Algebraic Simplification

Lecture 12

Simplification is fundamental to mathematics

Numerous calculations can be phrased as "simplify this command"

The notion, informally, is "find something equivalent but easier to comprehend or use."

Note the two informal portions of this:

EQUIVALENT

EASIER

References

J. Moses: Simplification, a guide for the Perplexed, *CACM* Aug 1971.

B. Buchberger, R. Loos, Algebraic Simplification in *Computer Algebra: Symbolic and Algebraic Computation*, (ed: Buchberger, Collins, Loos). Springer-Verlag p11-43. (142 refs)

Trying to be rigorous, let T be a class of expressions

We could define this by some grammar, e.g.

E → n | v

d → 1|2|3|4|5|6|7|8|9 ;;nonzero digit

n → d | 0 | dn

E → E+E | E*E | E^E | E-E| E/E | (E) | Σ E …

v → x | y | z ….

etc.

Define an equivalence relation on T, say ~

x+x ~ 2*x ;; functional equivalence

true ~ not(false) ;; logical constant equivalence

(consp a) ~ (equal a(cons (car a)(cdr a)))

etc etc etc

Define an ordering

$R \prec S$ if R is simpler than S.

For example, R is expressible in fewer symbols, or if it has the same number of symbols, is alphabetically lower.

Find an algorithm K

For every t in T, K(t) ~ t

that is, it maintains equivalence.

K(t) < t or K(t) = t

that is, running K either produces a simpler result or leaves t unchanged.

If you have a zero-equivalence algorithm Z

For every t in T, Z(t) returns true iff t~0

You can make a simplification algorithm if T allows for subtraction.

Enumerate all expressions e_1, e_2, ... in dictionary order up to t. The first one encountered such that $Z(e_i - t)$ tells us that e_i is the simplest expression for t.

This is a really bad algorithm. In addition to the obvious inefficiency, consider that integers need not be simplest "themselves". 2^20 vs 1048576. Which has fewer characters?

We'd prefer some kind of "canonicalization"

That is, K(t) has some kind of nice properties.

K(t)=0 if Z(t). That is, everything equivalent to zero simplifies to zero.

K(<polynomial>) is a polynomial in some standard form, e.g. expanded, terms sorted.

K(t) is usually small ... is a concise description of the expression t

(Maybe "smallest" ideal member)

We'd prefer some kind of valuation

That is, every expression in T can be evaluated at a point in n-space to get a real or complex number. Expressions equivalent to 0 will evaluate to 0.

Floating-point evaluation does not work perfectly: This may not be 0: 4 arctan(1)-π

Evaluation in a finite field has no roundoff BUT how does one evaluate sin(x), x 2 Z_p?

(W. Martin, G. Gonnet, Oldehoeft)

Sometimes simplest seems rather arbitrary

We generally agree that $\sum^{k}_{i=1} f(i) - \sum^{k}_{j=1} f(j) = 0$, assuming i, j do not occur "free" in f.

But what is the simplest form of the sum $\sum^{k}_{i=1} f(i)$? Do we use i, j, or some "simplest" index? And if both are simplest, why are they not identical?

The same problem occurs in integrals, functions (λ-bound parameters), logical statements $\forall x$ ... etc.

Sometimes we encounter an attempt to formalize the notion: "Regular" simplifiers

Consider rational expressions whose components are not indeterminates, but algebraically independent objects.

Easy to detect 0.

Not necessarily canonical:

y:= sqrt(x^2-1).. leave this alone or transform to w*z = sqrt(x-1)*sqrt(x+1) ?

(e.g. in Macsyma, ratsimp, radcan commands)

(studied by Caviness, Brown, Moses, Fateman)

What basis to use for expressing as polynomial sub-parts?

A similar problem is....

y:= sqrt(e^x-1).. leave this alone or transform to w*z =

sqrt($e^{x/2}$-1)*sqrt($e^{x/2}$+1)?

Consider integration of sqrt(e^x-1)/sqrt($e^{x/2}$-1), which is the same as integrating sqrt($e^{x/2}$+1). The latter is integrated by Macsyma to

4 * sqrt($e^{x/2}$ + 1) - 2 * log(sqrt($e^{x/2}$ + 1) + 1) + 2 * log(sqrt($e^{x/2}$ + 1) - 1)

Leads to studies of various cases

Algebraic extensions, minimal polynomials (classical algebra)

Radical expressions and nested radical simplifications (R. Zippel, S. Landau, D. Kozen)

Differential field simplification can get even more complicated than we have shown,

e.g. $\exp(1/(x^2-1)) / \exp(1/(x-1))$. This requires partial fraction expansion of exponents. And then what about $\exp(1/(\exp(x)-1))$?

