Formalizing a Proof that e is Transcendental

Jesse Bingham
Intel Corporation, Hillsboro OR 97124, USA

We describe a HOL Light formalization of Hermite's proof that the base of the natural logarithm e is transcendental. This is the first time a proof of this fact has been formalized in a theorem prover.

1. INTRODUCTION

A transcendental number is one that is not the root of any non-zero polynomial having integer coefficients. It immediately follows that no rational number q is transcendental, since q can be written as a/b where a and b are integers, and thus q is a root of $bx - a$. Furthermore, the transcendentals are a *proper* subset of the irrationals, since for example the irrational $\sqrt{2}$ is a root of $x^2 - 2$.

The existence of transcendental numbers was first established by Liouville in 1844 [11] by exhibiting a transcendental continued fraction. A later and simpler proof for their existence is due to Cantor [2, 4], who used a straightforward counting argument to show that the non-transcendental (called *algebraic*) numbers are countable. The result then follows from the fact that the reals are uncountable. The first decimal number demonstrated to be transcendental $\sum_{n=1}^{\infty} 10^{-n!}$ has come to be known as *Liouville's constant.* Transcendental numbers play an important role in Mathematics historically; for examples the fact that π is transcendental was used in the proof of the impossibility of squaring the circle, and the 7th Hilbert problem pertains to transcendental numbers.

The first non-fabricated number proven to be transcendental was the base of the natural logarithm e, as established by Hermite in 1873 [9]. This paper describes a formalization of (a simplification of) Hermite's proof using the HOL Light theorem prover; this is the first time this theorem has been formalized.[1]

2. HOL LIGHT PRELIMINARIES

HOL Light (hereafter simply *HOL*) is an interactive theorem prover for classical higher order logic [8]. Though HOL traces its ancestral roots to formal verification of computer systems, it has extended its applicability into the realm of many areas of Mathematics. Wiedijk [15] provides a comprehensive comparison of doing Mathematics in HOL with many other theorem proving systems by considering proofs of the irrationality of $\sqrt{2}$. Currently, proofs of 76 of the 100 Mathematical theorems tracked by Wiedijk's website [16] have been formulated in HOL Light, more than any other theorem prover. These include a selection of well-known results from diverse fields such as Number Theory, Geometry, Logical Foundations, Computer Science, Analysis, and Combinatorics. For a recent example of an intricate proof in HOL see Harrison's formalization of Dirichlet's Theorem [7].

[1] The HOL Light proof script is available for download at `www.cs.ubc.ca/~jbingham/etrans.html`.

The logic used by HOL is called *simple type theory*, which was proposed by Church as a potential foundation for Mathematics [3]. Like most theorem proving systems, all proofs are ultimately performed by the computer according to a small set of primitive inference rules. A key innovation in HOL and related provers is the notion of a *tactic*, which allows the user to perform backwards reasoning in order to prove a conjecture. Though HOL includes decision procedures and semi-procedures for various fragments of its logic, much of the reasoning to prove deep mathematical results must ultimately be done manually. The manual reasoning manifests as a proof script written in HOL's meta language Ocaml, weaving together chains of forward inferences and backwards tactics. It is important to emphasize, however, that no matter how complex this code is, HOL ensures soundness – it is impossible to prove a theorem that is not true.

In HOL, formal mathematical expressions are called *terms*. HOL has a rich typing system and each term has a well-defined *type*, which for examples may be $\mathbb{B}$ (boolean), $\mathbb{N}$ (natural number), $\mathbb{R}$ (real number), T^* (finite list with elements having type T), or $T_1 \to T_2 \to \cdots \to T_k \to T$ (k-ary functions with arguments of types $T_1, T_2, \ldots, T_k$ that return type T). Terms of different types semantically denote distinct objects, an important implication being that e.g. 42 the natural is not equal to 42 the real. A function `&` is used to map from the former to the latter; i.e. the term `42` represents a natural while `&42` is a real.

Although a HOL term and all its sub-terms have types, often these types are left implicit since they can be inferred from context. For example the function `pow` has type $\mathbb{R} \to \mathbb{N} \to \mathbb{R}$, and raises the given real to the power of the given natural and returns the real result. We can infer that the term `z * (x pow n) + y` has type $\mathbb{R}$. Note that whereas traditional Mathematics notation usually indicates a function's arguments as a comma separated list wrapped in parenthesis, HOL uses neither the commas nor the parentheses (though parentheses are used to delimit sub-terms). So for example if f and h are respectively functions of two and three arguments, HOL expresses $h(w, f(x, y), z)$ as the term `h w (f x y) z`. Note, however, that HOL allows for selected functions to be written infix; in the example term above each of the functions `*`, `pow`, and `+` are displayed in this style.

It is important to mention HOL's treatment of *predicates*. Traditionally, a predicate P over a set X (also called a *relation* when X is a Cartesian product) is simply a subset of X, i.e. $P \subseteq X$. For instance, the predicate `prime` defines a subset of $\mathbb{N}$. Since the notion of a function is central in the HOL logic (and the notion of sub-set is not-so-central), HOL predicates are functions of the type $X \to \mathbb{B}$ with the obvious connection to the traditional predicate: the function yields true for $x \in X$ iff $x \in P$.

