Proving an Execution of an Algorithm Correct?

James Davenport
masjhd@bath.ac.uk

University of Bath

16 February 2023

SAT solving

The quintessenial NP-complete problem: Given a Boolean statement $\Phi(x_1, \ldots, x_n)$ produce

either $f : \{x_i\} \mapsto \{T, F\}$ such that $\Phi(f(x_1), \ldots, f(x_n)) = T$ (a satisfying assignment)
$\perp$ indicating that no satisfying assignment exists.

The first can be verified easily enough: what about the second? Since at least 2016, contestants in the annual SAT contests have been required to produce proofs (occasionally > 100GiB!) in DRAT format, which can be checked (Marijn says there are subtleties to "easy" checking).

Integration

P is algebra professor, S is awkward student

- P e^{-x^2} has no integral.
- S But in analysis the professor proved that every continuous function has an integral.
- P I meant that there was no formula for the integral.
- S But in statistics the professor used $\mathrm{erf}(x)$ and everything seemed OK.
- P I meant that there was no *elementary* formula, in terms of exp, log and the solution of polynomial equations.
- S How do you prove that?
- P Differential Algebra!
- S What's that?
- P A field K equipped with $' : K \to K$ such that $(a+b)' = a' + b'$ and $(ab)' = a'b + ab'$.

Algebraic Theory of Integration [Rit48, Rit50]

Given $f \in K = \mathbf{Q}(x, \theta_1, \ldots, \theta_n)$ where $x' = 1$ and each θ_i is elementary over $\mathbf{Q}(x, \theta_1, \ldots, \theta_{i-1})$ (need *decidable* [Ric68]) produce

either F in some elementary extension L of K such that $F' = f$ (an elementary integral)

or $\perp$ indicating that no such elementary integral exists.

The first can be verified: what about the second?

The verification isn't necessarily trivial: there are issues of simplification of elementary functions.

Because of branch cuts, F might not denote a continuous function $\mathbf{R} \to \mathbf{R}$, despite the student's memory of analysis [CDJW00].

The Heaviside function differentiates to 0, so it's a "constant" in terms of differentiable algebra.

Liouville's Principle [Lio35, Rit50]

Looking for any elementary might seem like "needle in a haystack".

Theorem (Liouville's Principle)

Let f be a expression from some expression field K. If f has an elementary integral over K, it has an integral of the following form:

$$\int f = v_0 + \sum_{i=1}^{n} c_i \log v_i, \tag{1}$$

where v_0 belongs to K, the v_i belong to $\hat{K}$, an extension of K by a finite number of constants algebraic over $\mathrm{const}\, K$, and the c_i belong to $\hat{K}$ and are constant.

Alternatively

$$f = v_0' + \sum_{i=1}^{n} c_i \frac{v_i'}{v_i}. \tag{2}$$

Only a single bale of hay! Proof by equating coefficients in $f = F'$.

Risch's idea [Ris69]

$f, g \in \overline{\mathbf{Q}}(x, \theta_1, \ldots, \theta_n)$ where each θ_i is either

logarithmic $\theta_i' = \frac{u_i'}{u_i}$, $u_i \in \overline{\mathbf{Q}}(x, \theta_1, \ldots, \theta_{i-1})$.

exponential $\theta_i' = u_i'\theta_i$, $u_i \in \overline{\mathbf{Q}}(x, \theta_1, \ldots, \theta_{i-1})$.

Induct on n, that we can

$\int$ Solve (or $\perp$) $f = v_0' + \sum_{i=1}^n c_i \frac{v_i'}{v_i}$

Risch o.d.e. Solve (or $\perp$) $y' + fy = g$ for $y \in \overline{\mathbf{Q}}(x, \theta_1, \ldots, \theta_n)$.

In both cases, the algorithm is a fairly messy "comparison of terms" argument, and the Risch o.d.e. for exponential θ_n was a "similarly", which wasn't quite [Dav86].

