Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2013, Article ID 160875, 7 pages
http://dx.doi.org/10.1155/2013/160875

Research Article

The Gauge Integral Theory in HOL4

Zhiping Shi,[1,2] Weiqing Gu,[1] Xiaojuan Li,[1] Yong Guan,[1] Shiwei Ye,[3] Jie Zhang,[4] and Hongxing Wei[5]

[1] *Beijing Engineering Research Center of High Reliable Embedded System, Capital Normal University, Beijing 100048, China*
[2] *State Key Laboratory of Computer Architecture, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China*
[3] *College of Information Science and Engineering, Graduate University of Chinese Academy of Sciences, Beijing 100049, China*
[4] *College of Information Science and Technology, Beijing University of Chemical Technology, Beijing 100029, China*
[5] *School of Mechanical Engineering and Automation, Beijing University of Aeronautics and Astronautics, Beijing 100191, China*

Correspondence should be addressed to Zhiping Shi; shizhiping@gmail.com

Received 6 February 2013; Accepted 27 February 2013

Academic Editor: Xiaoyu Song

The integral is one of the most important foundations for modeling dynamical systems. The gauge integral is a generalization of the Riemann integral and the Lebesgue integral and applies to a much wider class of functions. In this paper, we formalize the operational properties which contain the linearity, monotonicity, integration by parts, the Cauchy-type integrability criterion, and other important theorems of the gauge integral in higher-order logic 4 (HOL4) and then use them to verify an inverting integrator. The formalized theorem library has been accepted by the HOL4 authority and will appear in HOL4 Kananaskis-9.

1. Introduction

In the recent years, hardware and software systems are widely used in safety critical applications like car, highway and air control systems, medical instruments, and so on. The cost of a failure in these systems is unacceptably high, thus making it important to make sure of the correctness of the functions in design. The traditional verification methods, which include simulation and testing, are not sufficient to validate confidence. Formal methods can be helpful in proving the correctness of systems. Theorem proving is one method for performing verification on formal specifications of system models [1]. It allows to mathematically reason about system properties by representing the behavior of a system in logic in a general model. In this way, the specification and implementation are expressed as the general mathematical model so that all the cases are covered when they are proved to be equivalent.

The integral is a mathematical tool to solve many practical problems in geometry, physics, economics, electrical systems, and so on. In order to formalize dynamic systems, some theorem provers have already formalized integral theorem library. The Isabelle/Isar theorem prover has the formalization of the Lebesgue integral [2], and the Isabelle/HOL has the formalization of the gauge Integral [3]. Cruz-Filipe reported a constructive theory of real analysis [4], which includes continuous functions and differential, integral, and transcendental functions in the COQ theorem prover. The PVS theorem prover has the Riemann integral formalized by Butler [5]. Mhamdi et al. [6] formalized the Lebesgue integration in HOL4 in order to formalize statistical properties of continuous random variables. Harrison formalized the gauge integral in HOL light [7]. Although there are the definition of the gauge integral and the fundamental theorem of calculus in HOL4 [7], there are no operation property and other theorems yet.

This paper presents the formalization of the complete gauge integral theory in HOL4 [8], including linearity, inequality, integration by parts, and the Cauchy-type integrability criterion, as well as the formal analysis of an integral circuit based on the formalization. The properties of vectors and matrices are characterized in accordance with linear space properties. In this paper, we use HOL4 notations, and some notations are listed in Table 1.

Table 1: Some HOL4 notations and their semantics.