In this paper, we follow the formatting convention of Harrison, where HOL terms are placed in a box, and are typeset using fixed-font ASCII almost exactly as they appear on the computer screen, except the ASCII is augmented with a few logic symbols (∀, ∃, ∧, ⇒, λ, etc). Terms of boolean type that have been proven equivalent to the boolean constant TRUE are called *theorems* and are indicated by prefixing with the traditional turn-style notation `|-`, for example the HOL theorem that states that real multiplication (right) distributes over real addition is displayed as:

```
|- ∀ x y z. (x + y) * z = x * z + y * z
```

HOL has a sound mechanism for introducing definitions into its logic; the result of which is simply a theorem asserting the definition.[2] Hence there is no distinction between a definition and a theorem; both are indicated using `|-`. For example, the predicate `prime` is defined by the theorem

```
|- ∀ p. prime p ⇔ ¬(p = 1) ∧ (∀ x.  x divides p ⇒ x = 1 ∨ x = p)
```

This says that for all $p \in \mathbb{N}$, p is prime if and only if $p \neq 1$ and any x that divides p must be equal to either 1 or p.

Polynomials in HOL [5] are represented simply as lists of reals specifying the coefficients, with the head being the constant term, the second element being the coefficient of x, the third the coefficient of x^2, etc.[3] To evaluate a polynomial f at the point x one applies the fundamental function `poly`:

```
|- (poly [] x = &0) ∧
   (poly (CONS h t) x = h + x * poly t x)
```

Here `CONS` is the list constructor function of type $\mathbb{R} \to \mathbb{R}^* \to \mathbb{R}^*$ that pre-appends the real to the list-of-reals, yielding a new list, while `[]` is the empty list. Thus evaluating the empty polynomial is always 0 for any x, while a non-empty polynomial f is evaluated recursively by adding the constant term to x multiplied by the evaluation of the tail of f at x. Thus `poly` can be though of as characterizing Horner's Rule:

$$\sum_{i=0}^{n} c_i x^i \quad = \quad c_0 + x(c_1 + x(c_2 + \cdots + x(c_{n-1} + xc_n)\cdots))$$

Common operations one might apply to polynomials are defined to directly act on $\mathbb{R}^*$, for example polynomial addition `++` has type $\mathbb{R}^* \to \mathbb{R}^* \to \mathbb{R}^*$ and is defined recursively by

```
|- ([] ++ p2 = p2) ∧
   (p1 ++ [] = p1) ∧
   ((CONS h1 t1) ++ (CONS h2 t2) = CONS (h1 + h2) (t1 ++ t2))
```

Multiplying a polynomial by a real constant and by another polynomial, denoted `##` and `**` respectively, are defined similarly:

```
|- c ## [] = [] ∧ c ## CONS h t = CONS (c * h) (c ## t)
|- ([] ** l2 = []) ∧
   ((CONS h t) ** l2 =
       (if t = [] then h ## l2 else (h ## l2) ++ CONS (&0) (t ** l2)))
```

HOL definitions that involve iteration are most commonly expressed in the inductive style of the above definitions; the HOL system requires a proof that the induction is well-founded, although in many cases it can deduce this proof automatically.

[2] Soundness is ensured by in some cases demanding that before defining an object with a given property, one must supply a theorem stating that such an object exists.

[3] HOL lists are displayed with the head on the left, meaning that the coefficient order is reversed; e.g. the list `[&7; &0; -- &42; &1]` represents the polynomial $x^3 - 42x^2 + 7$.

Many of the polynomials we manipulate in our proof have integer coefficients. HOL uses the predicate `integer` over $\mathbb{R}$ to indicate if a real is an integer. Since polynomials are just lists of reals, we can assert that a polynomial f has integer coefficients by `ALL integer f`, where `ALL` is a list-theoretic operator that is true iff all elements of the given list satisfy the given predicate. In the coarse of this work, we found it necessary to prove many obvious theorems about how `integer` commutes with various polynomial operations, for examples:

```
|- ∀ f1 f2. (ALL integer f1) ∧ (ALL integer f2)
                ⇒ (ALL integer (f1 ** f2))
|- ∀ f. (ALL integer f) ⇒ (ALL integer (poly_diff f))
```

Here `poly_diff` performs differentiation on polynomials in the expected way.

Since a polynomial is any list of reals, polynomials can very well have trailing zeros, which means the degree is not necessarily one less than the length. HOL defines a function `degree` that is one less than the length of the polynomial after any such zeros are chopped off. It follows that `(LENGTH p) - 1` is guaranteed to be at least `degree p`. This fact is exploited in some of the summations in our proof; even though it is only necessary to sum up to the degree, it makes proofs simpler to have some summations go to `(LENGTH p) - 1` or simply `LENGTH p`; in such cases the theorems still hold since any additional terms are 0.