Simplification subject to side conditions

f := $s^6+3c^2s^4+3c^4s^2+c^6$ with $s^2+c^2 = 1$. This should be reduced to 1, since it is $(s^2+c^2)^3$. (think of $\sin^2 x + \cos^2 x = 1$ with s=sin x c=cos x)

How to do this with

(a) many side conditions

(b) large expressions

(c) deterministically, converging

(d) expressions like $f+s^7$ which could be either $s^7 + 1$ or $(-c^6+3c^4-3c^2+1)s+1$ which is arguably of lower complexity (if s ?c)

Rationalizing the denominator

2/sqrt(2) -> sqrt(2), but

$1/(x^{1/2}+z^{1/4} + y^{1/3})$

"simplifies" to

$$(((z^{1/4})^3 + (- y^{1/3} - \mathrm{sqrt}(x))(z^{1/4})^2 + ((y^{1/3})^2 + 2\mathrm{sqrt}(x)y^{1/3} + x)z^{1/4} - y - 3\mathrm{sqrt}(x)\,(y^{1/3})^2 - 3xy^{1/3} - \mathrm{sqrt}(x)\,x) \;/\; (z + (- y^{1/3} - 4\mathrm{sqrt}(x))y - 6x(y^{1/3})^2 - \mathrm{sqrt}(x)xy^{1/3} - x^2))$$

Simplification subject to side conditions

Solved heuristically by division with remainder, substitutions

e.g. divide f by s^2+c^2-1:

$f = g*(s^2+c^2-1)+h = g*0+h = h.$

Solved definitively by Gröbner basis reduction

(more discussion later).

Still trying to be rigorous. Simplification is undecidable.

t~0 is undecidable for T defined by R1:

(a) one variable x

(b) constants for rationals and π

(c) +, *, sin, abs and composition.

.. Daniel Richardson, "Some Unsolvable Problems Involving Elementary Functions of a Real Variable." *J. Symbolic Logic* **33**, 514-520, 1968.

(We will go over a version of this, a reduction to Hilbert's 10th problem.)

Still trying to be rigorous (cf. Brown's REX)

Let **Q** be the rational numbers.

If B is a set of complex numbers and z is complex, we say that z is algebraically dependent on B if there is a polynomial

$p(t)=a_d t^d+\ldots+a_0$ in $\mathbf{Q}[B][t]$ with $a_d \neq 0$ and $p(z)=0$.

If S is a set of complex numbers, a transcendence basis for S is a subset B such that no number in B is algebraically dependent on the rest of B and such that every number in S is algebraically dependent on B.

The transcendence rank of a set S of complex numbers is the cardinality of a transcendence basis B for S. (It can be shown that all transcendence bases for S have the same cardinality.)

Simplification of subsets of R1 may be merely difficult

Schanuel's conjecture: If $z_1, \ldots, z_n$ are complex numbers which are linearly independent over **Q** then $(z_1, \ldots, z_n, \exp(z_1), \ldots \exp(z_n))$ has transcendence rank at least n.

It is generally believed that this conjecture is true, but that it would be extremely hard to prove. Even though this is known…

Lindemann's thm: If $z_1, \ldots, z_n$ are complex numbers which are linearly independent over **Q** then $(\exp(z_1), \ldots \exp(z_n))$ are algebraically independent.

What we don't know

Note that we do not even know if $e+\pi$ is rational. From Lindemann we know that $\exp(x)$, $\exp(x^2)$, ... are algebraically independent, and so a polynomial in these forms can be put into a canonical form.

More material at D. Richardson's web site

http://www.bath.ac.uk/~masdr/

What about sin, cos?

- Periodic real functions with algebraic relations
- sin(π/12) = ¼ (sqrt(6)-sqrt(2))
- etc

