

Formalization and Automated Reasoning: A Personal and Historical Perspective

John Harrison

13th Feb 2023 (14:30-15:20)

Summary of talk

- ▶ Retrospective
- ▶ Automated and interactive theorem proving
- ▶ Effective libraries, reasons for formalizing
- ▶ Case study: the isoperimetric theorem.

A personal retrospective

I wrote my first formal proof in 1990 and have been doing formal proofs and implementing theorem proving procedures for most of the intervening time. What have three decades taught me?

Automation, interaction, libraries

- ▶ Automation has advanced, but only incrementally, and nothing in modern systems would particularly surprise or impress anyone familiar with the state of the art in the mid-1970s.

Automation, interaction, libraries

- ▶ Automation has advanced, but only incrementally, and nothing in modern systems would particularly surprise or impress anyone familiar with the state of the art in the mid-1970s.
- ▶ In some ways we have advanced by the conscious choice to use interactive rather than automated proof, to retain a higher degree of control and programmability.

Automation, interaction, libraries

- ▶ Automation has advanced, but only incrementally, and nothing in modern systems would particularly surprise or impress anyone familiar with the state of the art in the mid-1970s.
- ▶ In some ways we have advanced by the conscious choice to use interactive rather than automated proof, to retain a higher degree of control and programmability.
- ▶ The sheer amount of formalized material available in prover libraries has greatly increased, and this makes the biggest difference to the work involved in formalizing new results.

Automation, interaction, libraries

- ▶ Automation has advanced, but only incrementally, and nothing in modern systems would particularly surprise or impress anyone familiar with the state of the art in the mid-1970s.
- ▶ In some ways we have advanced by the conscious choice to use interactive rather than automated proof, to retain a higher degree of control and programmability.
- ▶ The sheer amount of formalized material available in prover libraries has greatly increased, and this makes the biggest difference to the work involved in formalizing new results.
- ▶ Ironically, this may be leading to a resurgence in AI-style automation because the large libraries of results proved via interaction provide fodder for machine learning.

Automation, interaction, libraries

- ▶ Automation has advanced, but only incrementally, and nothing in modern systems would particularly surprise or impress anyone familiar with the state of the art in the mid-1970s.
- ▶ In some ways we have advanced by the conscious choice to use interactive rather than automated proof, to retain a higher degree of control and programmability.
- ▶ The sheer amount of formalized material available in prover libraries has greatly increased, and this makes the biggest difference to the work involved in formalizing new results.
- ▶ Ironically, this may be leading to a resurgence in AI-style automation because the large libraries of results proved via interaction provide fodder for machine learning.
- ▶ Developing an effective formal library often requires a blend of application-driven and systematic bottom-up construction.

Automated and interactive proof

Automated provers came first

Most early theorem provers (1950s–60s) were fully automatic, with two main approaches:

- ▶ Human-oriented AI style approaches (Newell-Simon, Gelerntner)
- ▶ Machine-oriented algorithmic approaches (Davis, Gilmore, Wang, Prawitz)

Automated theorem proving in its pomp

The 1960s and 1970s saw rapid development of machine-oriented automated theorem proving:

Automated theorem proving in its pomp

The 1960s and 1970s saw rapid development of machine-oriented automated theorem proving:

- ▶ Robinson's resolution method and other techniques for first-order logic
- ▶ Knuth-Bendix completion for equational logic
- ▶ Boyer-Moore style automation of inductive proof
- ▶ Shostak and Nelson-Oppen work on cooperating decision procedures, congruence closure

Automated theorem proving in its pomp

The 1960s and 1970s saw rapid development of machine-oriented automated theorem proving:

- ▶ Robinson's resolution method and other techniques for first-order logic
- ▶ Knuth-Bendix completion for equational logic
- ▶ Boyer-Moore style automation of inductive proof
- ▶ Shostak and Nelson-Oppen work on cooperating decision procedures, congruence closure

However, when the power of such methods began to plateau, it was hard to make further progress and the field stagnated.

Interactive theorem proving

The idea of a more 'interactive' approach was already anticipated by pioneers, e.g. Wang (1960):


[...] the writer believes that perhaps machines may more quickly become of practical use in mathematical research, not by proving new theorems, but by formalizing and checking outlines of proofs, say, from textbooks to detailed formalizations more rigorous than Principia [Mathematica], from technical papers to textbooks, or from abstracts to technical papers.

But serious interest had to wait, perhaps for disillusion with pure automation to set in, or for the interactive capacities of computer systems to improve.

First steps in interactive theorem proving

Early interactive provers by Paul Abrahams, then Bledsoe and Gilbert:

seminar | computer implementation of the



JULY 17-19

$$\begin{aligned} & (0 \rightarrow p) \\ & ((0 \in p) \leftrightarrow p) \\ & (x \subset y \rightarrow (x \rightarrow y)) \\ & (\nabla A \equiv \forall y (y \in A \wedge y)) \\ & (\forall x \wedge y \underline{u} : x y \equiv \wedge y \forall x \underline{u} : x y) \\ & (f = \wedge x \underline{u} x \wedge x \in \text{dom } f \rightarrow f x = \underline{u} x) \\ & (a \subset b \wedge c \subset d \rightarrow a \cap c \subset b \cap d) \end{aligned}$$

mathematical language of A.P. Morse

The Mathematics Department of Sandia Laboratory will sponsor during July a continuation of a study first started in the summer of 1966 investigating the possibility of computer implementation of the mathematical language of Professor A. P. Morse. The initial objective of this work was to write a program which would accept a statement in this language, determine if the statement was a formula, analyze the structure of a formula, and categorize the variables.

