Are Theorem Provers Powerful Enough For Pure Mathematicians? (Formalizing Riemann Integration)

by

Ricky W. Butler
NASA Langley Research Center

http://shemesh.larc.nasa.gov/fm/

October 4, 2001

Outline

1. Definition Of Riemann Integral and Formalization (based upon Maxwell Rosenlicht's classic textbook "Introduction To Analysis")

2. Key Properties

3. Proof of a lemma

4. Thoughts about why PVS theorem prover not yet acceptable to mathematicians

Motivation

- Develop libraries needed for hybrid system analysis
- Explore the question of whether semi-automatic theorem proving could be useful to mathematicians
  - teaching aid
  - proof checking

Riemann Integral: Definition of Partition

Definition: Let $a, b \in \Re, a < b$. By a partition of the closed interval [a, b] is meant a finite sequence of numbers $x_0, x_1, ..., x_N$ such that $a = x_0 < x_1 < x_2 ... < x_N = b$.

```
integral_def[T: TYPE FROM real]: THEORY
BEGIN
 a,b,x: VAR T
 closed_interval(a:T,b:{x:T|a<x}): TYPE = { x | a <= x AND x <= b}

 partition(a:T,b:{x:T|a<x}): TYPE =
           {fs: finite_sequence[closed_interval(a,b)] |
                Let N = length(fs), xx = seq(fs) IN
                   N > 1 AND xx(0) = a AND xx(N-1) = b AND
                    (FORALL (ii: below(N-1)): xx(ii) < xx(ii+1))}
```

NOTE: in prelude we have

```
  finite_sequence: TYPE = [# length: nat, seq: [below[length] -> T] #]
```

Riemann Integral: Definition of Partition (cont.)

The width of this partition is defined to be

$$max\{x_i - x_{i-1} : i = 1, 2, ..., N\}$$

```
width(a:T, b:{x:T|a<x}, P: partition(a,b)): posreal =
          LET xx = seq(P), N = length(P) IN
                   max({ l: real | EXISTS (ii: below(N-1)):
                           l = xx(ii+1) - xx(ii)})
```

- **Note that** `width(a,b,P(a,b))` **must carry the endpoints** `a,b`
- **Note the convenience of** $max\{x_i - x_{i-1} : i = 1, 2, ..., N\}$
- **There is an implicit existential quantifier hidden by traditional notation**

Definition of Riemann Sum

Definition: If f is a real-valued function on $[a, b]$ by a Riemann sum for f corresponding to the given partition is meant a sum

$$\sum_{i=1}^{N} f(x_i')(x_i - x_{i-1})$$

where $x_{i-1} \leq x_i' \leq x_i$ for each $i = 1, 2, ..., N$.

At first one might try

```
x_in(aa:T,bb:{x:T|aa<x}): {t: T | aa <= t AND t <= bb}

Riemann_sum(a:T,b:{x:T|a<x},P:partition(a,b),f:[T->real]): real =
          LET xx = seq(P), N = length(P)-1 IN
          sigma[upto(N)](1,N,(LAMBDA (n: upto(N)):
                     f(x_in(xx(n-1),xx(n)))*(xx(n)-xx(n-1))))
```

Using `sigma` from the `reals` library. But this will not typecheck (unprovable TCC) because the signature of the `sigma` function is:

```
sigma[T: TYPE FROM int]: THEORY
   F: VAR function[T -> real]
   sigma(low, high, F): RECURSIVE real
```

Revised Definition of Riemann Sum

Definition: If f is a real-valued function on $[a,b]$ by a Riemann sum for f corresponding to the given partition is meant a sum

$$\sum_{i=1}^{N} f(x_i')(x_i - x_{i-1})$$

where $x_{i-1} \le x_i' \le x_i$ for each $i = 1, 2, ..., N$.

```
x_in(aa:T,bb:{x:T|aa<x}): {t: T | aa <= t AND t <= bb}

Riemann_sum(a:T,b:{x:T|a<x},P:partition(a,b),f:[T->real]): real =
  LET xx = seq(P), N = length(P)-1 IN
    sigma[upto(N)](1,N,(LAMBDA (n: upto(N)): IF n = 0 THEN 0 ELSE
                   f(x_in(xx(n-1),xx(n)))*(xx(n)-xx(n-1)) ENDIF))
```

or alternatively

```
Riemann_sum_alt: LEMMA a < b IMPLIES FORALL (P: partition(a,b)):
      Riemann_sum(a,b,P,f) =
        LET xx = seq(P), N = length(P)-1 IN
          sigma[below(N)](0,N-1,(LAMBDA (n: below(N)):
                         f(x_in(xx(n),xx(n+1)))*(xx(n+1)-xx(n))))
```

