Proofs of transcendance

Sophie Bernard, Laurence Rideau, Pierre-Yves Strub
Yves Bertot

November 2015

Objectives

- Study the gap between practical mathematics and computer-verified reasoning
- Explore structures used in various areas of mathematics
- Explore interfaces between two domains
  - Algebra: polynomials
  - Analysis: exponentiation, integration, limits
- Extend proof systems and libraries
  - Extending in the direction of multi-variate polynomials
- A long studied theme around the π number
  - Machin-like formulas, Arithmetic-geometric means, spiggot

Context of work

- Subsets of complex numbers
- Polynomials in various rings
- Integration of functions with a real variable
- Multivariate polynomials
- A proof plan provided by Niven (1939)

Complex numbers

- A place where constructive mathematics take a turn
- Nijmegen experiment: C-CoRN, constructive presentation of analysis
  - No excluded middle
  - No discontinuity in functions
- Coq standard library: incursion of classical logic in type theory
  - Loose the property that proofs of existence are algorithms
  - Explore the consequences of the axioms defining real numbers
- Alternative take in Mathematical Components
  - A constructive study of real-closed fields and field extensions
  - `complex` is not a type but a type constructor

The main lemma of the proof

- If $T = c \times \prod_{i<n}(X - \alpha_i)$ has integer coefficients $(\alpha_i \neq 0)$
- And $k + \sum_{i<n} \gamma_i e^{\alpha_i} = 0$, with k, γ integers, $k \neq 0$
- Then, there exists a polynomial G with integer coefficients and degree np such that $c^{np} \sum_{i<n} \gamma_i G(\alpha_i)$ is not an integer

Using the main lemma for e

- Assume e is algebraic
  $k + \sum_{i<n} \gamma_i e^{\alpha_i} = 0$ with $\alpha_i = i + 1$
- $\prod_{i<n} (X - \alpha_i)$ trivially has integer coefficient
- For any G with integer coefficients,
  $\sum_{i<n} \gamma_i G(\alpha_i)$ is an integer, obviously.

Using the main lemma for π

- Assume $i\pi$ algebraic, a root of $c \times \prod_{i<n}(X - \beta_i)$
- Consider $\prod_{i<n}(1 + e^{\beta_i}) = 0$

  In fact $\sum_{f:\{1\cdots n\}\to\{0,1\}} e^{\sum_{1<n} f(i)\times\beta_i} = 0$
- The α_i will be the $\sum_{1<n} f(i) \times \beta_i \neq 0$ (n' such elements)
- $c^m \times \prod(X - \alpha_i)$ has integer coefficients by symmetry arguments
- $\gamma_i = 1$ so $c^{mn'p} \sum_i \gamma_i G(\alpha_i)$ is an integer by symmetry arguments

Symmetry arguments

- if $a_0 + a_1 X + \cdots a_n X^n = \prod_{i<n}(X - \alpha_i)$, the coefficients a_j are elementary symmetric multivariate polynomials in the α_i

$$a_j = (-1)^{n-j}\sigma_{n,j}\overline{\alpha} \qquad \sigma_{n,j} = \sum_{\substack{|h| = j \\ h \subset \{1 \dots n\}}} \prod_{i \in h} X_i$$

- Example: $(X - \alpha_1)(X - \alpha_2)(X - \alpha_3) =$
$-\alpha_1\alpha_2\alpha_3 + (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_2)X - (\alpha_1 + \alpha_2 + \alpha_3)X^2 + X^3$
- Elementary symmetric polynomials generate all symmetric polynomial expressions
example: $X_1^2 + X_2^2 + X_3^2 =$
$(X_1 + X_2 + X_3)^2 - 2(X_1X_2 + X_2X_3 + X_1X_3) = \sigma_{3,1}^2 - 2\sigma_{3,2}$

Proof of the main lemma

- $\int_0^1 \alpha e^{-\alpha x} P(\alpha x)\mathrm{d}x = \sum_{i=0}^{deg(P)} P^{(i)}(0) - e^{-\alpha} \sum_{i=0}^{deg(P)} P^{(i)}(\alpha)$
- Name $I_P(\alpha)$ the integral, $P_d = \sum_{i=0}^{deg(P)} P^{(i)}$
- consider $P = c^n X^{p-1} T^p$, roots of T have multiplicity p in P

$$c^{np} \sum -\gamma_i e^{\alpha_i} I_P(\alpha_i) = -c^{np} \sum \gamma_i e^{\alpha_i} P_d(0) + c^{np} \sum \gamma_i P_d(\alpha_i)$$