The persons involved in the earlier work were J. W. Weihe, D. R. Morrison, E. J. Gilbert, L. T. Ritchie, and R. R. Berlind of Sandia Corporation; T. J. McMinn, University of Nevada; W. W. Bledsoe, University of Texas; and D. C. Peterson, U. S. Air Force Academy. Weihe, McMinn, Bledsoe, and Peterson are former students of Morse. Programs were written — primarily by Peterson, Berlind and Ritchie — which met the 1966 summer objective.

Since this summer program, Peterson has implemented a program on the Burroughs 5500 which will perform certain syntactic operations on several languages, including the Morse language and ALGOL. Bledsoe and Gilbert have been investigating an enlarged set of rules of inference which are to simplify proofs and enhance the proof checking capability of the program.

In order to afford an opportunity to summarize past accomplishments and to examine the possibilities for future work, the Mathematics Department will host a seminar July 17-19 at the Coronado Club on Sandia Base. The first day of the Seminar will be devoted to presentations of results achieved so far, as set forth in the agenda. Attendees will spend the next two days in informal discussions of the future of this work as well as certain aspects of the current achievements.

This invitation is extended to those whose interest is known to us. Although Sandia Laboratory can offer financial assistance only to participating members, it is hoped that other mathematicians interested in the work will

be able to attend. A list of the persons to whom invitations have been extended is enclosed. Should you know persons whom we have overlooked, they also are cordially invited.

If there are any questions or if we can be of assistance, please call COLLECT J. W. Weihe at 565-564-5743 or D. R. Morrison at 565-564-2549. A registration form is attached for your convenience. Although there are a number of nearby motels, the White Winrock Motor Hotel is perhaps the most convenient. We would be glad to make reservations for you there or any other motel you designate.

AGENDA JULY 17, 1967

9:00 A.M. TO 4:00 P.M.

J. W. Weihe	Introduction
A. P. Morse	Language and Inference
W. W. Bledsoe	Rules of Inference
D. R. Morrison	Library Automata
LUNCH	
T. J. McMinn	Simultaneous Substitution
E. J. Gilbert	Proof Checking
D. C. Petersen	Syntactic Analysis for Phrase Structure Grammars

SAM

First successful family of interactive provers were the SAM systems:

Semi-automated mathematics is an approach to theorem-proving which seeks to combine automatic logic routines with ordinary proof procedures in such a manner that the resulting procedure is both efficient and subject to human intervention in the form of control and guidance. Because it makes the mathematician an essential factor in the quest to establish theorems, this approach is a departure from the usual theorem-proving attempts in which the computer unaided seeks to establish proofs.

SAM V was used to settle an open problem in lattice theory.

Three influential proof checkers

- ▶ AUTOMATH (de Bruijn, ...) — Implementation of type theory, used to check non-trivial mathematics such as Landau's *Grundlagen*

Three influential proof checkers

- ▶ AUTOMATH (de Bruijn, ...) — Implementation of type theory, used to check non-trivial mathematics such as Landau's *Grundlagen*
- ▶ Mizar (Trybulec, ...) — Block-structured natural deduction with 'declarative' justifications, used to formalize large body of mathematics

Three influential proof checkers

- ▶ AUTOMATH (de Bruijn, ...) — Implementation of type theory, used to check non-trivial mathematics such as Landau's *Grundlagen*
- ▶ Mizar (Trybulec, ...) — Block-structured natural deduction with 'declarative' justifications, used to formalize large body of mathematics
- ▶ LCF (Milner et al) — Programmable proof checker for Scott's Logic of Computable Functions written in new functional language ML.

Three influential proof checkers

- ▶ AUTOMATH (de Bruijn, ...) — Implementation of type theory, used to check non-trivial mathematics such as Landau's *Grundlagen*
- ▶ Mizar (Trybulec, ...) — Block-structured natural deduction with 'declarative' justifications, used to formalize large body of mathematics
- ▶ LCF (Milner et al) — Programmable proof checker for Scott's Logic of Computable Functions written in new functional language ML.

Ideas from all these systems are used in present-day systems.

Milner on automation and interaction

I wrote an automatic theorem prover in Swansea for myself and became shattered with the difficulty of doing anything interesting in that direction and I still am. I greatly admired Robinson's resolution principle, a wonderful breakthrough; but in fact the amount of stuff you can prove with fully automatic theorem proving is still very small. So I was always more interested in amplifying human intelligence than I am in artificial intelligence.

Libraries: their motivations and problems

Libraries

To avoid always starting from ground level, it's vital to build up “libraries” of basic mathematical results. Otherwise any interesting proof tends to regress into a long stream of elementary and often barely relevant lemmas.