Meaning	HOL notations	Standard notations
Truth	T	T
Falsity	F	$\perp$
Negation	$\sim t$	$\neg t$
Disjunction	$t1 \vee t2$	$t1 \vee t2$
Conjunction	$t1 \wedge t2$	$t1 \wedge t2$
Implication	$t1 ==> t2$	$t1 \Rightarrow t2$
Equality	$t1 = t2$	$t1 = t2$
$\forall$-quantification	$!x \cdot t$	$\forall x \cdot t$
$\exists$-quantification	$?x \cdot t$	$\exists x \cdot t$
Lambda	$\backslash x \cdot t$	$\lambda x \cdot t$

The rest of the paper is organized as follows. In Section 2, we give an overview of the gauge integral and present the formalization of the properties and theorems in HOL4. In Section 3, the formal analysis of an integral circuit is presented. Section 4 concludes the paper. The definitions and theorems in this paper are described as formalizations in HOL4 and have been verified for correctness using the HOL4 theorem prover.

2. The Gauge Integral in HOL4

There are many ways of formally defining an integral, not all of which are equivalent. The differences exist mostly to deal with differing special cases which may not be integrable under other definitions. The definitions include the Newton integral, the Riemann integral, the Lebesgue integral, and the gauge integral, which had been proposed in different senses. The gauge integral proposed by Kurzweil and Henstock is a generalization of the Riemann integral and the Lebesgue integral, and it is suitable for wider situations [8]. The gauge integral is far simpler than the Lebesgue integral—it is not to be preceded by explanations of sigma-algebras and measures [9] but to be based on the special properties of the closed interval [8]. Harrison made a detailed analysis of advantages of the gauge integral [7].

For any function f, which may be not a derivative, we say that it has the gauge integral I on the interval $[a,b]$ if for any $\varepsilon > 0$, there is a gauge δ such that for any δ-fine division, the usual Riemann-type sum approaches I are closer than ε:

$$\left|\sum_{i=0}^{n} f\left(t_i\right)\left(x_{i+1}-x_i\right)-I\right|<\varepsilon. \quad (1)$$

So, the above reasoning shows that a derivative f' always has the gauge integral $f(b)-f(a)$ over the interval $[a,b]$; that is, the fundamental theorem of calculus holds.

Definition 1 (the gauge integral). Let $f:[a,b] \rightarrow R$ be some function, and let V be some number. We say that V is the gauge integral of f, written $V=\int_a^b f(t)dt$, if for each number $\varepsilon > 0$, there exists a corresponding function $\delta:[a,b] \rightarrow (0,+\infty)$ with the following property: whenever n is a positive integer and $t_0, t_1, t_2, \ldots, t_n$ and $s_1, s_2, \ldots, s_n$ are some numbers satisfying $a=t_0 \leq s_1 \leq t_1 \leq s_2 \leq t_2 \leq \cdots \leq t_{n-1} \leq s_n \leq t_n = b$ and $t_i - t_{i-1} < \delta(s_i)$ for all i, then $|V-\sum_{i=1}^{n} f(s_i)(t_i-t_{i-1})| < \varepsilon$.

Definition 1 is formalized in HOL4 as [7]

```
|- !a b f k.
    Dint (a, b) f k <=>
    !e. 0 < e ==>
       ?g. gauge (\x.a <= x ∧ x <= b) g∧
          !D p. tdiv (a, b) (D, p)∧ fine g (D, p) ==>
             abs (rsum (D, p) f − k) < e,
```

where division (a,b) D denotes a division D on interval $[a,b]$:

division (a,b) D <=>
(D 0 = a)∧?N.(!n.n < N ==> D n < D (SUC n))∧!n.n >= N ==> (D n = b).

tdiv $(a,b)(D,p)$ denotes to get any value between two contiguous dividing points:

tdiv $(a,b)(D,p)$ <=> division (a,b) D∧!n.D n <= p n ∧ p n <= D(SUC n).

The gauge E g indicates that g is a measure over a set E (an interval commonly), formally as

|−!E g. gauge E g <=>!x.E x ==> 0 < g x,

and fine means as follows:

|−!g D p. fine g (D,p) <=>!n.n < dsize D ==> D (SUC n) − D n < g (p n).

dsize D denotes the number of divisions of the interval divided by the division D:

dsize D = @N.!n.n < N ==> D n < D(SUC n))∧!n.n >= N ==> (D n = D N).