The "mess" comes in showing that every case is covered, and that the "bug fix" in [Dav86] is complete: each individual case is fairly straightforward.

Producing a proof of $\perp$

1. Have a formal proof of Liouville's Principle.

   I haven't done this formally, but it doesn't look outrageous: it's all algebra in [Rit48].

2. At each comparison of terms, spit this out in a form that a theorem-prover can digest.

   Again, I haven't done this, but I did have an implementation in Axiom which produced a (very stylised) informal proof.

Note that I am *not* considering the case of θ_i algebraic. θ_1 algebraic is in [Dav81], but there is much more mathematics involved in finding the c_i, v_i or proving they don't exist. More general is in [Bro90, Bro91], again more mathematics.
"Mathematics" *may* reduce to "is a divisor on an elliptic curve a torsion divisor", and $\perp$ here is hard.

Thanks to this conference, I knew I should talk to Anne Baanen.

And now done, but we should keep talking.

Real Quantifier Elimination [Tar51, Sei54]

Let each Q_i be one of the quantifiers $\forall, \exists$. Real Quantifier Elimination problem is the following: given a statement

$$\Phi_0 := Q_1 x_{1,1}, \ldots, x_{1,k_1} \cdots Q_{a+1} x_{a+1,1}, \ldots, x_{a+1,k_{a+1}} \Phi(y_i, x_{i,j}), \quad (3)$$

where Φ is a Boolean combination of equalities and inequalities between real polynomials $P_\alpha(y_i, x_{i,j})$, produce a Boolean combination Ψ of equalities and inequalities between polynomials $Q_\beta(y_i)$ which is equisatisfiable, i.e. Ψ is true if and only Φ_0 is true. If all the polynomials $Q_\beta(y_i)$ in $\Psi(y_i)$ have integer coefficients, we call $\Psi(y_i)$ a Tarski formula.

- Proved decidable in 1950s
- First feasible solution by [Col75] through Cylindrical Algebraic Decomposition

Cylindrical Algebraic Decomposition [Col75]

Fix coordinates in $\mathbf{R}^n$ consistent with quantifier order.
Given a set of polynomials $\{p_\alpha\}$ in $\overline{Q}[x_1,\ldots,x_n]$, produce a finite set of cells $C_i \subset \mathbf{R}^n$ which is:

- **Cylindrical** $\forall i,j,k \operatorname{Proj}_{\mathbf{R}^k}(C_i), \operatorname{Proj}_{\mathbf{R}^k}(C_j)$ are equal or disjoint;
- **Algebraic** Defined by polynomials in $\overline{Q}[x_1,\ldots,x_n]$;
- **Decomposition** disjoint and cover $\mathbf{R}^n$;
- **Sampled** each cell has a sample point s_i (cylindrical);

such that on each cell every p_α is sign-invariant $(+,-,0)$.
Then the truth of Φ is invariant on a cell, and we can write down Ψ as the union of those cells where Φ_0 is true at the sample point.
Unfortunately QE is doubly exponential in n [DH88], so CAD's worst case must be, and in practice CAD nearly always is.

Challenges with Cylindrical Algebraic Decomposition

- CAD doesn't care about the quantifiers (other than variable order), in particular $\exists x_1, \ldots, x_n \Phi$ (the SAT problem) isn't treated as a special case.
- As formulated, it doesn't care about the Boolean structure of Φ.

$\surd$ When it's $(p_1 = 0) \wedge \Phi'$ we can do better [McC99].

$\surd$ Even if this is only part of Φ, we can use an equality [EBD15].

- If f, g, h have degree d, $\mathrm{res}_y(\mathrm{res}_z(f, g), \mathrm{res}_z(f, h))$ has degree $O(d^4)$, even though there are only $O(d^3)$ common solutions $f(x, y, z) = g(x, y, z) = h(x, y, z)$.

! $f(x, y, z_1) = g(x, y, z_1)$; $f(x, y, z_2) = h(x, y, z_2)$. Note that these points *are* relevant for cylindricity in the worst case, and are used in [DH88].