Libraries

To avoid always starting from ground level, it's vital to build up "libraries" of basic mathematical results. Otherwise any interesting proof tends to regress into a long stream of elementary and often barely relevant lemmas.

- ▶ Sometimes flashy or exciting theorems (e.g. the Picard theorems) aren't as useful as less showy ones that are the workhorses of libraries (the change of variables formula for integrals etc.)

Libraries

To avoid always starting from ground level, it's vital to build up “libraries” of basic mathematical results. Otherwise any interesting proof tends to regress into a long stream of elementary and often barely relevant lemmas.

- ▶ Sometimes flashy or exciting theorems (e.g. the Picard theorems) aren't as useful as less showy ones that are the workhorses of libraries (the change of variables formula for integrals etc.)
- ▶ Large formalizations (Odd Order Theorem, Flyspeck) have motivated formalization of ‘foundational’ material as a by-product, making similar efforts easier in future.

Libraries

To avoid always starting from ground level, it's vital to build up “libraries” of basic mathematical results. Otherwise any interesting proof tends to regress into a long stream of elementary and often barely relevant lemmas.

- ▶ Sometimes flashy or exciting theorems (e.g. the Picard theorems) aren't as useful as less showy ones that are the workhorses of libraries (the change of variables formula for integrals etc.)
- ▶ Large formalizations (Odd Order Theorem, Flyspeck) have motivated formalization of ‘foundational’ material as a by-product, making similar efforts easier in future.
- ▶ The earliest large mathematical library is the Mizar Mathematical Library (MML), following the style of mathematical papers with extracted text and references.

Libraries

To avoid always starting from ground level, it's vital to build up “libraries” of basic mathematical results. Otherwise any interesting proof tends to regress into a long stream of elementary and often barely relevant lemmas.

- ▶ Sometimes flashy or exciting theorems (e.g. the Picard theorems) aren't as useful as less showy ones that are the workhorses of libraries (the change of variables formula for integrals etc.)
- ▶ Large formalizations (Odd Order Theorem, Flyspeck) have motivated formalization of ‘foundational’ material as a by-product, making similar efforts easier in future.
- ▶ The earliest large mathematical library is the Mizar Mathematical Library (MML), following the style of mathematical papers with extracted text and references.
- ▶ Many theorem provers including Coq, HOL Light, Isabelle/HOL (including the ‘archive of formal proofs’) and Lean also have large and every-expanding mathematical libraries.

Reasons for developing library results

- ▶ 'As needed': some high-level application in verification or formalization needs key definitions or lemmas

Reasons for developing library results

- ▶ 'As needed': some high-level application in verification or formalization needs key definitions or lemmas
- ▶ Conscious development of foundations with an overall application in mind (e.g. measure theory in Euclidean space for the Flyspeck project).

Reasons for developing library results

- ▶ 'As needed': some high-level application in verification or formalization needs key definitions or lemmas
- ▶ Conscious development of foundations with an overall application in mind (e.g. measure theory in Euclidean space for the Flyspeck project).
- ▶ Simple curiosity, fun, excuse to more thoroughly understand a piece of mathematics or exercise the theorem prover.

Reasons for developing library results

- ▶ 'As needed': some high-level application in verification or formalization needs key definitions or lemmas
- ▶ Conscious development of foundations with an overall application in mind (e.g. measure theory in Euclidean space for the Flyspeck project).
- ▶ Simple curiosity, fun, excuse to more thoroughly understand a piece of mathematics or exercise the theorem prover.
- ▶ Completionism, often takes over once some other motivation provided the initial push.

Reasons for developing library results

- ▶ 'As needed': some high-level application in verification or formalization needs key definitions or lemmas
- ▶ Conscious development of foundations with an overall application in mind (e.g. measure theory in Euclidean space for the Flyspeck project).
- ▶ Simple curiosity, fun, excuse to more thoroughly understand a piece of mathematics or exercise the theorem prover.
- ▶ Completionism, often takes over once some other motivation provided the initial push.

All of these different motivations and approaches tend to result in stylistically different libraries. The best are often motivated by a combination of all of these.

Libraries: what can go wrong?

- ▶ Applications turn out to require more general forms of some basic lemmas

Libraries: what can go wrong?

- ▶ Applications turn out to require more general forms of some basic lemmas
- ▶ Even though all hypotheses of a lemma hold in the particular application, a more economical list would be easier to discharge

Libraries: what can go wrong?

- ▶ Applications turn out to require more general forms of some basic lemmas
- ▶ Even though all hypotheses of a lemma hold in the particular application, a more economical list would be easier to discharge
- ▶ Some subtle mismatch or forgotten degenerate cases can make lemmas or even axioms vacuous or contradictory, or definitions inconvenient.

Libraries: what can go wrong?

- ▶ Applications turn out to require more general forms of some basic lemmas
- ▶ Even though all hypotheses of a lemma hold in the particular application, a more economical list would be easier to discharge
- ▶ Some subtle mismatch or forgotten degenerate cases can make lemmas or even axioms vacuous or contradictory, or definitions inconvenient.

My rule of thumb: if you haven't used a library for a non-trivial application, there's probably something significantly wrong about the way it is organized, and quite possibly about the basic definitions.