For specifying derivatives of functions of type $\mathbb{R} \to \mathbb{R}$, HOL defines a relation `diffl` $\subseteq (\mathbb{R} \to \mathbb{R}) \times \mathbb{R} \times \mathbb{R}$ [6]. Intuitively, $(f, a, x) \in$ `diffl` iff the function f *has* a derivative at x, and furthermore the derivative has value a. Basic calculus tells us that this holds iff

$$a \;=\; \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

after expanding the limit operator into its epsilon-delta definition, the definition in HOL becomes[4]

```
|- ∀ f x a.
     (f diffl a) x ⇔
     (∀ e. &0 < e
         ⇒ (∃ d. &0 < d ∧
               (∀ x'. &0 < abs x' ∧ abs x' < d
                   ⇒ abs ((f (x + x') - f x) / x' - a) < e)))
```

One of several equivalent ways to define the natural exponentiation function is via an infinite summation: $e^x \;=\; \sum_{n=0}^{\infty} x^n/n!$. In HOL this manifests as

```
|- ∀ x. exp x = suminf (λ n. inv (&(FACT n)) * x pow n)
```

Intuitively, `suminf` takes a function $g : \mathbb{N} \to \mathbb{R}$ and returns the infinite sum $g(0) + g(1) + g(2) + \cdots$, assuming it converges. Here g is the function that takes $n \in \mathbb{N}$ to the HOL term `inv (&(FACT n)) * x pow n`, where `inv` reciprocates a real number, `&` is the injection from $\mathbb{N}$ to $\mathbb{R}$, and `FACT` is the factorial function on $\mathbb{N}$. Note also that here we use λ-abstraction, which is a central notion in HOL; given a term

[4] HOL prints `diffl f a x` using an infix notation `(f diffl a) x`.

t of type T_1 and a variable v of type T_2, $\lambda v.t$ is a term of type $T_2 \to T_1$ representing the function that substitutes a value for v in t. Given the above definition of `exp`, the number of interest e itself is simply written by the HOL term `exp &1`.

The formalization of the transcendental predicate in HOL was done previously, since Harrison has done a HOL proof of Liouville's Theorem.
Noting that `poly p = poly []` is a way of asserting that p's coefficients are all 0, the following predicate definitions should be self-explanatory:

```
|- ∀ x. algebraic x ⇔
   (∃ p. ALL integer p ∧ ¬(poly p = poly []) ∧ poly p x = &0)
|- ∀ x. transcendental x ⇔ ¬algebraic x
```

3. THE PROOF

The proof was constructed following the informal proof at the PlanetMath website [1], which in turn follows a simplification of Hermite's proof [9] done by Hurwitz in 1893 [10].

We start by assuming that e is algebraic and hence there exists a polynomial with integer coefficients $c(x)$ such that $c(e) = 0$. A central operation on a polynomial $f(x)$ used by the proof is to take the sum of all derivatives, which we denote $\widehat{f}(x)$. From our assumption that e is algebraic and some lemmas about how $f(x)$ and $\widehat{f}(x)$ are related, a certain equation (†) is constructed. (†) involves the *assumed* polynomial $c(x)$, an *arbitrary* polynomial $f(x)$ (and the corresponding $\widehat{f}(x)$), and e itself. Next a particular choice of $f(x)$ called $g_{n,p}(x)$ is defined (4); $g_{n,p}(x)$ is parameterized by positives integer n and p. The proof reaches a contradiction by showing that if we set $n = deg(c)$ and select p to be a large enough prime (which is always possible thanks to the infitude of the primes), then taking $f = g_{n,p}$ in (†) yields a contradiction since the LHS is a non-zero integer whereas the RHS has absolute value less-than 1.

In Section 3.1 we make some definitions and give two preliminary lemmas. Next the key equation (†) is developed in Section 3.2. The contradictory properties involving the LHS and RHS of the key equation are respectively proven in Sections 3.3 and 3.4. These results are put together to prove e's transcendence in Section 3.5.

3.1 Preliminary Lemmas

For a polynomial $f(x)$, let $deg(f)$ denote the degree of f, and let $f^{(i)}(x)$ denote the ith derivative of $f(x)$. Let $\widehat{f}(x)$ denote the sum of derivatives (SOD) of $f(x)$, i.e.

$$\widehat{f}(x) \quad = \quad \sum_{i=0}^{deg(f)} f^{(i)}(x) \tag{1}$$

In HOL we define `SOD` as a function of type $\mathbb{R}^* \to \mathbb{R}^*$, building up the definition from that of iterated polynomial differentiation and `SODN`, which sums the first n derivatives. Note also that `SUC` is the successor function on $\mathbb{N}$.

```
|- ∀ f. (poly_diff_iter f 0 = f) ∧
        (poly_diff_iter f (SUC n) = poly_diff (poly_diff_iter f n))
|- ∀ f n. SODN = iterate poly_add (0..n) (λ i.poly_diff_iter f i)
|- ∀ f. SOD = SODN f (LENGTH f)
```