$$\text{sine}\,(3\,\pi) = 0$$

$$\text{sine}\left(\frac{3\,\pi}{2}\right) = -1$$

$$\text{sine}\,(\pi) = 0$$

$$\text{sine}\left(\frac{3\,\pi}{4}\right) = \frac{1}{\sqrt{2}}$$

$$\text{sine}\left(\frac{3\,\pi}{5}\right) = \cos\left(\frac{\pi}{10}\right)$$

$$\text{sine}\left(\frac{\pi}{2}\right) = 1$$

$$\text{sine}\left(\frac{3\,\pi}{7}\right) = \cos\left(\frac{\pi}{14}\right)$$

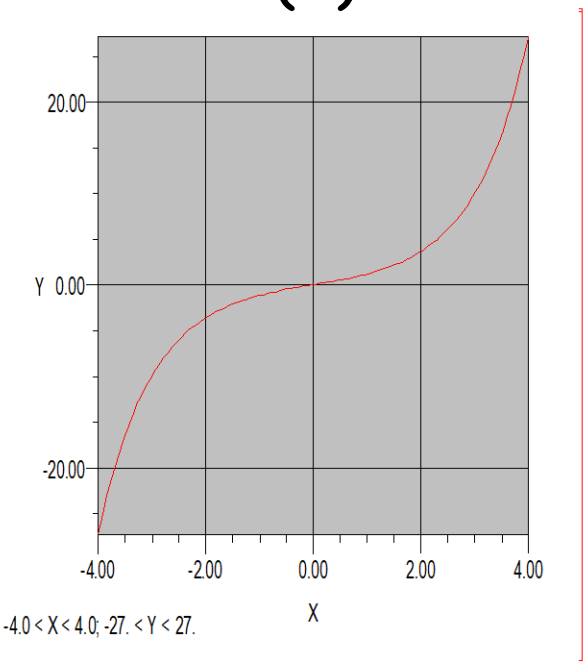
$$\text{sine}\left(\frac{3\,\pi}{8}\right) = \cos\left(\frac{\pi}{8}\right)$$

$$\text{sine}\left(\frac{\pi}{3}\right) = \frac{\sqrt{3}}{2}$$

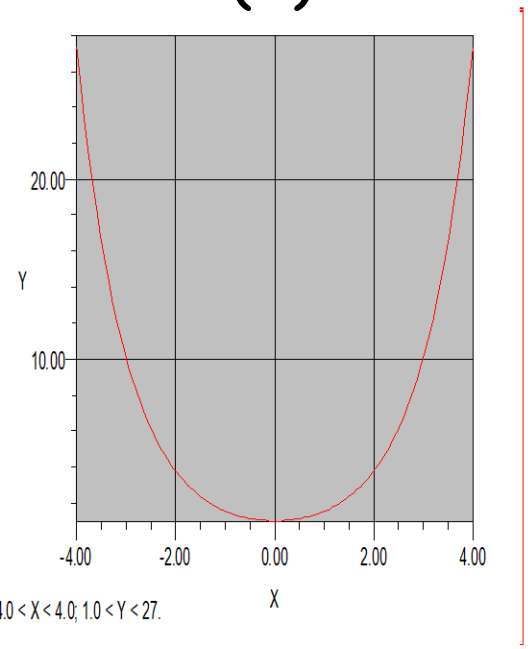
What about sin(complex)?

- sin(a+b*i)= *i* cos(a)sinh(b)+sin(a)cosh(b)
- etc

sinh(x)



cosh(x)



What about sin(something else)?

- Consider sin series as a DEFINITION

$$\sin x = \sum_{i1=0}^{\infty} \frac{(-1)^{i1}\ x^{2\,i1+1}}{(1+2\,i1)!}$$

implications for e.g. matrix calculations

What about arcsin, arccos

- arcsin($\frac{1}{4}$ (sqrt(6)-sqrt(2))) = $\pi/12$

$$\arcsin(120\,\pi) = \frac{\pi}{2} - i\,\log\left(\sqrt{14400\,\pi^2 - 1} + 120\,\pi\right)$$

arcsin(sin(x)) is not x, necessarily

arcsin(sin(0)) = arcsin(0) = 0

arcsin(sin(π)) = arcsin(0) = 0

arctan(tan(4)) is not 4, but 4-π $= .85842..$

What about exponential and log?

- Log(exp(x)) is not the same as x, but is x reduced modulo 2π i. Difference between log and Log? (principal value?)
- Exp(log(x)) is x
- One recent proposal (Corless) introduces the "unwinding number" *K*

$$\mathcal{K}(z) = \frac{z - \log \exp z}{2\pi i} = \left\lceil \frac{\Im z - \pi}{2\pi} \right\rceil \in \mathbf{Z}$$

- log(1/x) = -log(x)-2π i *K* (-log(x))

What about other multi-branched identities?

- arctan(x)+arctan(y)=arctan((x+y)/(1-xy)) $+\pi K$(arctan(x)+arctan(y))

$$\mathcal{K}(z) = \frac{z - \log \exp z}{2\pi i} = \left\lceil \frac{\Im z - \pi}{2\pi} \right\rceil \in \mathbf{Z}$$

- However, not all functions have such a simple structure (The Lambert-W function)
- z=w*exp(w) has solution w=lambert(z), whose branches do not differ by 2π i or any constant.