Case study: the isoperimetric theorem

The Great 100 Theorems

Formalizing 100 Theorems

There used to exist a "[top 100 of mathematical theorems](#)" on the web, which is a rather arbitrary list (and most of the theorems seem rather elementary), but still is nice to look at. On the current page I will keep track of which theorems from this list have been formalized. Currently the fraction that already has been formalized seems to be

99%

The page does not keep track of *all* formalizations of these theorems. It just shows formalizations in systems that have formalized a significant number of theorems, or that have formalized a theorem that none of the others have done. The systems that this page refers to are (in order of the number of theorems that have been formalized, so the more interesting systems for mathematics are near the top):

Isabelle	87
HOL Light	87
Coq	79
Metamath	74
Lean	74
Mizar	69
ProofPower	43
PVS	22
ngthm/ACL2	18
NuPRL/MetaPRL	8

Theorems in the list which have not been formalized yet are in *italics*. Formalizations of constructive proofs are in *italics* too. The difficult proofs in the list (according to John all the others are not a serious challenge "given a week or two") have been underlined. The formalizations under a theorem are in the order of the list of systems, and *not* in chronological order.

The List

The goal was to get the total from 98% to 99%.

The Isoperimetric Theorem (informally)

A typical statement:

**BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 84, Number 6, November 1978**

THE ISOPERIMETRIC INEQUALITY

BY ROBERT OSSERMAN¹

The circle is uniquely characterized by the property that among all simple closed plane curves of given length L , the circle of circumference L encloses maximum area. This property is most succinctly expressed in the isoperimetric inequality

$$L^2 \geq 4\pi A, \tag{1}$$

The Isoperimetric Theorem (formally)

The formalized HOL Light statement in HOL Light ASCII syntax, as presented on the “Great 100 Theorems” page.

43. The Isoperimetric Theorem

ISOPERIMETRIC_THEOREM

```
|- !L g.  
  rectifiable_path g /\  
  simple_path g /\  
  pathfinish g = pathstart g /\  
  path_length g = L  
  ==> measure(inside (path_image g)) <= L pow 2 / (&4 * pi) /\  
    (measure(inside (path_image g)) = L pow 2 / (&4 * pi)  
    ==> (?a r. path_image g = sphere (a,r)))
```


Unpacking the definitions (standard)

The notions of 'path', 'simple path', 'rectifiable', 'length' etc. are pretty standard; paths are just functions out of $[0, 1]$, apart from some vector type tweaks.

```
|- path(g:real^1->real^N) <=> g continuous_on interval[vec 0,vec 1]
```

```
|- rectifiable_path (g:real^1->real^N) <=>  
  path g /\ g has_bounded_variation_on interval[vec 0,vec 1]
```

```
|- path_length (g:real^1->real^N) =  
  vector_variation (interval[vec 0,vec 1]) g
```

Unpacking the definitions (standard)

The notions of 'path', 'simple path', 'rectifiable', 'length' etc. are pretty standard; paths are just functions out of $[0, 1]$, apart from some vector type tweaks.

```
|- path(g:real^1->real^N) <=> g continuous_on interval[vec 0,vec 1]
```

```
|- rectifiable_path (g:real^1->real^N) <=>  
  path g /\ g has_bounded_variation_on interval[vec 0,vec 1]
```

```
|- path_length (g:real^1->real^N) =  
  vector_variation (interval[vec 0,vec 1]) g
```

These in turn unpack to more integration theory, which was all initially developed to support the Flyspeck proof.

Unpacking the definitions (not so standard)

The “inside” function returns the union of bounded components of the complement:

```
|- inside (s:real^N->bool) =  
  {x | ~(x IN s) /\  
    bounded(connected_component ((:real^N) DIFF s) x)}
```

Unpacking the definitions (not so standard)

The “inside” function returns the union of bounded components of the complement:

```
|- inside (s:real^N->bool) =  
  {x | ~(x IN s) /\  
    bounded(connected_component ((:real^N) DIFF s) x)}
```

This notion is completely different from “interior”, and is somewhat distinctive but convenient, applying even to non-simple curves and other shapes.

Jordan with inside and outside

With its “outside” dual (union of unbounded components of the complement) this gives a tidy-looking general form of the Jordan Curve Theorem:

```
JORDAN_INSIDE_OUTSIDE_GEN =  
|- !s:real^N->bool.  
  2 <= dimindex(:N) /\  
  s homeomorphic sphere(vec 0:real^N,&1)  
==> ~(inside s = {}) /\  
  open(inside s) /\  
  connected(inside s) /\  
  ~(outside s = {}) /\  
  open(outside s) /\  
  connected(outside s) /\  
  bounded(inside s) /\  
  ~bounded(outside s) /\  
  inside s INTER outside s = {} /\  
  inside s UNION outside s = (:real^N) DIFF s /\  
  frontier(inside s) = s /\  
  frontier(outside s) = s
```

Jordan with inside and outside

With its “outside” dual (union of unbounded components of the complement) this gives a tidy-looking general form of the Jordan Curve Theorem:

```
JORDAN_INSIDE_OUTSIDE_GEN =  
|- !s:real^N->bool.  
  2 <= dimindex(:N) /\  
  s homeomorphic sphere(vec 0:real^N,&1)  
==> ~(inside s = {}) /\  
  open(inside s) /\  
  connected(inside s) /\  
  ~(outside s = {}) /\  
  open(outside s) /\  
  connected(outside s) /\  
  bounded(inside s) /\  
  ~bounded(outside s) /\  
  inside s INTER outside s = {} /\  
  inside s UNION outside s = (:real^N) DIFF s /\  
  frontier(inside s) = s /\  
  frontier(outside s) = s
```

This Euclidean topology was originally developed just for fun/interest.