- Major improvements to CAD import more mathematics, up to "Puiseux with parameters" [MPP19].
- Despite attempts [CM10], there is no formal proof of correctness of even basic Collins.

Cylindrical Algebraic Coverings I [ADEK21]

For purely existential problems $\exists x_k, \ldots, x_n \Phi$.
$\sigma_{i,j} \in \{=, <, \leq, >, \geq\}$, but for exposition, assume all $\sigma_{i,j} \in \{<, >\}$.

1. $\Phi = (p_{1,1}\sigma_{1,1}0 \wedge \cdots) \vee (p_{2,1}\sigma_{2,1}0 \wedge \cdots) \vee \cdots$
2. Commute $\exists$ and $\vee$ and treat each disjunct Φ_i separately

So we don't care where $p_{1,1}$ and $p_{2,1}$ meet. Doesn't change asymptotics, but may well be useful in practice.

3. Choose a sample point $(s_1, \ldots, s_n^{(1)})$.
4. If this satisfies Φ_i return SAT (and witness)
5. Otherwise $\exists j : p_{i,j}(s_1, \ldots, s_n^{(1)}) \not\sigma_{i,j}0$. Remember j with $(s_1, \ldots, s_n^{(1)})$.
6. Compute largest interval $I_{n,1} = (l, u)$ such that $\forall x_n \in (l, u) p_{i,j}(s_1, \ldots, x_n) \not\sigma_{i,j}0$.
7. If $I_{n,1} \neq \mathbf{R}$ choose $s_n^{(2)} \notin I_1$. If $(s_1, \ldots, s_n^{(2)})$ satisfies Φ_i return SAT (and witness).
8. Repeat steps 5–7 until $(s_1, \ldots, s_{n-1}, \mathbf{R})$ is covered.

* Some intervals might be redundant, so prune

9. Each of $I_{n,i}$ defines an oval in $(s_1,\ldots,s_{n-2},x,y)$ space which cover $(s_1,\ldots,s_{n-1},\mathbf{R})$.
10. Compute largest interval $I_{n-1,1}=(l,u)$ such that $\forall x_{n-1}\in(l,u)$ the $I_{n,i}$ cover $(s_1,\ldots,s_{n-2},x_{n-1},\mathbf{R})$.
11. If $I_{n-1,1}\neq\mathbf{R}$ choose a different value of $s_{n-1}, \notin I_{n-1,1}$.
12. Repeat steps 4–11 until $(s_1,\ldots,s_{n-2},\mathbf{R})$ is covered.
13. Repeat, decreasing the dimension, until we're covered the whole of the x_1-axis (or we get SAT).

Termination isn't entirely obvious, but each cell we compute contains at least one cell (the cell its sample point is in) from a CAD for the same polynomials, and the CAD itself is finite.

How might these be verifiable?

This is still work in progress, and there is more than one option

A. Verifying each (non-redundant) calculation in reverse

1. For each $I^{(1)} = (l_1, r_1)$ as an interval of $\mathbf{R}^1$ prove that it's covered because
2. For each $I^{(2)} = (l_2, r_2)$ covering the cylinder above $I^{(1)}$ prove that $I^{(1)} \times I^{(2)}$ is covered because
3. ...
4. For each $I^{(n)} = (l_n, r_n)$ covering the cylinder above $I^{(1)} \times I^{(2)} \times \cdots$ prove that $I^{(1)} \times I^{(2)} \times \cdots \times I^{(n)}$ is covered by the p_j we remembered for that sample point.

B Reverse-engineering a rough "CAD".

1. For each sample point $(s_1, \ldots, s_n)$ check that the corresponding cuboid $I^{(1)} \times I^{(2)} \times \cdots I^{(n)}$ is contained within the $p_j \not\sigma_j 0$ region.
2. Verify that these cuboids are arranged cylindrically, and are complete.