Revised Definition of Riemann Sum: Reflection

Definition: If f is a real-valued function on $[a, b]$ by a Riemann sum for f corresponding to the given partition is meant a sum

$$\sum_{i=1}^{N} f(x'_i)(x_i - x_{i-1})$$

where $x_{i-1} \le x'_i \le x_i$ for each $i = 1, 2, ..., N$.

```
x_in(aa:T,bb:{x:T|aa<x}): {t: T | aa <= t AND t <= bb}

Riemann_sum(a:T,b:{x:T|a<x},P:partition(a,b),f:[T->real]): real =
   LET xx = seq(P), N = length(P)-1 IN
       sigma[upto(N)](1,N,(LAMBDA (n: upto(N)): IF n = 0 THEN 0 ELSE
                      f(x_in(xx(n-1),xx(n)))*(xx(n)-xx(n-1)) ENDIF))
```

- **Is it really appropriate to define the x'_is with `x_in` ?**
- **Should the x'_is be parameters instead?**
- **If so, then we have an arbitrary number of them, so they would have to be in a list.**

Definition of Riemann Integral

Definition: Let $a, b \in \Re, a < b$. Let f be a real-valued function on $[a, b]$. We say that f is **Riemann integrable on [a,b]** if there exists a number $A \in \Re$ such that, for any $\epsilon > 0$, there exists a $\delta > 0$ such that $|S - A| < \epsilon$ whenever S is a Riemann sum for f corresponding to any partition of $[a, b]$ of width less than δ. In this case A is called the **Riemann Integral of f between a and b** and is denoted

$$\int_a^b f(x)dx$$

- For any given ϵ must find a δ and a real number A such that
- No matter how we partition the interval, if the width of that interval is less than δ, then
- if S is the Riemann sum corresponding to that partition
- we have $|S - A| < \epsilon$.

Definition of Riemann Integral

Definition: Let $a, b \in \Re, a < b$. Let f be a real-valued function on $[a, b]$. We say that f is Riemann integrable on [a,b] if there exists a number $A \in \Re$ such that, for any $\epsilon > 0$, there exists a $\delta > 0$ such that $|S - A| < \epsilon$ whenever S is a Riemann sum for f corresponding to any partition of $[a, b]$ of width less than δ. In this case A is called the Riemann Integral of f between a and b and is denoted $\int_a^b f(x)dx$

```
is_integral(a:T,b:{x:T|a<x},f:[T->real],S:real): bool =
            (FORALL (epsi: posreal): (EXISTS (delta: posreal):
                (FORALL (P: partition(a,b)):
                   width(a,b,P) < delta IMPLIES
                       abs(S - Riemann_sum(a,b,P,f)) < epsi)))
```

- **First define this relation then define** `integrable?` **and** `integral`
- **Must first demonstrate uniqueness of the value S.**

Definition of integral

```
A1, A2: VAR real
integral_unique: LEMMA a < b AND is_integral(a,b,f,A1) AND
                          is_integral(a,b,f,A2) IMPLIES A1 = A2


integrable?(a:T,b:{x:T|a<x},f:[T->real]): bool =
                   (EXISTS (S: real): is_integral(a,b,f,S))

integral(a:T,b:{x:T|a<x}, ff: { f | integrable?(a,b,f)} ):
                  {S: real | is_integral(a,b,ff,S)}
```

Definition of integral

```
Integrable?(a:T,b:T,f:[T->real]): bool = (a = b) OR
                              (a < b AND integrable?(a,b,f)) OR
                              (b < a  AND integrable?(b,a,f))

Integrable_funs(a,b): TYPE = { f | Integrable?(a,b,f)}

is_Integral(a:T,b:T,f:[T->real],S:real): bool = (a = b AND S = 0) OR
                            (a < b AND is_integral(a,b,f,S))
                            OR (b < a AND is_integral(b,a,f,-S))

Integral(a:T,b:T,f:Integrable_funs(a,b)): real =
                                     IF a = b THEN 0
                                     ELSIF a < b THEN integral(a,b,f)
                                     ELSE -integral(b,a,f)
                                     ENDIF
```

Sample Properties

```
Integral_sum: LEMMA Integrable?(a,b,f) AND Integrable?(a,b,g) IMPLIES
                       Integrable?(a,b,(LAMBDA x: f(x) + g(x)))
                       AND Integral(a,b,(LAMBDA x: f(x) + g(x))) =
                             Integral(a,b,f) + Integral(a,b,g)


Integral_split: LEMMA Integrable?(a,b,f) AND Integrable?(b,c,f)
                          IMPLIES Integrable?(a,c,f) AND
                 Integral(a,b,f) + Integral(b,c,f) = Integral(a,c,f)


Integral_bounded: LEMMA Integrable?(a,b,f) AND
            (FORALL (x: Closed_interval(a,b)): abs(f(x)) <= M) IMPLIES
               abs(Integral(a,b,f)) <= M*abs(b-a)


fundamental: THEOREM continuous(f) AND
                     (FORALL x: F(x) = Integral(a,x,f))
                IMPLIES derivable(F) AND deriv(F) = f
```