Reduction to the convex case (informally)

Given any non-convex simple closed curve, there is a convex curve that is shorter and encloses a larger area:

A proof of the isoperimetric inequality for convex \hat{K} implies it for any set. In the first place, since $K \subset \hat{K}$ by its definition, we have $\hat{A} \geq A$. On the other hand, taking convex hull reduces the boundary length because the interior segments of the boundary curve, that is the components of $\gamma - \partial\hat{K}$ of γ are replaced by straight line segments in $\partial\hat{K}$.

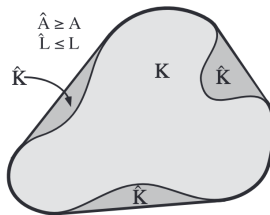


Fig. 1. The region K and its convex hull \hat{K} .

Thus, knowing the isoperimetric inequality for convex sets, we deduce

$$4\pi A \leq 4\pi \hat{A} \leq \hat{L}^2 \leq L^2.$$

Andrejs Treibergs, "The Strong Isoperimetric Inequality of Bonnesen"

Reduction to the convex case (formally)

Easy? But even a rectifiable curve can have infinitely many “wiggles”, so it seemed to call for a limit argument.

```
...
?h. (!n. simple_path (h n) /\
      rectifiable_path (h n) /\
      pathstart (h n) = pathstart g /\
      pathfinish (h n) = pathfinish g /\
      convex hull path_image (h n) = convex hull path_image g /\
      (!x y.
        x IN interval [vec 0,vec 1] /\ y IN interval [vec 0,vec 1]
        ==> dist (h n x,h n y) <= L * dist (x,y)) /\
      (!x.
        x IN UNIONS {interval (a m,b m) | m < n}
        ==> h n x IN frontier (convex hull path_image g)) /\
      (!x. ~(x IN UNIONS {interval (a m,b m) | m < n})
        ==> h n x = g x)) /\
(!n x. ~(x IN interval(a n,b n) /\
      !m. m < n ==> ~(x IN interval(a m,b m)))
  ==> (h:num->real^1->real^2)(SUC n) x = h n x)
...
```


Reduction to the convex case (formally)

The end result is at least natural:

```
|- !g:real^1->real^2.  
  rectifiable_path g /\  
  simple_path g /\  
  pathfinish g = pathstart g /\  
  ~convex(inside(path_image g))  
==> ?h:real^1->real^2.  
  rectifiable_path h /\  
  simple_path h /\  
  pathfinish h = pathstart h /\  
  path_length h <= path_length g /\  
  convex hull path_image h = convex hull path_image g /\  
  path_image h = frontier (convex hull path_image g) /\  
  measure(inside(path_image g)) < measure(inside(path_image h))
```

Brunn-Minkowski?

One natural argument is based on the Brunn-Minkowski theorem:

Theorem 3 (Isoperimetric inequality) For any smooth closed hypersurface S in \mathbb{R}^n , we have

$$\left(\frac{\text{Vol}(\Omega)}{b_n} \right)^{\frac{1}{n}} \leq \left(\frac{\text{Area}(S)}{s_{n-1}} \right)^{\frac{1}{n-1}},$$

where Ω is the region enclosed by S .

Proof: Let $S_t = \{x + t\nu(x) : x \in S\}$ be the “parallel” hypersurface, where $\nu(x)$ is the inward unit normal of S at x . For small t , S_t is a smooth hypersurface which bounds a region Ω_t . Let B_t be the open ball with radius t (centered at O). Then it can be seen that $\Omega_t + B_t \subset \Omega$. Therefore by the Brunn-Minkowski inequality (Theorem 2), we have (we’ll write $|\Omega| = \text{Vol}(\Omega)$ and $|S| = \text{Area}(S)$, which shouldn’t cause confusion.)

$$|\Omega| \geq |\Omega_t + B_t| \geq \left(|\Omega_t|^{\frac{1}{n}} + |B_t|^{\frac{1}{n}} \right)^n = \left(|\Omega_t|^{\frac{1}{n}} + b_n^{\frac{1}{n}} t \right)^n.$$

Therefore

$$\begin{aligned} |S| &= \lim_{t \rightarrow 0^+} \frac{|\Omega| - |\Omega_t|}{t} \\ &\geq \lim_{t \rightarrow 0^+} \frac{\left(|\Omega_t|^{\frac{1}{n}} + b_n^{\frac{1}{n}} t \right)^n - |\Omega_t|}{t} \\ &= n|\Omega|^{1-\frac{1}{n}} b_n^{\frac{1}{n}}. \end{aligned}$$