There are unhappy consequences like..

- arctan(x)+arctan(y)=arctan((x+y)/(1-xy)) $+\pi K$(arctan(x)+arctan(y))
- therefore arctan(x)-arctan(x) might reasonably be a set, namely {$n\pi$ | n 2 **Z**}. Where does this lead us??

Even if we nail down exponential and log what happens next?

- Is sqrt(x) the same as exp($\frac{1}{2}$ log(x)) ? Probably not.
- Is there a way around multiple values of algebraic numbers or functions?
- let sqrt(x) ? {y | $y^2 = x$}
- thus sqrt(9) = {3, -3}
- Or would it be better to say that sqrt(9) is "some root of" p(r) = r^2-9 = 0?

Radicals (surds): Finding a primitive element

- Functions of sqrt(2), sqrt(3)...

Roots:

$$\sqrt{2},\ \sqrt{3}$$

$$z^4 - 10z^2 + 1$$

$$\sqrt{2} = z^3/2 - 9z/2,\ \sqrt{3} = -z^3/2 + 11z/2$$

Using primitive element

- sqrt(2)* sqrt(3) is

$$\frac{\left(\frac{11\,z}{2}-\frac{z^3}{2}\right)\left(z^3-9\,z\right)}{2}=-\frac{z^6-20\,z^4+99\,z^2}{4}$$

modulo the defining polynomial z^4-10z+1 this is (z^2-5)/2 .

Squaring again gives (z^4-10z^2+25)/4, which reduces to 6. So sqrt(2)*sqrt(3) is sqrt(6).

Tada.

Macsyma allow us to factor, this way..

- (C1) factor(x^2-3, z^4-10*z^2+1);

  (D1) ((- z^3 + 11z + 2x) * (z^3 - 11 z + 2x)/4)

- (C2) tellrat(z^4-10*z^2+1);

  (D2) x^2-3

This is really treating algebraic numbers as sets

- Just about the only way to "get rid of" sqrt(s) is to square it and get s.
- If we could distinguish the roots $\{r_1, r_2\}$ such that $r_i^2 = s$, then $r_1 + r_2 = 0$, also.
- Any other transformation is algebraically dangerous, even if it is tempting.
- Programs sometimes provide:
- sqrt(x)*sqrt(y) vs. sqrt(x*y)
- sqrt(x^2) vs. x or abs(x) or sign(x)*x
- However sqrt(1-z)*sqrt(1+z)=sqrt($1-z^2$) IS TRUE
- How to prove this?? (Monodromy Thm)

Moses' characterization of politics of simplification

- Radical
- Conservative
- Liberal
- New Left
- catholic (= eclectic)

- <discuss Moses' *CACM* article>

Richardson's undecidability problem

- We start with the unsolvability of Hilbert's 10 problem, proved by Matiyasevic in 1970.
- Thm: There exists a set of polynomials over the integers $P = \{P(x_1, \ldots, x_n)\}$ such that over all P in P the predicate "there exists non-negative integers $a_1, \ldots, a_n$ such that $P(a_1, \ldots, a_n)=0$" is recursively undecidable."
- (proof: see e.g. Martin Davis, AMM 1973,)

David Hilbert, 1900

- http://aleph0.clarku.edu/~djoyce/hilbert/

"Hilbert's address of 1900 to the International Congress of Mathematicians in Paris is perhaps the most influential speech ever given to mathematicians, given by a mathematician, or given about mathematics. In it, Hilbert outlined 23 major mathematical problems to be studied in the coming century."

I guess mathematicians should be given some leeway here...

Martin Davis, Julia Robinson, Yuri Matiyasevich

Reductions we need:

- Richardson requires only one variable x, Hilbert's 10^{th} problem requires n (3, perhaps?)
- Richardson is talking about continuous everywhere defined functions, the Diophantine problem is INTEGERS.