Need Resultants and inequalities, but no topology.

Thoughts

- UNSAT, or its equivalent, can be a bigger challenge than positive answers.
- Completeness proofs of algorithms can be challenging.
- But *in some cases*, we may not need the completeness proof.
- (At least not in all cases).
- This may require more book-keeping in the algorithm, to keep the "hints" that drove us this way.
- Possibly (e.g. algebraic integration) we may not be able to prove UNSAT in all circumstances.

? is this still valuable?

Bibliography I

E. Ábrahám, J.H. Davenport, M. England, and G. Kremer.
Deciding the Consistency of Non-Linear Real Arithmetic Constraints with a Conflict Driven Search Using Cylindrical Algebraic Coverings.
Journal of Logical and Algebraic Methods in Programming Article 100633, 119, 2021.

M. Bronstein.
Integration of elementary function.
J. Symbolic Comp., 9:117–173, 1990.

M. Bronstein.
The Algebraic Risch Differential Equation.
In *Proceedings ISSAC 91*, pages 241–246, 1991.

Bibliography II

R.M. Corless, J.H. Davenport, D.J. Jeffrey, and S.M. Watt.
According to Abramowitz and Stegun, or arccoth needn't be uncouth.
SIGSAM Bulletin 2, 34:58–65, 2000.

C. Cohen and A. Mahboubi.
A Formal Quantifier Elimination for Algebraically Closed Fields.
In S. Autexier *et al.*, editor, *Proceedings CICM 2010*, pages 189–203, 2010.

G.E. Collins.
Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition.
In *Proceedings 2nd. GI Conference Automata Theory & Formal Languages*, pages 134–183, 1975.

J.H. Davenport.
On the Integration of Algebraic Functions, volume 102 of *Springer Lecture Notes in Computer Science*.
Springer Berlin–Heidelberg–New York (Russian ed. MIR Moscow 1985), 1981.

J.H. Davenport.
On the Risch Differential Equation Problem.
SIAM J. Comp., 15:903–918, 1986.

J.H. Davenport and J. Heintz.
Real Quantifier Elimination is Doubly Exponential.
J. Symbolic Comp., 5:29–35, 1988.

Bibliography IV

M. England, R. Bradford, and J.H. Davenport.
Improving the Use of Equational Constraints in Cylindrical Algebraic Decomposition.
In D. Robertz, editor, *Proceedings ISSAC 2015*, pages 165–172, 2015.

J. Liouville.
Mémoire sur l'intégration d'une classe de fonctions transcendantes.
Crelle's J., 13:93–118, 1835.

S. McCallum.
On Projection in CAD-Based Quantifier Elimination with Equational Constraints.
In S. Dooley, editor, *Proceedings ISSAC '99*, pages 145–149, 1999.

Bibliography V

S. McCallum, A. Parusiński, and L. Paunescu.
Validity proof of Lazard's method for CAD construction.
J. Symbolic Comp., 92:52–69, 2019.

D. Richardson.
Some Unsolvable Problems Involving Elementary Functions of a Real Variable.
Journal of Symbolic Logic, 33:514–520, 1968.

R.H. Risch.
The Problem of Integration in Finite Terms.
Trans. A.M.S., 139:167–189, 1969.

J.F. Ritt.
Integration in Finite Terms: Liouville's Theory of Elementary Methods.
Columbia University Press, 1948.

Bibliography VI

J.F. Ritt.
Differential Algebra.
Colloquium Proceedings vol. XXXIII. American Mathematical Society, 1950.

A. Seidenberg.
A new decision method for elementary algebra.
Ann. Math., 60:365–374, 1954.

A. Tarski.
A Decision Method for Elementary Algebra and Geometry.
2nd ed., Univ. Cal. Press. Reprinted in *Quantifier Elimination and Cylindrical Algebraic Decomposition* (ed. B.F. Caviness & J.R. Johnson), Springer-Verlag, Wein-New York, 1998, pp. 24–84., 1951.