Let us define $\Phi(x) = e^{-x}\widehat{f}(x)$ and consider its derivative

$$\Phi'(x) \;=\; e^{-x}(\widehat{f'}(x) - \widehat{f}(x)) \;=\; -e^{-x}f(x) \tag{2}$$

In HOL, Φ is really a function of both the implicit polynomial f and the explicit real argument x and thus has type $\mathbb{R}^* \to \mathbb{R} \to \mathbb{R}$. We make the definition[5]

```
|- Phi f x = (exp (-- x)) * (poly (SOD f) x)
```

and prove (2), formulated in terms of the `diffl` predicate:

```
|- ∀ x f.( (Phi f) diffl (--(exp (--x)) * (poly f x)) ) x
```

We now apply the Mean Value Theorem (MVT) to the function Φ on the interval with end points 0 and x. Much to the author's delight, MVT comes pre-proven in the HOL Library:

```
|- ∀ f a b.
     a < b ∧
     (∀ x. a <= x ∧ x <= b ⇒ f contl x) ∧
     (∀ x. a < x ∧ x < b ⇒ f differentiable x)
     ⇒ ∃ l z.
          a < z ∧
          z < b ∧
          (f diffl l)(z) ∧
          (f(b) - f(a) = (b - a) * l)
```

Note that f ranges over *all* functions of type $\mathbb{R} \to \mathbb{R}$, hence the pre-conditions of continuity and differentiability on the interval of interest $[a, b]$. By applying MVT to Φ on the interval $[0, x]$, the informal proof asserts that there exists a real ξ such that $0 < \xi < x$ and

$$\Phi(x) - \Phi(0) \;=\; e^{-x}\widehat{f}(x) - \widehat{f}(0) \;=\; \Phi'(\xi)x \;=\; -e^{-\xi}f(\xi)x \tag{3}$$

Similar to Φ, ξ is implicitly dependent on both x and f, which means that in HOL ξ has type $\mathbb{R} \to \mathbb{R}^* \to \mathbb{R}$. Thus (3) becomes

```
|- ∀ x f. &0 < x
          ⇒ &0 < xi x f ∧
             xi x f < x ∧
             Phi f x - Phi f (&0) = x * --exp (--xi x f) * poly f (xi x f)
```

Noting that (3) implies $\widehat{f}(0) = e^{-x}\widehat{f}(x) + e^{-\xi}f(\xi)x$, we arrive at the following lemma about ξ.

Lemma 1. *For any $x > 0$, there exists $0 < \xi_x < x$ such that*

$$\widehat{f}(0)e^x = \widehat{f}(x) + xe^{x-\xi_x}f(\xi_x)$$

In HOL, the range constraint on ξ is woven into the definition of ξ given above, hence Lemma 1's manifestation does not mention this constraint explicitly

[5] Negation of a real number or integer in HOL is expressed using the unary operator `--`.

```
|- ∀ x f. &0 < x ⇒
            poly (SOD f) (&0) * exp x =
               poly (SOD f) x + x * exp (x - xi x f) * poly f (xi x f)
```

Considering the Taylor expansion of the polynomial f about the point $x = a$:

$$f(x) \quad = \quad \sum_{i=0}^{deg(f)} f^{(i)}(a)\frac{(x-a)^i}{i!}$$

Comparing with (1) we obtain:

Lemma 2. *The value $\widehat{f}(a)$ is obtained so that in the Taylor expansion of the polynomial $f(x)$ about the point a, the powers $x-a$, $(x-a)^2$, ..., $(x-a)^{deg(f)}$ are replaced respectively by the numbers* $1!, 2!, \ldots, deg(f)!$.

Formalizing Lemma 2 must be done somewhat indirectly. The lemma makes a claim about making appropriate substitutions for certain non-trivial sub-expressions of some formula (that is equal to $f(x)$) yielding a new formula with a known value (i.e. $\widehat{f}(a)$). As far as the author knows, it is impossible to directly define an operator in the HOL logic that describes this substitution. However, using λ-abstractions, one can in effect describe a substitution where the substitution target is simply a variable. We thus construct a HOL term τ that is the Taylor expansion of $f(x)$ about the point a, except $(x-a)^i$ is replaced by the term `s i`, where `s` is a free variable. In this light we formalize Lemma 2 as *two* HOL theorems; the first says roughly that substituting $(x-a)^i$ for `s` in τ is equal to $f(x)$, while the second states that substituting $i!$ for `s` in τ is equal to $\widehat{f}(a)$. These substitutions are simply formalized by applying the λ-abstraction $\lambda s.\tau$ to the terms to be substituted in. Recalling that in HOL $f(x)$ and $\widehat{f}(a)$ are respectively written `poly f x` and `poly (SOD f) a`, the two theorems are as follows.

```
|- ∀ f a x.
    poly f x =
    (λ s. psum (0,LENGTH f)
              (λ m. poly (poly_diff_iter f m) a / &(FACT m) * s m))
    (λ i. (x - a) pow i)
|- ∀ f x a.
    poly (SOD f) a =
    (λ s. psum (0,LENGTH f)
              (λ m. poly (poly_diff_iter f m) a / &(FACT m) * s m))
    (λ i. &(FACT i))
```

Both of these theorems have three lambda abstractions, only the third of which differs between them.