Lemma (Pg 120 Rosenlicht)

Lemma: A real-valued function f on the interval $[a, b]$ is integrable on $[a, b]$ if and only for each $\epsilon > 0$ there exists step functions f_1, f_2 on $[a, b]$ such that

$$f_1(x) \leq f(x) \leq f_2(x) \text{ for each } x \in [a, b]$$

and

$$\int_a^b (f_2(x) - f_1(x))dx < \epsilon$$

```
step_function?(a:T,b:{x:T|a<x},f:[T -> real]): bool
           = (EXISTS (P: partition(a,b)):
              Let N = length(P), xx = seq(P) IN
              (FORALL (ii: below(N-1)): (EXISTS (fv: real):
                  (FORALL (x: open_interval(xx(ii),xx(ii+1))):
                             f(x) = fv))))
```

Theorem (Pg 123 Rosenlicht)

Theorem: If f is s continuous real-valued function on the interval $[a, b]$ then $\int_a^b f(x)dx$ exists.

Proof: We shall prove this theorem by showing that the criterion of the preceding lemma obtains. Since f is uniformly continuous on [a,b], given any $\epsilon > 0$ we can find a δ such that whenever $x, x'' \in [a, b]$ and $|x' - x''| < \delta$ then $|f(x') - f(x'')| < \epsilon/(b - a)$. Choose any partition $x_0, x_1, \ldots x_N$ of $[a, b]$ of width less than δ. For each $i = 1, \ldots, N$ choose $x_i', x_i'' \in [x_{i-1}, x_i]$ such that the restriction of f to $[x_{i-1}, x_i]$ attains a minimum at a_i' and a maximum at x_i''. Define step functions f_1, f_2 on $[a, b]$ by

$$f_1(x) = \begin{cases} f(x_i') & \text{if } x_{i-1} < x < x_i, i = 1, \ldots N \\ f(x) & \text{if } x = x_i, i = 0, 1, \ldots, N \end{cases}$$

$$f_2(x) = \begin{cases} f(x_i'') & \text{if } x_{i-1} < x < x_i, i = 1, \ldots N \\ f(x) & \text{if } x = x_i, i = 0, 1, \ldots, N \end{cases}$$

Then $f_1(x) \leq f(x) \leq f_2(x)$ for all $x \in [a, b]$. Furthermore for each $i = 1, \ldots, N$ we have $|x_i' - x_i''| \leq x_i' - x_i'' < \delta$, so that $|f(x_i') - f(x_i'')| < \epsilon/(b - a)$ and therefore $f_2(x) - f_1(x)\epsilon/(b - a)$ for all $x \in [a, b]$. Therefore

$$\int_a^b (f_2(x) - f_1(x))dx < max\{f_2(x) - f_1(x) : x \in [a, b]\} \cdot (b - a)$$

$$< \frac{\epsilon}{b - a} \cdot (b - a) = \epsilon$$

Formal Proof of This Theorem

- Informal proof is 16 lines in Rosenlicht
- Formal PVS proof trace is 7836 lines long (not counting the auxiliary lemmas and TCCs)
- PVS proof script (i.e. M-x edit-proof) is 417 command lines

WHY THE BIG DIFFERENCE?

The Proof Involves a Sophisticated Construction

$$f_1(x) = \begin{cases} f(x'_i) & \text{if } x_{i-1} < x < x_i, i = 1, ...N \\ f(x) & \text{if } x = x_i, i = 0, 1, ..., N \end{cases}$$

```
min_x(a:T,b:{x:T|a<x}, f: continuous_on(a,b)):
        {mx: T |  a <= mx AND mx <= b AND
                 (FORALL (x: T): a <= x AND x <= b IMPLIES
                                f(mx) <= f(x))}
```

```
fmin(a:T,b:{x:T|a<x},P: partition(a,b), f: continuous_on(a,b)):
      {ff: [T -> real] | LET xx = seq(P) IN
               FORALL (ii : below(length(P)-1)):
       FORALL (x: T): (xx(ii) < x AND x < xx(ii+1) IMPLIES
                        ff(x) = f(min_x(xx(ii),xx(ii+1),f))) AND
                      ((xx(ii) = x OR x = xx(ii+1)) IMPLIES
                        ff(x) = f(x))}
```