In sum, "Dint (a,b) f k" denotes the integral of f on $[a,b]$ is k. Then, we give the definitions of integrable and integral based on Definition 1.

Definition 2 (integrable). Function f is integrable on interval $[a,b]$ means that there exist a number i that satisfy Definition 1.

Definition 2 is formalized in HOL4 as
integrable = |−!a b f. integrable (a,b) f <=>?i. Dint (a,b) f i.

Definition 3 (integral value). A function's integral value is formalized as follows:
integral = |−!a b f. integral (a,b) f = @i. Dint $(a,b) f$ i.
The relations between the definitions are described in Theorems 4 and 5.

Theorem 4 (INTEGRABLE_DINT). *One has*
|−!f a b. *integrable* (a,b) f ==>Dint (a,b) f *(integral* $(a,b) f$*).*

Theorem 5 (DINT_INTEGRAL). *Consider*
|−!f a b i. a <= b ∧ Dint $(a,b) f$ i ==> *(integral* $(a,b) f$ = i*).*

Then, we formalizes the operational properties of the gauge integral [8].

2.1. Linearity of the Gauge Integral. In this subsection, the formalizations of the linear properties are presented after the respective mathematical expressions.

Theorem 6 (DINT_CONST). *The integral of a constant function is computed by:*

$$\int_a^b c dx = c * (b - a). \tag{2}$$

The formalization is as follows:

$$|-!a\,b\,c.\ \text{Dint}\ (a,b)\ (\backslash x.c)\ (c * (b - a)). \tag{3}$$

Theorem 7 (DINT_0). *The integral of zero is zero:*

$$\int_a^b 0 dx = 0. \tag{4}$$

The formalization is as follows:

$$|-!a\,b.\ \text{Dint}\ (a,b)\ (\backslash x.0)\ 0. \tag{5}$$

Theorem 8 (DINT_NEG). *The integral is negated when the function is negated:*

$$\int_a^b f(x)\,dx = i \Longrightarrow \int_a^b (-f(x))\,dx = -i. \tag{6}$$

The formalization is as follows:

$$|-!f\,a\,b\,i.\ \text{Dint}\ (a,b)\ f\ i ==> \ \text{Dint}\ (a,b)\ (\backslash x. - f\ x)\ (-i). \tag{7}$$

Theorem 9 (DINT_CMUL). *The integral of the product of a function multiplied by a constant equals the product of the constant and the integral of the function:*

$$\int_a^b f(x)\,dx = i \Longrightarrow \int_a^b c * f(x)\,dx = c * i. \tag{8}$$

The formalization is as follows:

$$\begin{aligned} &|-!f\,a\,b\,c\,i.\ \text{Dint}\ (a,b)\ f\ i \\ &\quad ==> \ \text{Dint}\ (a,b)\ (\backslash x.c * f\ x)\ (c * i). \end{aligned} \tag{9}$$

Theorem 10 (DINT_ADD). *The integral of the sum of two functions is the sum of the integrals of the two functions:*

$$\begin{aligned} &\int_a^b f(x)\,dx = i \wedge \int_a^b g(x)\,dx = j \\ &\qquad \Longrightarrow \int_a^b (f(x) + g(x))\,dx = i + j. \end{aligned} \tag{10}$$

The formalization is as follows:

$$\begin{aligned} &|-!f\,g\,a\,b\,i\,j.\ \text{Dint}\ (a,b)\ f\ i \wedge \ \text{Dint}\ (a,b)\ g\ j \\ &\quad ==> \ \text{Dint}\ (a,b)\ (\backslash x.\ f\ x + g\ x)\ (i + j). \end{aligned} \tag{11}$$

Theorem 11 (DINT_SUB). *The integral of the difference of two functions is the difference of the integrals of the two functions:*

$$\begin{aligned} &\int_a^b f(x)\,dx = i \wedge \int_a^b g(x)\,dx = j \\ &\qquad \Longrightarrow \int_a^b (f(x) - g(x))\,dx = i - j. \end{aligned} \tag{12}$$