This is equivalent to the isoperimetric inequality by Remark 1. \square

Brunn-Minkowski ... doesn't quite fit

We already have a proof of Brunn-Minkowski in a general setting formalized in HOL Light, so this looks promising:

```
BRUNN_MINKOWSKI_MEASURABLE =  
  |- !s t:real^N->bool.  
    (s = {} <=> t = {}) /\  
    measurable s /\ measurable t /\  
    measurable {x + y | x IN s /\ y IN t}  
    ==> root (dimindex(:N)) (measure {x + y | x IN s /\ y IN t})  
        >= root (dimindex(:N)) (measure s) +  
            root (dimindex(:N)) (measure t)
```

Brunn-Minkowski ... doesn't quite fit

We already have a proof of Brunn-Minkowski in a general setting formalized in HOL Light, so this looks promising:

```
BRUNN_MINKOWSKI_MEASURABLE =  
  |- !s t:real^N->bool.  
    (s = {} <=> t = {}) /\  
    measurable s /\ measurable t /\  
    measurable {x + y | x IN s /\ y IN t}  
    ==> root (dimindex(:N)) (measure {x + y | x IN s /\ y IN t})  
        >= root (dimindex(:N)) (measure s) +  
            root (dimindex(:N)) (measure t)
```

Unfortunately, it doesn't seem easy to relate "length" as a limit of area differences to our "length" of a rectifiable path.

Steiner's hinge argument (informally)

One of Steiner's many proofs of the isoperimetric theorem was based on the “hinge” argument

Consider one of these halves. Suppose it is not a semicircle. Then there will be some point on the boundary where lines drawn from the points on the symmetry line meet at an angle that is not a right angle.

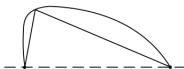


Figure 12.

Think of there being a void inside the triangle and think of the pieces on the sides as glued on. Slide the endpoints along the symmetry line to make the angle a right angle (Figure 13).

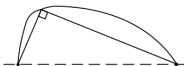


Figure 13.

Blåsjö, Evolution of The Isoperimetric Problem

Existence of maximal curve

So any “maximal area” curve of a given length must be a circle. Steiner famously overlooked the need to actually prove, however that there *is* a “maximal area” curve.

Existence of maximal curve

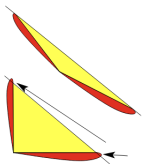
So any “maximal area” curve of a given length must be a circle. Steiner famously overlooked the need to actually prove, however that there *is* a “maximal area” curve.

Using the Arzela-Ascoli theorem we were able to prove in HOL Light that there is a maximal solution.

```
ARZELA_ASCOLI_LIPSCHITZ =  
  |- compact s /\ bounded t /\  
    (!n x. x IN s ==> ~(IMAGE (f n) s INTER t = {})) /\  
    (!n x y. x IN s /\ y IN s ==> norm(f n x - f n y) <= b * norm(x - y))  
  ==> ?g. (!x y. x IN s /\ y IN s ==> norm(g x - g y) <= b * norm(x - y)) /\  
    ?r. (!m n. m < n ==> r m < r n) /\  
      !e. &0 < e  
        ==> ?N. !n:num x. n >= N /\ x IN s  
          ==> norm(f (r n) x - g x) < e
```

The hinge gets stuck

However, we found formalizing Steiner's hinge argument surprisingly fiddly, e.g.

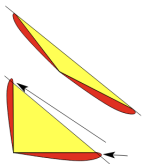


For completeness, we note that for some figures, decreasing $\angle ABC$ to 90° will cause portions of the region to spread across the bisection line L as shown. There are several ways to fix this problem; the details are left as an exercise for the interested reader.

Siegel, "A Historical Review of the Isoperimetric Theorem"

The hinge gets stuck

However, we found formalizing Steiner's hinge argument surprisingly fiddly, e.g.



For completeness, we note that for some figures, decreasing $\angle ABC$ to 90° will cause portions of the region to spread across the bisection line L as shown. There are several ways to fix this problem; the details are left as an exercise for the interested reader.

Siegel, "A Historical Review of the Isoperimetric Theorem"

In the end we gave up and switched to a completely different "analytic" proof following Osserman.

Osserman's analytical proof (1)

1. The classical case: curves in the plane. To begin, consider how one might prove the classical isoperimetric inequality. If C is a simple closed smooth curve given parametrically, then its arc length L can be expressed as

$$L = \int_a^b \sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2} dt. \quad (1.1)$$

The area A enclosed by C can also be expressed as a line integral:

$$A = - \int_C y dx = - \int_a^b y \frac{dx}{dt} dt, \quad (1.2)$$

where the orientation determined by C may be assumed to be the positive one with respect to its interior. A little experimentation reveals that the usual integral inequalities go the wrong way, giving an upper bound on L^2 , and one is forced to the simple artifice of introducing a special parameter in order to eliminate the square root in the integral (1.1). Any multiple of the parameter s of arc length will do. The most convenient is $t = (2\pi/L)s$. Then