(1) `s` is the target of the substitution in τ, having type $\mathbb{N} \to \mathbb{R}$

(2) `m` has type $\mathbb{N}$ and is the abstraction that `psum` sums over

(3) `i` abstracts the respective expressions $(x-a)^i$ and $i!$ so they become functions as required by λ `s`

3.2 The Equation (†)

Let us make the supposition that e is algebraic. Then there exists integers $c_0, \ldots, c_n$ with $c_0 > 0$ such that

$$\sum_{i=0}^{n} c_i e^i \;=\; 0$$

Now let f be any polynomial, and let us multiply the above by $\widehat{f}(0)$

$$c_0\widehat{f}(0) + \sum_{i=1}^{n} c_i\widehat{f}(0)e^i \;=\; 0$$

By virtue of Lemma 1 we can rewrite this as

$$c_0\widehat{f}(0) + \sum_{i=1}^{n} c_i \left(\widehat{f}(i) + ie^{i-\xi_i} f(\xi_i)\right) \;=\; 0$$

Rearranging we obtain the key equation

$$\sum_{i=0}^{n} c_i\widehat{f}(i) \;=\; -\sum_{i=1}^{n} ic_ie^{i-\xi_i} f(\xi_i) \tag{†}$$

For readability and convenience, we have elected to define HOL constants corresponding to the LHS and RHS of (†). Of course since both sides depend on the polynomials c and f, these become arguments; note that extracting the ith element of a list (where the first element is the 0th) is done via the function `EL`:

```
|- LHS c f = sum (0..(PRE (LENGTH c)))
                 (λ i.(EL i c) * (poly (SOD f) (&i)))
|- RHS c f = -- sum (1..(PRE (LENGTH c)))
                    (λ i.  (&i)
                           * (EL i c)
                           * (exp ((&i) - (xi (&i) f)))
                           * (poly f (xi (&i) f))       )
```

Armed with these definitions we can more succinctly formalize the condition under which (†) holds, i.e. the assumption that e is *not* transcendental, which is hence added as an antecedent. Note also the existential and universal quantification, respectively, over the polynomials c and f.

```
|- ¬(transcendental (exp &1)) ⇒
         ∃ c. (ALL integer c) ∧
             ((LENGTH c) > 1) ∧
             ((EL 0 c) > &0) ∧
             (∀ f .((LHS c f) = (RHS c f)))
```

The proof proceeds by demonstrating that one may select a polynomial $f(x)$ such that the LHS of (†) is a non-zero integer whereas the RHS has absolute value strictly less than 1, which is contradictory. We will denote the particular choice of $f(x)$ by $g_{n,p}(x)$, which is defined by

$$g_{n,p}(x) \;=\; \frac{x^{p-1}}{(p-1)!}\left((x-1)(x-2)\cdots(x-n)\right)^p \tag{4}$$

Later n will be set to (an upper bound on) $deg(c)$, while p will be a prime number that is large enough to satisfy certain bounds. An important feature of the polynomial $g_{n,p}(x)$ is that it has a zero of order p at $x = 0$ and a zero of order p at each of $x = 1, \ldots, n$; also the derivatives have zeros at these points. The higher order of the latter zeros along with the primality of p are involved with showing that the LHS of (†) is non-zero [13].

The formal definition of $g_{n,p}$ in HOL is:

```
|- g n p = (&1/(&(FACT (p - 1)))) ##
           ((poly_exp [&0; &1] (p-1))
            ** (poly_exp (poly_mul_iter (λ i.[-- &i; &1]) n) p))
```

Note that x is absent from this definition because g has type $\mathbb{N} \rightarrow \mathbb{N} \rightarrow \mathbb{R}^*$, i.e. it maps to the *polynomial* represented by (4), not the evaluation of this polynomial at a point x. This definition involves the polynomial-level functions `##` and `**` discussed in Section 2, as well as functions for iterative polynomial multiplication and polynomial exponentiation, which have straightforward definitions. Also, note the polynomials x and $x - i$ are respectively represented by `[&0; &1]` and `[-- &i; &1]`
.