Thoughts about min_x

```
min_x(a:T,b:{x:T|a<x}, f: continuous_on(a,b)):
         {mx: T |  a <= mx AND mx <= b AND
                   (FORALL (x: T): a <= x AND x <= b IMPLIES
                                   f(mx) <= f(x))}
```

```
min_x_TCC1: OBLIGATION
  EXISTS (x1:
          [d: [a: T, b: {x: T | a < x}, continuous_on(a, b)] ->
             {mx: T |
                    d`1 <= mx AND
                     mx <= d`2 AND
                      (FORALL (x: T):
                         d`1 <= x AND x <= d`2 IMPLIES
                          d`3(mx) <= d`3(x))}]):
    TRUE;
```

- **Generates existence TCC (PVS generates a particularly ugly one)**
- **Parameters are rolled up into a tuple form (yuk!)**
- **Proof depends upon continuity over a closed interval**

Need Special Induction

Then $f_1(x) \le f(x) \le f_2(x)$

```
{-1}  FORALL (ii: below(length(PP) - 1)):
        FORALL (x: T):
          (seq(PP)(ii) < x AND x < seq(PP)(1 + ii) IMPLIES
            fmin(a!1, b!1, PP, f!1)(x) =
             f!1(min_x[T](seq(PP)(ii), seq(PP)(1 + ii), f!1)))
           AND
           ((seq(PP)(ii) = x OR x = seq(PP)(1 + ii)) IMPLIES
             fmin(a!1, b!1, PP, f!1)(x) = f!1(x))
[-2]  a!1 < b!1
  |-------
[1]   fmin(a!1, b!1, PP, f!1)(xx!1) <= f!1(xx!1)
```

```
   Prop: VAR [T -> bool]
   part_induction: LEMMA  (FORALL (P: partition(a,b)):
                              (FORALL ( x: closed_interval(a,b)):
                           LET xx = seq(P), N = length(P) IN
                   (FORALL (ii : below(N-1)):
                           xx(ii) <= x AND x <= xx(ii+1) IMPLIES
                                Prop(x))
                  IMPLIES Prop(x) ) )
```

Function Domain Restrictions

```
continuous[closed_interval[T](seq(PP)(ii!1), seq(PP)(1 + ii!1))]
       (restrict[T,
                 closed_interval[T](seq(PP)(ii!1), seq(PP)(1 + ii!1)),
                 real]
            (f!1),
        x!1)
```

- `f` **defined from** `[T -> real]`
- `continuous` **over** `[a,b]` **but not necessarily elsewhere**
- `continuous[T](f)` **different from** `continuous[closed_interval(a,b)](f)`

Trivialities Must Be Dealt With

```
[-1]  seq(P!1)(ii!2) < x!1
[-2]  x!1 < seq(P!1)(1 + ii!2)
[-3]  seq(P!1)(ii!1) < x!1
[-4]  x!1 < seq(P!1)(1 + ii!1)
  |-------
[1]   ii!2 = ii!1
```

- **partitions are disjoint**
- **but proof requires an induction**

List of Some of The Problem Areas

- **A partition $a = x_0 < x_1 < x_2... < x_N = b$ must be referenced by strange notation `seq(P)(i)` instead of x_i.**
- **The `sigma` functional is parameterized by the domain: `sigma[nat]` and `sigma[upto[N]]` not interchangeable**
- **Lists must be formalized as functions `[nat -> T]`**
- **Constructs such as $x_0, x_1, ..., x_N$ inevitably lead to inductions, the details of which mathematicians such as Rosenlicht rarely delve into.**
- **Minimums and maximums lead to non-emptyness TCCs that involve unfamiliar syntax, e.g. `proj_1`'s etc.**
- **Restrictions of function domains lead to ugliness involving restrict/extend.**
- **Trivialities must be dealt with via induction proofs**

Left Undone

```
step_function_integrable?: AXIOM a < b AND step_function?(a,b,f)
                                      IMPLIES integrable?(a,b,f)



integral_split: AXIOM a < b AND b < c AND integrable?(a,b,f) AND
                                          integrable?(b,c,f)
                          IMPLIES integrable?(a,c,f) AND
                integral(a,b,f) + integral(b,c,f) = integral(a,c,f)

integrable?_split: AXIOM a < b AND b < c AND
                       integrable?(a, c, f) IMPLIES
                       integrable?(a, b, f) AND integrable?(b, c, f)



a,b: VAR T
unif_cont_interval: AXIOM a < b IMPLIES   % PROVE LATER
                     LET D = {xx:T| a <= xx AND xx <= b} IN
                        continuous(f,D) IMPLIES
                           uniformly_continuous(f,D)
```