- as p grows, the left hand side can be shown to be smaller than $(p-1)!$

Decomposing the right hand side

- Use the hypothesis $k + \sum \gamma_i e^{\alpha_i} = 0$
- Use the fact that 0 is a root with multiplicity $(p-1)$ of P
- When $P \in \mathbb{Z}[X]$, $P^{(i)}$ has coefficients divisible by $i!$

$$-c^{np} \sum \gamma_i e^{\alpha_i} P_d(0) = kc^{np}(p-1)!\,T(0)^p + \sum_{i=p}^{deg(P)} P^{(i)}(0)$$

- If p is large enough, this number is a multiple of $(p-1)!$ but not of $p!$

Decomposing right hand side (second part)

- Use the fact that α_i are roots with multiplicity p of P

$$\sum \gamma_i P_d(\alpha_i) = \sum_i \gamma_i \sum_{j=p}^{deg(P)} P^{(j)}(\alpha_i)$$

- Then use the fact coefficients of $P^{(j)}$ are multiples of coefficients of P and $p!$ when $p \leq j$
- Exhibit $G = \displaystyle\sum_{j=p}^{deg(P)} \frac{P^{(j)}}{p!}$, G has integer coefficients
- if $c^{np} \displaystyle\sum_i \gamma_i G(\alpha_i)$ is an integer, then
  - the right hand side is a multiple of $(p-1)!$ and not of $p!$
  - it must be larger than $(p-1)!$, in contradiction with slide 10.

Difficulties in formalization effort

- Different definitions of complex numbers
  - Coquelicot and Math-Components each have their own hierarchy
- Exponentiation and powers
- products of sums, filters on lists
- The fundamental theorem of symmetric polynomials

Complex numbers

- Relying on the Coquelicot library
  - Coquelicot provides a 600 line-file with basic operations
  - $\mathbb{C}$ is defined as $\mathbb{R}^2$
  - Properties of field, complete normed module, with a notion of derivative
- Relying on Math-components library
  - First include R (from standard library) into math-comp. hierarchy
  - Use a type-constructor: build a new field from an existing one
  - Provides the fund. th. of alg. as soon as existing field is RCF
  - Reproduce mathematical hierarchy of Coquelicot on top of math-comp

Equipment for complex numbers

- Complex integers, Complex natural numbers `Cint`, `Cnat`
- Generic notion of ring predicate and associated theorems

```
rpred_sum
     : forall (V : zmodType) (S : predPredType V)
         (addS : addrPred S) (kS : keyed_pred addS)
         (I : Type) (r : seq I)
         (P : pred I) (F : I -> V),
       (forall i : I, P i -> F i \in S) ->
       \sum_(i <- r | P i) F i \in S
```

Exponential and power

- Important property is : $a^{(n+p)} = a^n * a^p$
- Different ways to define x^y depending on x positive or y integer or real
- real exponential: e^x defined using a power series
- complex exponential $e^{x+\mathrm{i}y} = e^x \times (\cos y + \mathrm{i} \sin y)$

Big operations with filters

- For π, transforming $\prod_{i<n} 1 + e^{\beta_i}$ into a sum of products of exponentials
- Example $(1 + e^{\beta_1})(1 + e^{\beta_2})(1 + e^{\beta_3})$ contains $e^{\beta_1} e^{\beta_3} = e^{\beta_1 + \beta_3}$
- Discard the sums that are zero
- Lemmas already covered in the library

```
bigA_distr_bigA :
forall R (zero one : R) (times : Monoid.mul_law zero)
        (plus : Monoid.add_law zero times) (I J : finType)
        (F : I -> J -> R),
  \big[times/one]_i \big[plus/zero]_j F i j =
  \big[plus/zero]_(f : {ffun I -> J})
     \big[times/one]_i F i (f i)
```

Fundamental theorem of symmetric polynomials

- Proved for any commutative ring by `P.-Y. Strub`
- Stronger statement than usually found in litterature: bounding degree
- Need one more refinement: preserve integer coefficients
- Rely on “morphism” between Complex numbers that are integers and integers

Symmetry arguments in more details

- We have $c \times \prod(X - \alpha_i) \in \mathbb{Z}[X]$, not $\prod(X - \alpha_i)$
- $\sigma_{n,m}(\overline{\alpha})$ is only guaranteed to be rational, not integer
  Similarly $\sum G(\alpha_i)$ is only guaranteed to be rational
- But G is obtained from $T = c \times \prod(X - \alpha_i)$ by
  - Choosing an arbitrary p prime with $|c|$, $|k|$, $|T(0)|$
  - Raising to the power p
  - Multiplying by X^{p-1}
  - Computing derivatives
- Solution: multiply T by a power of c so that $\sum G(\alpha_i)$ is an integer

Lessons

- One the coming challenges is to combine libraries
  - Math-components and Coquelicot are still very close in spirit
  - Research in refactoring tools is on-going
- Navigate between types and predicates
  - `Cint` being a “ring” predicate
- Difficulties in finding the right level of abstraction
  - Very context dependent: completeness of interfaces