tilde{a}$ varies we get a family of systems.

Hovanski Systems

A family of systems (as described earlier) gives a **Hovanski system** if there are exactly n equations, where n is the length of the tuple $\bar{X}$, and we add the requirement that the $\bar{X}$-solution satisfies the extra condition (an inequation) that the formal Jacobian of the system with respect to $\bar{X}$ be nonzero. That is :

$$F_1(\bar{x}_1, ..., \bar{x}_n, E(\bar{x}_1), ..., E(\bar{x}_n), \tilde{w}_1, .., \tilde{w}_m) = 0,$$

$$...$$

$$F_n(\bar{x}_1, ..., \bar{x}_n, E(\bar{x}_1), ..., E(\bar{x}_n), \tilde{w}_1, .., \tilde{w}_m) = 0,$$

$$Jacobian_{\bar{X}} \neq 0.$$

Note that there is an obvious natural algebraic notion of formal derivative of an E-polynomial with respect to a variable, inducing a formal definition of Jacobian.

E-algebraic, E-closure

This definition is given for any E-field of characteristic 0.
An element t is E-algebraic over a set A if there is a Hovanski system $\Sigma(\bar{X}, \bar{Y}, \tilde{W})$ over $\mathbb{Q}$, and elements $\tilde{a}$ from A and a solution $\bar{x}$ of $\Sigma(\bar{X}, \bar{Y}, \tilde{a})$, so that t is the first entry of $\bar{x}$.

(NOTE that we impose no bound on the length of $\bar{X}$,and allow $\tilde{W}$ to be absent.)

FACT: E-algebraic is a dependence relation, and the E-closure of A (the set of elements E-algebraic over A) is an E-subfield.

E-algebraic, E-closure - Substantial results

1. (Hovanski 1980) In the real case the set of solutions of a Hovanski system is **finite**, with a cardinality bound depending only on the family of systems.(Use of Morse Theory).
2. (Macintyre-Wilkie). If Schanuel's Conjecture (see below), henceforward SC, holds in the complexes, π is not E-algebraic over the empty set in the reals. But if $\frac{\pi}{e}$ is rational, π is E-algebraic over the empty set in the reals.
   But, easily,
3. π is E- algebraic over the empty set in the complexes.
   (*Proof*: exercise).
4. The E-closure of a countable set is countable in the complexes, by elementary differential topology (solutions are isolated).

Dimension

From the dependence relation , which is easily seen to satisfy the Exchange Axiom, one gets a notion of E-dimension (either absolute, or relative), analogous to the algebraic-geometric one. (Note that for algebraically closed fields of characteristic 0 and polynomials not containing E, the definition we gave is equivalent to the usual algebraic-geometric one). Zilber started from a different notion of dimension, which turns out (Kirby, Macintyre, Wilkie) to be equivalent to the above in Zilber's setting. Zilber's notion is based on deep general ideas of Hrushovski.

Apparent Inadequacy of a Naive Definition

Why not define $E - \textit{algebraic}$ in terms of the vanishing of a single $E - \textit{polynomial}$ in one variable? Because we can't prove anything about it, and the above definition, if specialized to ordinary polynomials, gives the classical definition in characteristic zero.

Sketch of Proof of Main Result

Jonathan Kirby proved the nice result that SC holds in $\mathbb{C}$ if and only if SC holds in the E-closure of the empty set. I showed in "Turing Meets Schanuel" that every number in the E- closure of the empty set is computable (the proof is not "uniform"). An interesting consequence I drew is that although SC appears to involve nonarithmetic quantification, it is in fact equivalent to an arithmetical statement. The exact syntactic complexity of such a statement is under investigation by me, van den Dries and Marker. The best known so far is a Π^0_4 definition. We have hopes of removing one quantifier block, but getting down to purely universal would be dramatic indeed. This would say that there is one polynomial over the integers such that SC is equivalent to the unsolvability of that polynomial!

Some great conjectures are naturally equivalent to unsolvability statements

One should not overdramatize. Kreisel (following earlier work of Turing) showed that the Riemann Hypothesis is equivalent to such an unsolvability statement (strictly speaking one had to wait for Matejasevic's resul of 1970 giving unsolvability of Hilbert's Tenth Problem, but the essential work on complex approximations was done by Kreisel around 1950). More recently I showed that the Modularity Conjecture for elliptic curves over $\mathbb{Q}$ (from which Fermat's Last Theorem follows) is also equivalent to such an unsolvablity statement.

Uniformity in Real Case

Kirby and Zilber showed a very strong unconditional result (with a rather easy proof) for the real case, using cell-decomposition in o-minimality. Namely

Theorem

If SC holds in $\mathbb{R}$ then there is a computable function which to each variety V over $\mathbb{Q}$ of dimension less than n in $2n$ variables $z_1, ...z_n, w_1, ..w_n$ provides an integer M so that for any REAL numbers $a_1, ...a_n$ such that $(a_1, ..a_n, exp(a_1), ..exp(a_n))$ is in V then here is a nontrivial linear relation over $\mathbb{Z}$ in the $a_1, ..a_n$ with coefficients of absolute value bounded by M.

No such result is known for the complex exponential. Notice a subtlety. It is not immediate to deduce the real version of the Main Result from the complex version. But the Kirby-Zilber result , together with classical results about 0-minimality, does enable one to prove that the real version holds.