From many vars to one

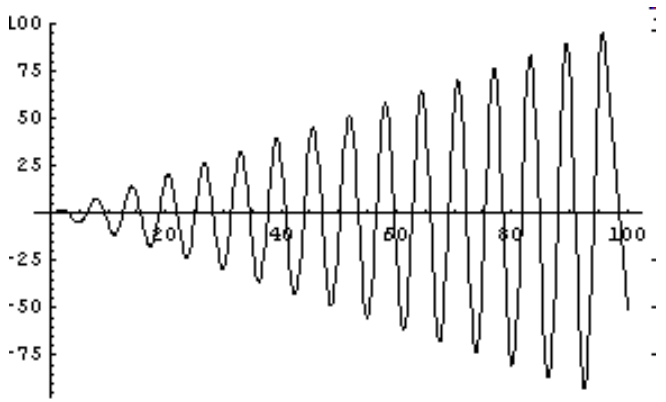
- Notation, for f: R→R by $f^{(0)}(x)$ we mean x, and by $f^{(i+1)}(x)$ we mean $f(f^{(i)}(x))$ for all i¸ 0.

- Lemma 1: Let $h(x)=x \sin(x)$ and $g(x)=x \sin(x^3)$.

Then for any real $a_1, \ldots, a_n$ and any $0 < \varepsilon < 1$, 9 b such that 8 $(1 \cdot k \cdot n)$, $|h(g^{(k-1)}(b))-a_k| < \varepsilon$

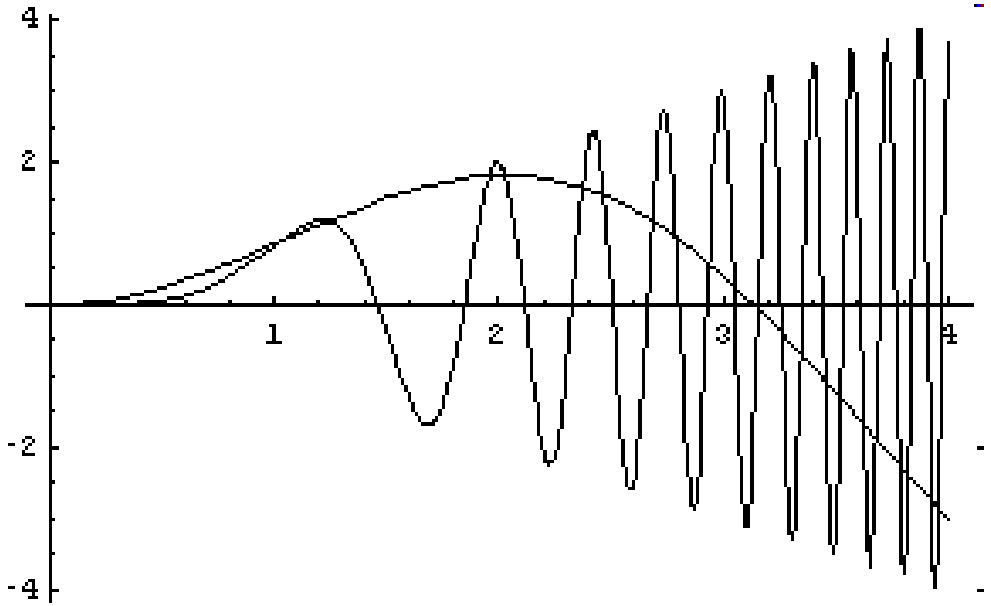
From many vars to one

- Sketch of proof. (by induction).. Given any 2 numbers a_1 and a_2, there exists b>0 such that $|h(b)-a_1|<\varepsilon$ and $g(b)=a_2$ Look at the graph of y=h(x):=x*sin(x). It goes arbitrarily close to any value of y arbitrarily many times.