The formalization is as follows:

$$\begin{aligned} &|-!f\,g\,a\,b\,i\,j.\ \text{Dint}\ (a,b)\ f\ i \wedge \ \text{Dint}\ (a,b)\ g\ j \\ &\quad ==> \ \text{Dint}\ (a,b)\ (\backslash x.\ f\ x - g\ x)\ (i - j). \end{aligned} \tag{13}$$

Theorem 12 (DINT_LINEAR). *The integral is linear:*

$$\begin{aligned} &\int_a^b f(x)\,dx = i \wedge \int_a^b g(x)\,dx = j \\ &\qquad \Longrightarrow \int_a^b (m * f(x) + n * g(x))\,dx \\ &\qquad = m * i + n * j. \end{aligned} \tag{14}$$

The formalization is as follows:

$$\begin{aligned} &|-!f\,g\,a\,b\,i\,j.\ \text{Dint}\ (a,b)\ f\ i \wedge \ \text{Dint}\ (a,b)\ g\ j \\ &\quad ==> \ \text{Dint}\ (a,b)\ (\backslash x.\ m * f\ x + n * g\ x)\ (m * i + n * j). \end{aligned} \tag{15}$$

These theorems are proven based on the definition of the gauge integral.

2.2. Inequalities of the Gauge Integral. The three inequalities are formalized in this subsection.

Theorem 13 (upper and lower bounds). *An integrable function f over $[a,b]$ is necessarily bounded on that interval. Thus, there are real numbers m and M so that $m \leq f(x) \leq M$ for all x in $[a,b]$. Since the lower and upper sums of f over $[a,b]$ are therefore bounded by, respectively, $m(b-a)$ and $M(b-a)$, it follows that*

$$m(b-a) \leq \int_a^b f(x)\,dx \leq M(b-a). \tag{16}$$

The formalization is as follows:

INTEGRAL_MVT_LE:
$|-!f\,a\,b.$
$a < b \wedge (!x.\ a <= x \wedge x <= b ==> f$ contl $x) \wedge$
$(!x.\ a <= x \wedge x <= b ==> m <= fx : f\ x <= M) ==>$
$m * (b - a) <=$ integral $(a,b)\ f \wedge$ integral $(a,b) f <= M * (b - a)$.

Theorem 14 (inequalities between functions). *If $f(x) \leq g(x)$ for each x in $[a,b]$, then each of the upper and lower sums of f is bounded above by the upper and lower sums of g, respectively:*

$$\int_a^b f(x)\,dx \leq \int_a^b g(x)\,dx. \tag{17}$$

The formalization is as follows:

```
INTEGRAL_LE:
|−!f g a b i j.
  a <= b ∧ integrable (a, b) f ∧ integrable (a, b)g ∧
  (!x. a <= x ∧ x <= b ==> f x <= g x)==>
  integral (a, b) f <= integral (a, b) g.
DINT_LE:
|−!f g a b i j. a <= b ∧ Dint (a, b)f i ∧ Dint(a, b)g
j ∧
      (!x. a <= x ∧ x <= b ==> f(x) <= g(x))
      ==> i <= j.
```

Theorem 15 (inequality of absolute value). *If f is the gauge-integrable on $[a,b]$, then the same is true for $|f|$ and*

$$\left|\int_a^b f(x)\,dx\right| \leq \int_a^b |f(x)|\,dx. \tag{18}$$

The formalization is as follows:

```
DINT_TRIANGLE:
|−!f a b i j.
  a <= b ∧ Dint(a, b)f i ∧ Dint(a, b)(\x.
abs(f x))j ==>
  abs i <= j.
```

This theorem could be proved by Theorem 14.