3.3 The LHS is a Non-zero Integer

The following lemma can be seen to be true by simple manipulation of (4):

Lemma 3. *There exists integers $A_{p-1}, A_p, A_{p+1} \ldots$ where $A_{p-1} = (-1)^{np}(n!)^p$ and*

$$g_{n,p}(x) \quad = \quad \frac{1}{(p-1)!}\left(A_{p-1}x^{p-1} + A_p x^p + A_{p+1}x^{p+1} + \cdots\right) \qquad (5)$$

In spite the conceptual simplicity, proving Lemma 3 in HOL turns out to be rather tedious. Nevertheless, we were able to establish:

```
|- ∀ n p.
      p > 0 ⇒ n > 0 ⇒
      ∃ As .
         ((g n p) = (&1/(&(FACT (p  - 1)))) ## As)
       ∧ (∀ i. i < (p-1) ⇒ (EL i As) = &0)
       ∧ ((EL (p-1) As) = ((-- &1) pow (n * p)) * ((&(FACT n)) pow p))
       ∧ (ALL integer As)
```

The above warrants some explanation. The sequence $A_{p-1}, A_p, \ldots$ is naturally formalized as a real list `As`. In HOL, extracting the ith element of a list (where the first element is the 0th) is done via the function `EL`. So that A_{p-1} is really the $(p-1)$th element, we conceptually pad `As` with $p - 1$ zeros at the beginning; the fact that the first $p-1$ entries are zeros is indicated by the fifth line of the theorem. Recalling that `##` multiplies a HOL polynomial by a real constant, it should be clear that the fourth line corresponds to (5). Lemma 3 includes the constraints that $A_{p-1} = (-1)^{np}(n!)^p$ and that the A_i are integers; these correspond to the final two lines respectively.

Observe[6] that (5) is essentially the Taylor expansion of $g_{n,p}(x)$ about the point $a = 0$. Hence we can apply Lemma 2 to (5) in order to establish a key fact about $\widehat{g_{n,p}}(0)$

$$\begin{aligned}\widehat{g_{n,p}}(0) &= \frac{1}{(p-1)!}\left(A_{p-1}(p-1)! + A_p p! + A_{p+1}(p+1)! + \cdots\right) \\ &= (n!)^p(-1)^{np} + pK_0\end{aligned}$$

for some integer K_0. The corresponding formalization has no surprises:

```
|- p > 1 ⇒ n > 0 ⇒
   ∃ K0. integer K0 ∧
         poly (SOD (g n p)) (&0)
              = &(FACT n) pow p * (-- &1) pow (n * p) + &p * K0
```

Now let us add the constraint that the prime p is strictly greater than n. Then $(n!)^p(-1)^{np}$ is not divisible by p, and it follows that $\widehat{g_{n,p}}(0)$ is a non-zero integer that is not divisible by p.

The only thing messy about formalizing this is that HOL understandably defines its `divides` predicate on the type $\mathbb{Z}$, so we must apply the mappings `&` : $\mathbb{N} \to \mathbb{Z}$ and `int_of_real` : $\mathbb{R} \to \mathbb{Z}$ to the terms we relate with `divides` (which are of type $\mathbb{N}$ and $\mathbb{R}$, respectively).

```
|- n > 0 ⇒ p > n ⇒ prime p ⇒
     (integer (poly (SOD (g n p)) (&0)))
   ∧ ¬((&p) divides (int_of_real (poly (SOD (g n p)) (&0))))
   ∧ ¬((poly (SOD (g n p)) (&0)) = &0)
```

We now do a similar analysis, but for $\widehat{g_{n,p}}(i)$ where $i \in \{1,,2,\ldots,n\}$. Let us Taylor-expand $g_{n,p}(x)$ about the point i.

$$g_{n,p}(x) = \frac{1}{(p-1)!}\left(B_p(x-i)^p + B_{p+1}(x-i)^{p+1} + \ldots\right)$$

where the B_i's are integers. Using Lemma 2 then gives the result

$$\widehat{g_{n,p}}(i) = \frac{1}{(p-1)!}\left(p!B_p + (p+1)!B_{p+1} + \cdots\right) = pK_i$$

for some integer K_i. We can conclude that $\widehat{g_{n,p}}(1), \widehat{g_{n,p}}(2), \ldots, \widehat{g_{n,p}}(n)$ are integers and are all divisible by p.

```
|- p > n ⇒ n > 0 ⇒
   ∀ v. (1 <= v ∧ v <= n) ⇒
         (integer (poly (SOD (g n p )) (&v)))
       ∧ ((&p) divides (int_of_real (poly (SOD (g n p )) (&v))))
```

Using the above two theorems about $\widehat{g_{n,p}}(0)$ and $\widehat{g_{n,p}}(i)$ for $1 \le i \le n$ we can infer that the LHS is an integer having the form $c_0\widehat{g_{n,p}}(0) + pK$ for some integer K, and that $\widehat{g_{n,p}}(0)$ is indivisible by p. Now if we assume that $p > |c_0|$ then also c_0

[6] The Taylor expansion of a polynomial about $a = 0$ is simply the polynomial itself.

is indivisible by p, and thus so too is $c_0\widehat{g_{n,p}}(0)$. This brings us to the result of this subsection about the LHS of (†) when we plug in $g_{n,p}$ for f.