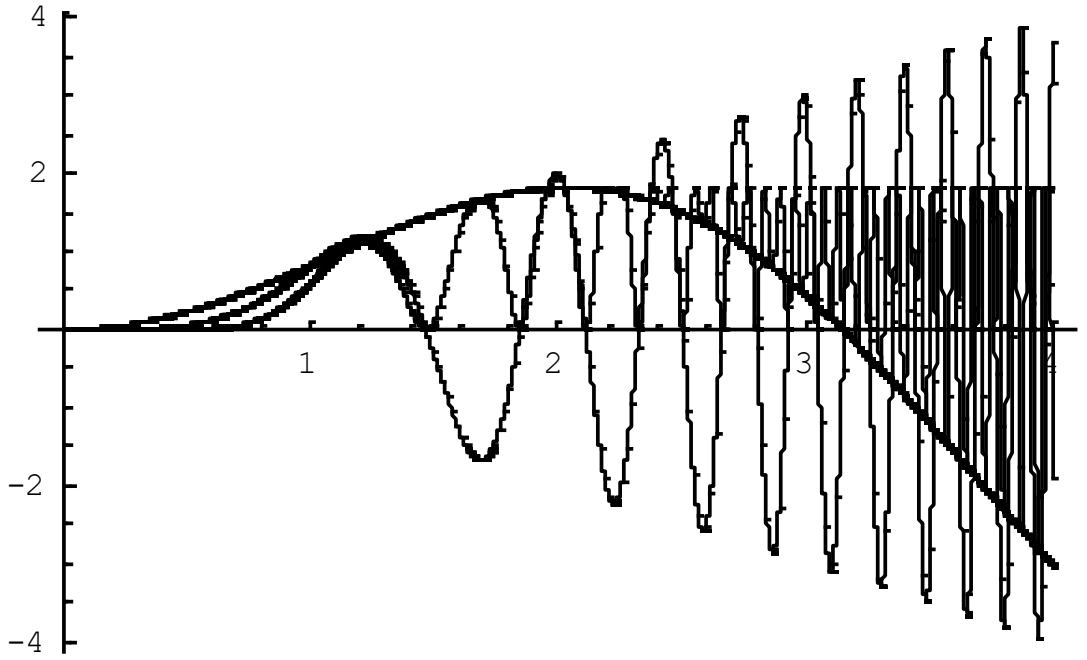
From many vars to one

- Look at the graph of g(x) as well as h(x). We look closer … Every time h(x), the slow moving curve, goes near some value, g(x) goes near it many more times.

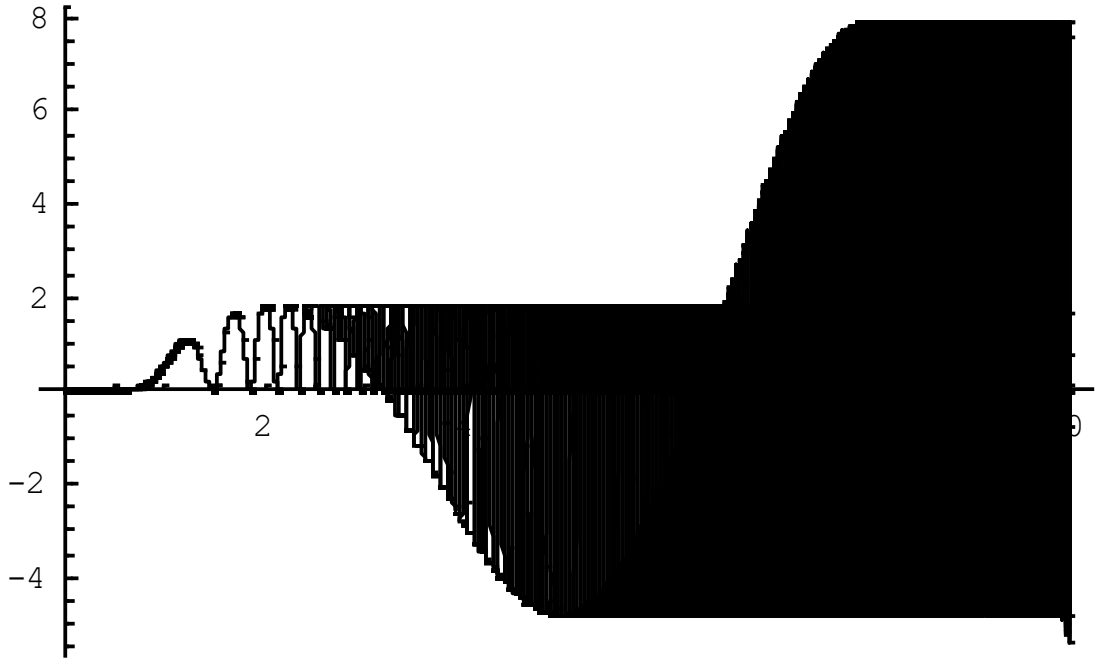


h(x), g(x), h(g(x))

- All plotted together



h(g(x)), alone, out to 10



Actually, the picture, at this resolution,
should fill in completely after about 4.
The (Mathematica) plotting program shows
“beats” at its sample rate.

h(g(x)), alone, out to 20

Actually, the
should fill in completely after about 4.
The (Mathematica) plotting program shows
“beats” at its sample rate.

Now suppose Lemma 1 is true for n.

- That is, 9 b′ such that $|h(b')-a_2| < \varepsilon$, $|h(g(b'))-a_3| < \varepsilon$ … $|h(g^{(n-1)}(b'))-a_3| < \varepsilon$. Hence 9 b>0 such that $|h(b)-a_1| < \varepsilon$ and g(b) = b′. Therefore the result holds for n+1. QED

- Why are we doing this? We wish to show that any finite collection of n real numbers can be encoded "close enough for any practical purpose" in one real number by using functions x*sin(x) and $x*\sin(x^3)$. This is not the only way to do this, but Richardson wanted a simple encoding. Interleaving decimal digits would be another way, but messier. Henceforth we assume we can encode any set of reals $\underline{b}= \{b_1,\ldots,b_n\}$ into a single real number.