2.3. The Integral of the Pointwise Perturbation and the Spike Functions

Theorem 16 (DINT_DELTA). *The integral of the delta function, which equals 1 only at one certain point otherwise keeps zero, is zero:*

$$f(x) = \begin{cases} 1 & x = c \\ 0 & else \end{cases} \Longrightarrow \int_a^b f(x)\,dx = 0. \tag{19}$$

The formalization is as follows:
|−!a b c. Dint (a, b) (\x. if x = c then 1 else 0) 0.

Theorem 17 (DINT_POINT_SPIKE). *The two functions which are equal except at a certain point have same integrals:*

$$\forall x \in [a,b] \wedge x \neq c \Longrightarrow (f(x) = g(x)) \wedge \int_a^b f(x)\,dx = i$$
$$\Longrightarrow \int_a^b g(x)\,dx = i. \tag{20}$$

The formalization is as follows:

```
|−!f g a b c i.
  (!x. a <= x ∧ x <= b ∧ x <> c ==> (f x = g x)) ∧
  Dint(a, b) f i ==> Dint(a, b)g i.
```

This shows that if one changes a function at one point, then its integral does not change.

2.4. Other Important Properties

Theorem 18 (integrable on subinterval). *For all c d. $a \leq c \wedge c \leq d \wedge d \leq b$, if f is integrable over $[a,b]$, then f is integrable over $[c,d]$.*

The formalization is as follows:

```
INTEGRABLE_SUBINTERVAL:
|−!f a b c d. a <= c ∧ c <= d ∧ d <= b∧ integrable
(a, b) f ==> integrable (c, d)f.
```

In order to prove Theorem 18, the following three lemmas need to be proved:

```
INTEGRABLE_SPLIT_SIDES =
  |− ! f a b c.
    a <= c ∧ c <= b∧ integrable (a, b)f ==>
    ?i. ! e. 0 < e ==>
      ?g. gauge (\x. a <= x ∧ x <= b) g∧
        ! d1 p1 d2 p2.
        tdiv(a, c) (d1,p1) ∧ fine g(d1, p1) ∧
        tdiv(c, b) (d2,p2) ∧ fine g(d2, p2) ==>
        abs (rsum(d1, p1)f+rsum (d2, p2)f − i) <
e
INTEGRABLE_SUBINTERVAL_LEFT =
  |− ! f a b c. a <= c ∧ c <= b∧ integrable
(a, b) f ==> integrable (a, c) f
INTEGRABLE_SUBINTERVAL_RIGHT =
  |− ! f a b c. a <= c∧c <= b∧integrable (a, b) f ==>
integrable (c, b) f.
```

The INTEGRABLE_SPLIT_SIDES is used to prove INTEGRABLE_SUBINTERVAL_LEFT and INTEGRABLE_SUBINTERVAL_RIGHT, then the theorem INTEGRABLE_SUBINTERVAL can be proved by the transitivity of real number.

Theorem 19 (additivity of integration on intervals). *If b is any element of $[a,c]$, then*

$$\int_a^b f(x)\,dx + \int_b^c f(x)\,dx = \int_a^c f(x)\,dx. \tag{21}$$

The formalization is as follows:

```
INTEGRAL_COMBINE:
|− !f a b c.
  a <= b ∧ b <= c ∧ integrable (a, c) f ==>
  (integral (a, c) f = integral (a, b) f +
integral (b, c) f).
```

The proof of Theorem 19 is sophisticated. We utilize multiple lemmas shown in Table 2.
The proof is branched based on $a <= b \wedge b <= c$. It is easy in case of $a = b$ or $b = c$. In case $a < b \wedge b < c$, b is the tie point

Table 2: The lemmas proving Theorem 19.