LEMMA 4. *Let p be a prime such that $p > deg(c)$ and $p > |c_0|$. Then $\sum_{i=0}^{n} c_i\widehat{g_{n,p}}(i)$ is a non-zero integer.*

It turns out that without loss of generality we can assume $c_0 > 0$, hence we have added this antecedent and reduced $p > |c_0|$ to $p > c_0$ in the HOL's statement of Lemma 4.

```
|- n > 0 ⇒ p > n ⇒ prime p ⇒ &p > (EL 0 c) ⇒
   (EL 0 c) > (&0) ⇒ n = PRE (LENGTH (c)) ⇒ (ALL integer c) ⇒
   (integer (LHS c (g n p))) ∧ ¬((LHS c (g n p)) = &0)
```

3.4 The RHS has absolute value < 1

For this section we take n to be `PRE (LENGTH c)`, which is (an upper bound on) $deg(c)$. Assuming $0 < x < n$, the factors $x, x-1, \ldots, x-n$ in the definition of $g_{n,p}$ (4) all have absolute value less than n:

```
|- &0 < x ∧ x < &n
   ⇒ ∀ i. 0 <= i ∧ i <= n ⇒ abs(poly [-- &i; &1] x) <= &n)
```

and thus

$$|g_{n,p}(x)| \quad < \quad \frac{1}{(p-1)!}n^{p-1}(n^n)^p \tag{6}$$

```
|- p > 1 ⇒
   &0 < x ∧ x < &n ⇒
   (abs (poly (g n p) x)) <=
       (&1/(&(FACT (p - 1)))) * ((&n) pow (p - 1)) * ((&n pow n) pow p)
```

From Lemma 1 we have that $0 < \xi_i < n$ for each $1 \leq i \leq n$ and thus from (6) we find

$$|g_{n,p}(\xi_i)| \quad < \quad \frac{1}{(p-1)!}n^{p-1}(n^n)^p$$

Also since $0 < \xi_i < n$, we have that $e^{1-\xi_i} < e^n$ for all $1 \leq i \leq n$. Letting c_m be the greatest of $|c_0|, |c_1|, \ldots, |c_n|$, it follows that the RHS of (†) for $f = g_{n,p}$ has absolute value less than

$$\left(\sum_{i=1}^{n} i\right) c_m e^n \frac{1}{(p-1)!}n^{p-1}(n^n)^p \tag{7}$$

Using a HOL definition `max_abs` that picks out the maximum absolute value from a list of reals, we have the corresponding HOL theorem:

```
|- abs (RHS c (g (PRE (LENGTH c)) p)) <=
       (sum (1..PRE (LENGTH c)) &) *
       ( (max_abs c) *
         (exp (&(PRE (LENGTH c)))) *
         &1 / &(FACT (p - 1)) *
         &(PRE (LENGTH c)) pow (p - 1) *
         &(PRE (LENGTH c)) pow PRE (LENGTH c) pow p )
```

Proof Portion	Gzipped HOL/TeX
Lemma 1	3854/421 = 9.2
Lemma 2	2850/314 = 9.1
Equation (†)	3449/535 = 6.4
Definition of $g_{n,p}$	281/180 = 1.6
LHS (†)	16035/906 = 17.7
RHS (†)	4487/563 = 8.0
Finale	1467/331 = 4.4
all	32423/3250 = 10.0

Table I. The De Bruijn factor: the ratio of information content between HOL Light proof and PlanetMath LaTex source.

For fixed n, the the limit as $p \to \infty$ of (7) is 0, which brings us to the main result of this subsection.

Lemma 5. *There exists p_0 such that for all $p > p_0$ we have*

$$\left| -\sum_{i=1}^{n} ic_i e^{i-\xi_i} g_{n,p}(\xi_i) \right| \quad < \quad 1$$

In HOL, Lemma 5 is expressed

```
|- ∀ c. ∃ p0. ∀ p. p > p0 ⇒ abs (RHS c (g (PRE (LENGTH c)) p)) < &1
```

3.5 Finale

Outside of HOL, the informal proof is complete; clearly (†) along with Lemma 4, Lemma 5, and the infitude of the primes yield a contradiction, which arises from the supposition that e is algebraic. However HOL requires a bit of glue reasoning to get the final theorem. For instance, we had to prove that a real number that is nonzero and integral cannot have absolute value strictly less than 1:

```
|- ∀ x. ((integer x) ∧ ¬(x = &0)) ⇒ ¬(abs x < &1)
```

Also, HOL's library contains a theorem stating that there are infinite $p \in \mathbb{N}$ that are prime; but what we really need is this slightly different way of expressing the same result:

```
|- ∀ n. ∃ p. prime p ∧ p > n
```

which took a bit of work to prove. Regardless, the final goal was reached:

```
|- transcendental (exp (&1))
```

4. CONCLUSIONS

Wiedijk [14] has proposed a metric to estimate the ratio of the information content in formal vs. informal proofs. The idea is to compress the theorem prover proof script and the latex source of the informal proof; the ratio of the resulting file sizes gives some sense of the additional information (and hence human effort) involved in the formalization. This ratio, dubbed the *de Bruijn factor*, has been observed to often hover around 4, though in some cases it is as high as 9.8 for a part of a proof [7]. However, all known comparisons of this nature involve formal proofs done by very experienced theorem prover users, often the developers of the theorem prover itself. The present proof was the first substantial proof the author attempted in HOL light (or any theorem prover for that matter), and hence one expects higher factors.