Osserman's analytical proof (2)

$$\int_0^{2\pi} \left[\left(\frac{dx}{dt} \right)^2 + \left(\frac{dy}{dt} \right)^2 \right] dt = \int_0^{2\pi} \left(\frac{ds}{dt} \right)^2 dt = \frac{L^2}{2\pi},$$

and

$$\begin{aligned} L^2 - 4\pi A &= 2\pi \int_0^{2\pi} \left[\left(\frac{dx}{dt} \right)^2 + \left(\frac{dy}{dt} \right)^2 + 2y \frac{dx}{dt} \right] dt \\ &= 2\pi \int_0^{2\pi} \left(\frac{dx}{dt} + y \right)^2 dt + 2\pi \int_0^{2\pi} \left[\left(\frac{dy}{dt} \right)^2 - y^2 \right] dt. \quad (1.3) \end{aligned}$$

The first term on the right is obviously nonnegative, and the result will be proved if we can show that

$$\int_0^{2\pi} \left(\frac{dy}{dt} \right)^2 dt \geq \int_0^{2\pi} y^2 dt. \quad (1.4)$$

The inequality (1.4) cannot hold for an arbitrary function $y(t)$, since it fails when $y(t)$ is a nonzero constant. However, one has the following classical result. (For a history of this result, and a discussion of its usual attribution, “Wirtinger’s inequality,” see Mitrinović [1].)

Formalizing Osserman's proof

We need several ingredients:

- ▶ Integral-based formula for length (already formalized in HOL Light)
- ▶ Integral-based formula for area (no usable differential geometry like Green's theorem formalized in HOL Light)
- ▶ Proof of Wirtinger's inequality (none previously formalized but the proof seems not too difficult)

Formalizing Osserman's proof

We need several ingredients:

- ▶ Integral-based formula for length (already formalized in HOL Light)
- ▶ Integral-based formula for area (no usable differential geometry like Green's theorem formalized in HOL Light)
- ▶ Proof of Wirtinger's inequality (none previously formalized but the proof seems not too difficult)

Moreover, if we want to apply this to an arbitrary rectifiable curve, we need to generalize away all the smoothness and differentiability assumptions.

Wirtinger's inequality (informally)

Formalized straight from Hardy, Littlewood and Polya's *Inequalities*:

Another modification of (7.7.2) leads to a more interesting theorem due to Wirtinger^b.

258. *If y has the period 2π , y' is L^2 , and*

$$(7.7.4) \quad \int_0^{2\pi} y dx = 0,$$

then

$$\int_0^{2\pi} y^2 dx < \int_0^{2\pi} y'^2 dx$$

unless

$$y = A \cos x + B \sin x.$$

Wirtinger's inequality (informally)

Formalized straight from Hardy, Littlewood and Polya's *Inequalities*:

Another modification of (7.7.2) leads to a more interesting theorem due to Wirtinger^b.

258. *If y has the period 2π , y' is L^2 , and*

$$(7.7.4) \quad \int_0^{2\pi} y dx = 0,$$

then
$$\int_0^{2\pi} y^2 dx < \int_0^{2\pi} y'^2 dx$$

unless
$$y = A \cos x + B \sin x.$$

H-L-P superficially appear to be talking about derivatives, but really they're *antiderivatives*, so this is strong enough to avoid smoothness, with a little care.

Wirtinger's inequality (formally)

A simple formal version without mentioning derivatives explicitly:

```
WIRTINGER_INEQUALITY =  
  |- (!x. x IN real_interval[&0,&2 * pi]  
      ==> (f' has_real_integral (f x - f(&0))) (real_interval[&0,x])) /\  
    f(&2 * pi) = f(&0) /\  
    (f has_real_integral &0) (real_interval[&0,&2 * pi]) /\  
    (\x. f'(x) pow 2) real_integrable_on real_interval[&0,&2 * pi]  
  ==> (\x. f(x) pow 2) real_integrable_on real_interval[&0,&2 * pi] /\  
    real_integral (real_interval[&0,&2 * pi]) (\x. f(x) pow 2) <=  
    real_integral (real_interval[&0,&2 * pi]) (\x. f'(x) pow 2) /\  
    (real_integral (real_interval[&0,&2 * pi]) (\x. f(x) pow 2) =  
      real_integral (real_interval[&0,&2 * pi]) (\x. f'(x) pow 2)  
      ==> ?c a. !x. x IN real_interval[&0,&2 * pi]  
          ==> f x = c * sin(x - a))
```

Proof was not too bad but needed generalizations of several calculus lemmas like “integration by parts”.