Name of lemma	Description in HOL4
DIVISION_LE_SUC	∀ d a b. division (a, b) d ==> ∀n. d n <= d (SUC n)
DIVISION_MONO_LE	∀ d a b. division (a, b) d ==> ∀m n. m <= n ==> d m <= d n
DIVISION_MONO_LE_SUC	∀ d a b. division (a, b) d ==> ∀n. d n <= d (SUC n)
DIVISION_INTERMEDIATE	∀ d a b c. division (a, b) d ∧ a <= c ∧ c <= b ==> ∃ n. n <= dsize d ∧ d n <= c ∧ c <= d (SUC n)
DIVISION_DSIZE_LE	∀ a b d n. division (a, b) d ∧ (d (SUC n) = d n) ==> dsize d <= n
DIVISION_DSIZE_GE	∀ a b d n. division (a, b) d ∧ d n < d (SUC n) ==> SUC n <= dsize d
DIVISION_DSIZE_EQ	∀ a b d n. division (a, b) d ∧ d n < d (SUC n) ∧ (d (SUC (SUC n)) = d (SUC n)) ==> (dsize d = SUC n)
DIVISION_DSIZE_EQ_ALT	∀ a b d n. division (a, b) d ∧ (d (SUC n) = d n) ∧ (∀i. i < n ==> d i < d (SUC i)) ==> (dsize d = n)

of two measure intervals. It needs the lemmas of Table 1 to prove interval measure and division fine. The proof program consists of over 400 lines of HOL4 code. The proof procedure is described as follows.

In case $a < b \wedge b < c$, the proof goal is extended as follows:

$$\begin{aligned}&\text{abs}\left(\text{sum}\,(0,\text{dsize}\,d)\left(\backslash n.f\left(p\ n\right)*\left(d\left(\text{SUC}\ n\right)-d\ n\right)\right)\right.\\&\qquad\left.-\left(i+j\right)\right)<e.\end{aligned}\tag{22}$$

The proof goal transfers by using the fourth lemma:

$$\begin{aligned}&\text{abs}\left(\text{sum}\,(0,m+n)\left(\backslash n.f\left(p\ n\right)*\left(d\left(\text{SUC}\ n\right)-d\ n\right)\right)\right.\\&\qquad\left.-\left(i+j\right)\right)<e.\end{aligned}\tag{23}$$

This lemma is proven with two cases based on $n = 0$ or $n \neq 0$. In case of $n \neq 0$, the goal is

$$\begin{aligned}&\text{abs}\left(\text{sum}\,(0,m)\left(\backslash n.f\left(p\ n\right)*\left(d\left(\text{SUC}\ n\right)-d\ n\right)\right)\right.\\&\quad+\left(f\left(p\ m\right)*\left(d\left(\text{SUC}\ m\right)-d\ m\right)+\text{sum}\left(m+1,\text{PRE}\ n\right)\right.\\&\quad\times\left.\left.\left(\backslash n.f\left(p\ n\right)*\left(d\left(\text{SUC}\ n\right)-d\ n\right)\right)\right)-\left(i+j\right)\right)<e.\end{aligned}\tag{24}$$

The goal is rewritten by $p\ m = b$:

$$\begin{aligned}&\text{abs}\left(\text{sum}\,(0,m)\left(\backslash n.f\left(p\ n\right)*\left(d\left(\text{SUC}\ n\right)-d\ n\right)\right)\right.\\&\quad+\left(f\ b*\left(d\left(\text{SUC}\ m\right)-d\ m\right)+\text{sum}\left(m+1,\text{PRE}\ n\right)\right.\\&\quad\times\left.\left.\left(\backslash n.f\left(p\ n\right)*\left(d\left(\text{SUC}\ n\right)-d\ n\right)\right)\right)-\left(i+j\right)\right)<e.\end{aligned}\tag{25}$$