Next step: dominating functions.

- $F(x_1,\ldots,x_n) \in R$ is dominated by $G(x_1,\ldots,x_n) \in R$ if for all real $x_1, \ldots, x_n$

1. $G(x_1,\ldots,x_n) > 1$
2. For all real $\Delta_1, \ldots, \Delta_n$ such that $|\Delta_i| < 1$, $G(x_1,\ldots,x_n) > F(x_1+\Delta_1, \ldots, x_n+\Delta_n)$

Lemma 2: For any $F \in R$ there is a dominating function G.

Proof (by induction on the number of operators in G).

Proof of Lemma 2: dominating functions.

Lemma 2: For any F 2 R there is a dominating function G.

Proof (by induction on the number of operators in G).

If $F=f_1+f_2$, let $G=g_1^2+g_2^2+2$.

If $F= f_1*f_2$, let $G=(g_1^2+2)*(g_2^2+2)$.

If $F=x$, let $G=x^2+2$.

If $F=\sin(x)$, let $G=2$.

If $F = c$, a constant, let $G= c^2+2$

The theorem

- Theorem: For each P 2 *P* there exists F 2 R such that (i) there exists an n-tuple of nonnegative integers $\underline{A}$= (a_1, …,a_n) such that P(*A*)=0 iff (ii) there exists an n-tuple of nonnegative real numbers $\underline{B}$=(b_1, …,b_n) such that F($\underline{B}$)<0.
- *(note: (i) is Hilbert's 10th problem, undecidable)*

How we do this.

- We need to find only those real solutions of F which are integer solutions of P.
- Note that $\sin^2(\pi x_i)$ will be zero only if x_i is an integer. We can use this to force Richardson's continuous x_i to happen to fall on integers a_i!

Proof, (i) → (ii)

- Consider P 2 *P*, (i) →(ii): for $1 \cdot i \cdot n$, let K_i be a dominating function for $\partial/\partial x_i$ (P^2). Note that for $1 \cdot i \cdot n$, K_i 2 *P*.
- Let

$$F(x_1,\ldots,x_n)=(n+1)^2\{P^2(x_1,\ldots,x_n)+ \sum_{1 \cdot i \cdot n}\sin^2(\pi x_i)*K_i^2\ (x_1,\ldots,x_n)\}\ -1$$

- Now suppose $\underline{A}=(a_1,\ldots,a_n)$ is such that $P(\underline{A})=0$. Then $F(\underline{A})=-1$. So (i)→(ii).

Proof, continued (ii) → (i)

Still, let

$$F(x_1,\ldots,x_n)=(n+1)^2\{P^2(x_1,\ldots,x_n)+ \sum_{1 \cdot i \cdot n}\sin^2(\pi x_i)*K_i^2\ (x_1,\ldots,x_n)\} -1$$

- Now suppose $\underline{B}=(b_1,\ldots,b_n)$, a vector of non-negative real numbers is such that $F(\underline{B})<0$. Choose a_i to be the smallest integer such that $|a_i-b_i| \cdot \frac{1}{2}$. We will show that $P^2(\underline{A})<1$ which implies $P(\underline{A})=0$ since P assumes only integer values. $F(\underline{B})<0$ implies that...

Proof, continued (ii) → (i), F(b)<0

F($\underline{B}$)<0 means

$(n+1)^2\{P^2(\underline{B}) + \sum_{1 \cdot i \cdot n} \sin^2(\pi b_i) * K_i^2(\underline{B})\} - 1 < 0$

or

$P^2(\underline{B}) + \sum_{1 \cdot i \cdot n} \sin^2(\pi b_i) * K_i^2(\underline{B}) < 1/(n+1)^2$

- Since each of the factors in the sum on the left is non-negative, we have that each of the summands is individually less than $1/(n+1)^2$ which is itself < $1/(n+1)$. In particular, $P^2(\underline{B}) < 1/(n+1)^2 < 1/(n+1)$

and also for each i, $|\sin(\pi\, b_i) * K_i(\underline{B})| < 1/(n+1)$

Proof, continued (ii) → (i)

By the n-dimensional mean value theorem of calculus,

$P^2(\underline{A}) = P^2(\underline{B}) + \sum_{1 \cdot i \cdot n} |a_i - b_i| \, \partial/\partial x_i \, P^2(c_1,\ldots,c_n)$

for some set of c_i where $\min(a_i,b_i) \cdot c_i \cdot \max(a_i,b_i)$.