Absolute continuity

The concept of *absolute continuity* is useful in keeping the reasoning general enough, roughly “is an antiderivative”:

```
ABSOLUTE_INTEGRAL_ABSOLUTELY_CONTINUOUS_DERIVATIVE_EQ =  
  |- !f:real^1->real^N f' a b.  
    f' absolutely_integrable_on interval[a,b] /\  
    (!x. x IN interval[a,b]  
      ==> (f' has_integral (f x - f a)) (interval[a,x])) <=>  
    f absolutely_continuous_on interval[a,b] /\  
    ?s. negligible s /\  
      !x. x IN interval [a,b] DIFF s  
        ==> (f has_vector_derivative f' x)  
              (at x within interval[a,b])
```

Absolute continuity

The concept of *absolute continuity* is useful in keeping the reasoning general enough, roughly “is an antiderivative”:

```
ABSOLUTE_INTEGRAL_ABSOLUTELY_CONTINUOUS_DERIVATIVE_EQ =  
|- !f:real^1->real^N f' a b.  
  f' absolutely_integrable_on interval[a,b] /\  
  (!x. x IN interval[a,b]  
    ==> (f' has_integral (f x - f a)) (interval[a,x])) <=>  
  f absolutely_continuous_on interval[a,b] /\  
  ?s. negligible s /\  
    !x. x IN interval [a,b] DIFF s  
    ==> (f has_vector_derivative f' x)  
        (at x within interval[a,b])
```

or alternatively

```
BANACH_ZARECKI =  
|- f absolutely_continuous_on interval[a,b] <=>  
  f continuous_on interval[a,b] /\  
  f has_bounded_variation_on interval[a,b] /\  
  !t. t SUBSET interval[a,b] /\ negligible t ==> negligible(IMAGE f t)
```

All this was originally developed because of completionism.

Keeping the calculus general

A useful lemma following Serrin and Varberg's paper "A general chain rule..."

```
CONVERSE_SARD_1 =  
  |- !(f:real^1->real^1) f' s.  
    (!x. x IN s ==> (f has_vector_derivative f'(x)) (at x within s)) /\  
    negligible(IMAGE f s)  
    ==> negligible {x | x IN s /\ ~(f'(x) = vec 0)}
```

This is used to generalize the chain rule for derivatives and integration by parts to the required setting.

Area via Green's theorem

We prove an area formula for a very *special* shape but with very *general* differentiability assumptions:

GREEN_AREA_THEOREM =

```
| - !(g:real^1->real^2) g' u a b.  
  simple_path g /\ pathstart g = a /\ pathfinish g = a /\  
  b IN path_image g /\ a$1 < b$1 /\ a$2 = b$2 /\  
  dist(a,b) = diameter(path_image g) /\  
  convex(inside(path_image g)) /\  
  g absolutely_continuous_on interval[vec 0,vec 1] /\  
  negligible u /\  
  (!t. t IN interval[vec 0,vec 1] DIFF u  
    ==> (g has_vector_derivative g'(t)) (at t))  
==> (\t. lift(g'(t)$1 * g(t)$2)) absolutely_integrable_on  
  interval[vec 0,vec 1] /\  
  norm(integral (interval[vec 0,vec 1])  
    (\t. lift(g'(t)$1 * g(t)$2))) =  
  measure(inside(path_image g))
```

The overall isoperimetric proof

- ▶ Choose coordinate axes appropriately for the very special case of Green's theorem
- ▶ Reparametrize the curve by arc length (this is Lipschitz and so AC, strong enough to use our lemmas)
- ▶ Follow the analytic proof in Osserman using the general form of Wirtinger.

The final statement

```
ISOPERIMETRIC_THEOREM =  
  |- !L g:real^1->real^2.  
    rectifiable_path g /\  
    simple_path g /\  
    pathfinish g = pathstart g /\  
    path_length g = L  
    ==> measure(inside(path_image g)) <= L pow 2 / (&4 * pi) /\  
      (measure(inside(path_image g)) = L pow 2 / (&4 * pi)  
        ==> ?a r. path_image g = sphere(a,r))
```

The final statement

```
ISOPERIMETRIC_THEOREM =  
  |- !L g:real^1->real^2.  
    rectifiable_path g /\  
    simple_path g /\  
    pathfinish g = pathstart g /\  
    path_length g = L  
    ==> measure(inside(path_image g)) <= L pow 2 / (&4 * pi) /\  
      (measure(inside(path_image g)) = L pow 2 / (&4 * pi)  
        ==> ?a r. path_image g = sphere(a,r))
```

We could actually consider further generalizing by removing hypotheses ...

Retrospective

- ▶ All the basic definitions used in the statement of the theorem existed in the HOL Light libraries; none was developed just for this application.

Retrospective

- ▶ All the basic definitions used in the statement of the theorem existed in the HOL Light libraries; none was developed just for this application.
- ▶ The proof would probably have been much easier if the library contained more differential geometry or more results relating our version of 'length' to other notions.

Retrospective

- ▶ All the basic definitions used in the statement of the theorem existed in the HOL Light libraries; none was developed just for this application.
- ▶ The proof would probably have been much easier if the library contained more differential geometry or more results relating our version of 'length' to other notions.
- ▶ The ingredients used in the proof arose from many sources, with Flyspeck the motivation for much of the background theory, but general interest and completionism contributing too.

Retrospective

- ▶ All the basic definitions used in the statement of the theorem existed in the HOL Light libraries; none was developed just for this application.
- ▶ The proof would probably have been much easier if the library contained more differential geometry or more results relating our version of 'length' to other notions.
- ▶ The ingredients used in the proof arose from many sources, with Flyspeck the motivation for much of the background theory, but general interest and completionism contributing too.
- ▶ As with most non-trivial applications, we found cases where the existing library results (e.g. "integration by parts") could be generalized significantly.

Thank you!