Indeed, the de Bruijn factors for the present proof is 10.0; the factors for the various parts of our proof are given in Table I. Interestingly, before the definition of `poly_mul_iter` was added to the file that defines $g_{n,p}$, the ratio was incredibly close to 1 (181/180). In this case it appears that the effort involved in making a nontrivial *definition* (which involved no proof) is equivalent in the two domains.[7] After completing the proof and gaining a considerably deep "bag of tricks" for doing HOL light proofs, the author choose (rather arbitrarily) a theorem of LHS (†) (which has by far the highest de Bruijn factor) to re-prove. The new proof has a compressed file size that is a factor of 2.14 smaller than the original. If the same reduction was achievable for all of LHS (†), the factor for this part would become 8.3.

The author has little experience using any other theorem proving systems, especially for doing Mathematical proofs, hence we refrain from stating any comparisons. Generally we were quite pleased with HOL, but there was one notable frustration. Many terms in this work involved more than one of the types: naturals $\mathbb{N}$, integers $\mathbb{Z}$, and reals $\mathbb{R}$. Since HOL's default pretty printer suppresses type annotations, and common arithmetic functions like $+$ and $-$ are overloaded to work on all three types, there was often confusion about the typing of various subterms. Of course this is easily fixable if one installs their own pretty printer that always displays type annotations on variables of these types. A more fundamental issue is that one must apply mappings to go in between these three domains, which can be tedious. As a partial solution, the author wrote a conversion that takes a term over reals and returns a theorem stating that it is equivalent to an analogous term over integers, under the antecedent that all involved real variables `x` satisfy `integer x`.

Finally, we note that there exists a proof of the transcendence of π that is based on the machinery of Hermite's proof of the transcendence of e [12]. We are thus optimistic that much of the work of this paper can be leveraged to prove that π is transcendental in HOL.

Acknowledgments

We thank John Harrison for suggesting this problem, proving a HOL theorem needed for Lemma 5, and general supportiveness. We also acknowledge the PlanetMath website (where informal proof we followed was found) as a great resource, and especially for allowing one to download latex source, which the author exploited tremendously in writing this paper.

References

[1] PlanetMath online mathematics encyclopedia, e is transcendental. `http://planetmath.org/encyclopedia/EIsTranscendental2.html`, 2010. [Online; accessed Dec-2010].

[7] The definition of `poly_mul_iter` was added to that file since it was decided that definitions should be included in the first file that uses them.

[2] G. Cantor. Uber eine eigenschaft des inbegriffes aller reellen algebraischen zahlen. *J. Reine Angew. Math*, 77:258–262, 1874.

[3] A. Church. A formulation of the simple theory of types. *Journal of Symbolic Logic*, 5:56–68, 1940.

[4] R. Gray. Georg Cantor and transcendental numbers. *The American Mathematical Monthly*, 101:819–832, 1994.

[5] J. Harrison. Verifying the accuracy of polynomial approximations in HOL. In *Theorem Proving in Higher Order Logics: 10th International Conference (TPHOLs)*, pages 137–152, 1997.

[6] J. Harrison. *Theorem Proving with the Real Numbers*. Springer-Verlag, 1998.

[7] J. Harrison. A formalized proof of Dirichlet's theorem on primes in arithmetic progression. *Journal of Formalized Reasoning*, 2(1):63–83, 2009.

[8] J. Harrison. HOL Light: An overview. In *Proceedings of the 22nd International Conference on Theorem Proving in Higher Order Logics (TPHOLs)*, pages 60–66, 2009.

[9] C. Hermite. Sur la fonction exponentielle. *Comptes Rendus Acad. Sci. Paris*, 77:18–24, 1873. English translation: "On the exponential function".

[10] A. Hurwitz. Beweis der transzendenz der zahl e. *Math. Ann.*, 43:220–221, 1893.

[11] J. Liouville. Sur des classes trs tendues de quantits dont la valeur n'est ni algbrique, ni mme rductible des irrationnelles algbriques. *J. Math. Pures et Appl*, 18:883–885 and 910–911, 1844. English translation: "On a very wide classes of quantities of which the value is neither algebraic, nor even reducible with the irrational algebraics".

[12] I. Niven. The transcendence of π. *The American Mathematical Monthly*, 46(8):469–471, 1939.

[13] R. Tubbs. The transcendence of e and π. `http://euclid.colorado.edu/~tubbs/courses/Chapter%20Two.pdf`. Lecture notes, accessed Dec 2011.

[14] F. Wiedijk. The de bruijn factor. `http://www.cs.ru.nl/~freek/factor/`, 2000. Accessed July 2011.

[15] F. Wiedijk, editor. *The Seventeen Provers of the World*, volume 3600 of *Lecture Notes in Computer Science*. Springer, 2006.

[16] F. Wiedijk. Formalizing 100 theorems. `http://www.cs.ru.nl/~freek/100/`, 2011. Accessed Feb 2011.