Let $s1$ denote sum $(0,m)\,(\backslash n.f(p\ n)*(d(\text{SUC}\ n)-d\ n))$, and let $s2$ denote sum $(m+1,\text{PRE}\ n)\,(\backslash n.f(p\ n)*(d\ (\text{SUC}\ n)-d\ n))$; the simplized goal is as follows:

$$\begin{aligned}&\text{abs}\left(s1+f\ b*\left(b-d\ m\right)-i\right)\\&\quad<\frac{e}{2}\wedge\text{abs}\left(s2+f\ b*\left(d\left(\text{SUC}\ m\right)-b\right)-j\right)<\frac{e}{2}.\end{aligned}\tag{26}$$

For abs $(s1 + f\ b * (b - d\ m) - i) < e/2$, we prove it based on $d\ m = b$ and $d\ m \neq b$. Similarly, for abs $(s2 + f\ b * (d(\text{SUC}\ m) - b) - j) < e/2$, we prove it based on the cases $d\ (\text{SUC}\ m) = b$ or $d(\text{SUC}m) \neq b$, then the goal is proved.

Theorem 20 (the Cauchy-type integrability criterion). *Let $f : [a,b] \rightarrow \mathbb{R}$. Then, f is integrable over $[a,b]$ if and only if for every $\varepsilon > 0$, there is a gauge γ on $[a,b]$ such that if $D_1, D_2 \ll \gamma$, then $|S(f,D_1)-S(f,D_2)| < \varepsilon$, where $S(f,D)$ is a Riemann sum, and D_1, D_2 are partitions of $[a,b]$.*

The formalization is as follows:

```
INTEGRABLE_CAUCHY:
|- !f a b.
   integrable (a, b) f <=>
   !e. 0 < e ==>
      ?g. gauge (\x. a <= x ∧ x <= b) g ∧
         !d1 p1 d2 p2.
         tdiv(a, b) (d1, p1) ∧ fine      g(d1, p1)      ∧
tdiv(a, b) (d2, p2) ∧ fine g (d2, p2) ==>
         abs (rsum(d1, p1) f − rsum(d2, p2) f) < e.
```

The Cauchy criterion indicates that an integrable function is always convergent for any division on the interval.

First of all, we should prove that a function for any gauge over the set is δ-fine; we formalized the lemma as GAUGE_MIN_FINITE:

```
|- !s gs m.
   (!m. m <= n ==> gauge s (gs m))==>
   ?g.
      gauge s g ∧
      !d p. fine (d, p)  ==> !m. m  <=  n  ==> fine
(gs m) (d, p).
```

Theorem 21 (limit theorem). *Let $f : [a,b] \rightarrow \mathbb{R}$ and assume that for every $\varepsilon > 0$, there exists an integrable function $g : [a,b] \rightarrow \mathbb{R}$ such that $|f-g| \leq \varepsilon$ on $[a,b]$. Then, f is integrable over $[a,b]$.*

```
val SUMMING_INTEGRATOR = store_thm("SUMMING_INTEGRATOR",
"!x. 0<=x ==> (integral(0, x) (\t. (m * cos t) + (n * sin t)) = m * sin x + n *(cos 0 − cos x))",
RW_TAC std_ss[] THEN REWRITE_TAC[integral] THEN
SELECT_ELIM_TAC THEN CONJ_TAC THENL
  [EXISTS_TAC"m * sin x + n * (cos 0 − cos x)" THEN
  MATCH_MP_TAC DINT_LINEAR THEN CONJ_TAC THENL
  [SUBGOAL_THEN"sin x = sin x − sin 0"ASSUME_TAC THENL
      [SIMP_TAC std_ss[SIN_0] THEN REAL_ARITH_TAC, ONCE_ASM_REWRITE_TAC[]] THEN
  MATCH_MP_TAC FTC1 THEN RW_TAC std_ss[] THEN
      ASM_SIMP_TAC arith_ss[DIFF_SIN], ALL_TAC] THEN
  SUBGOAL_THEN"cos 0 − cos x = −cos x − cos 0"ASSUME_TAC THENL
  [REWRITE_TAC[REAL_SUB_NEG2], ALL_TAC] THEN
  ONCE_ASM_REWRITE_TAC[] THEN HO_MATCH_MP_TAC FTC1 THEN
  ASM_SIMP_TAC std_ss[DIFF_NEG_COS],ALL_TAC] THEN
RW_TAC std_ss[] THEN MATCH_MP_TAC DINT_UNIQ THEN
MAP_EVERY EXISTS_TAC["0:real","x:real",
                    "(\t. (m * cos t) + (n * sin t)):real->real"] THEN
ASM_REWRITE_TAC[] THEN MATCH_MP_TAC DINT_LINEAR THEN
CONJ_TAC THENL
[SUBGOAL_THEN "sin x = sin x − sin 0"ASSUME_TAC THENL
  [SIMP_TAC std_ss[SIN_0] THEN REAL_ARITH_TAC,
  ONCE_ASM_REWRITE_TAC[] THEN MATCH_MP_TAC FTC1 THEN
      RW_TAC std_ss[] THEN ASM_SIMP_TAC arith_ss[DIFF_SIN]], ALL_TAC] THEN
SUBGOAL_THEN"cos 0 − cos x = −cos x − cos 0"ASSUME_TAC THENL
  [REWRITE_TAC[REAL_SUB_NEG2], ONCE_ASM_REWRITE_TAC[]] THEN
HO_MATCH_MP_TAC FTC1 THEN ASM_SIMP_TAC std_ss[DIFF_NEG_COS]);
```