Since K_i is a dominating function for $\partial/\partial x_i P^2(x_1,\ldots,x_n)$ for each i,

$P^2(\underline{A}) < P^2(\underline{B}) + \sum_{1 \cdot i \cdot n} |a_i - b_i| K_i(\underline{B})$.

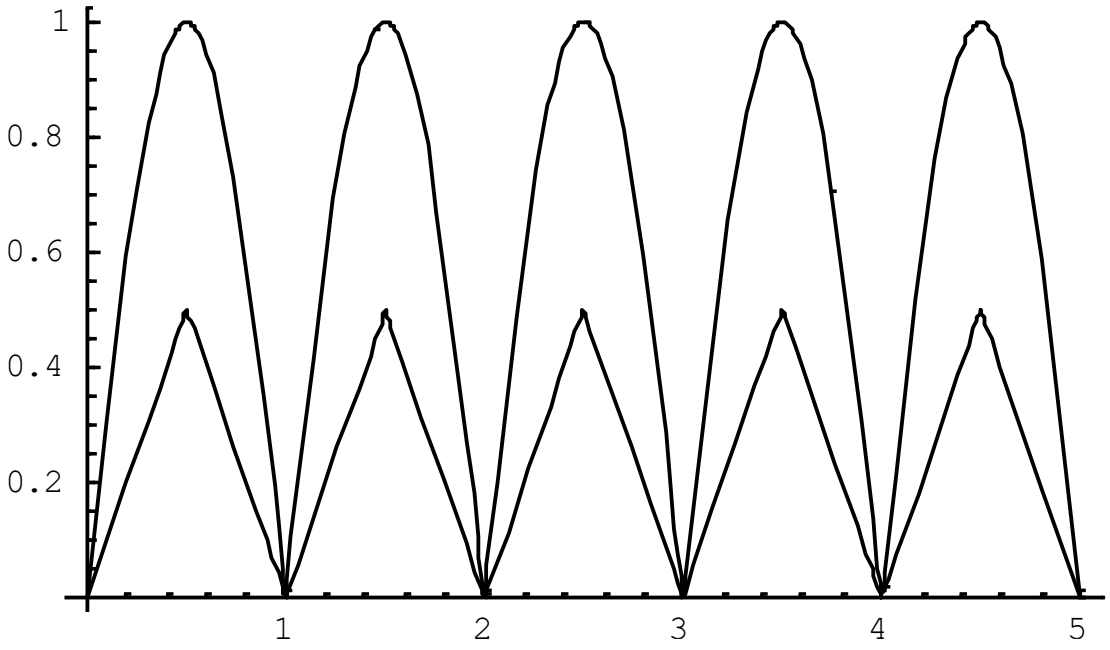
(Note that $|c_i - b_i| \cdot |a_i - b_i| < \frac{1}{2}$.)

Proof, continued (ii) → (i)

We need to show that $|a_i - b_i| < |\sin(\pi\, b_i)|$... but recall that a_i is the smallest integer such that $|a_i - b_i| \cdot \frac{1}{2}$. What do these functions look like?

Proof, continued (ii) → (i)

plot[{|sin(πx)|, |x-ceiling(x-1/2)|}, x=0..5]



the home stretch.. substituting for $|a_i - b_i|$

$P^2(\underline{A}) < P^2(\underline{B}) + \sum_{1 \cdot i \cdot n} |\sin(\pi b_i)| K_i(\underline{B})$

By previous results, each of the n+1
terms on the right is less than 1/(n+1),
so $P(\underline{A}) < 1$.

So the predicate "there exists a real number β, the encoding of $\underline{B}$ such that $G(\beta) = F(\underline{B}) \leq 0$" is recursively undecidable.

Now suppose $G(x) \in R$, then so is $|G(x)| - G(x) \in R$. We cannot tell if F(x) is zero if we cannot tell if $G(x) < 0$. So we have proved Richardson's result. QED (whew!)

More details in Caviness' paper.

Does this matter?

- Richardson's theorem tells us that we can't make certain statement about a computer algebra algorithms, e.g. "solves all integration problems" at least if the algorithm requires knowing if an expression from this class R is zero.
- It doesn't enter explicitly into our programs, since the difficulty of simplifying sub-classes of this, or "other" classes is computationally hard and/or ill-defined anyway, but we can often simplify effectively, regardless of this result.