ALGORITHM 1: The formalization and proof of SUMMING_INTEGRATOR.

The formalization is as follows:

INTEGRABLE_LIMIT:

|−!*f a b*.

(!*e*. 0 < *e* ==>

?*g*. (!*x*. *a* <= *x* ∧ *x* <= *b* ==> abs(*f x* − *g x*) <= *e*) ∧ integrable(*a*, *b*)*g*) ==>

integrable (*a*, *b*) *f*.

In order to make the proof easier, we proved the RSUM_DIFF_BOUND at first:

|−!*a b d p e f g*.

tdiv(*a*, *b*) (*d*, *p*) ∧

(!*x*. *a* <= *x* ∧ *x* <= *b* ==> abs(*f x* − *g x*) <= *e*) ==>

abs (rsum(*d*, *p*)*f* − rsum(*d*, *p*)*g*) <= *e* ∗ (*b* − *a*).

Theorem 22 (integrability of continuous functions). *If $f : [a,b] \to \mathbb{R}$ is continuous, then f is integrable over $[a,b]$.*

The formalization is as follows:

INTEGRABLE_CONTINUOUS:

|−!*f a b*. (!*x*. *a* <= *x* ∧ *x* <= *b* ==> *f* contl *x*) ==> integrable (*a*, *b*) *f*.

To prove Theorem 22, we first prove the uniform continuity theorem.

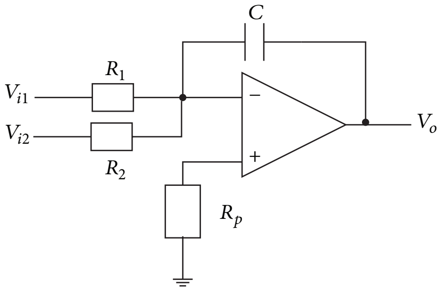


FIGURE 1: The summing inverting circuit.

If $f : [a,b] \to \mathbb{R}$ is continuous, f is uniformly continuous. And then, the result is given by that the uniformly continuous functions are integrable. The uniform continuity theorem is formalized as follows:

CONT_UNIFORM:

|−!*f a b*.

a <= *b* ∧ (!*x*. *a* <= *x* ∧ *x* <= *b* ==> *f* contl *x*)==>

!*e*. 0 < *e* ==>

?*d*. 0 < *d* ∧

!*x y*. *a* <= *x* ∧ *x* <= *b* ∧ *a* <= *y* ∧ *y* <= *b* ∧ abs(*x* − *y*) < *d* ==>

abs (*f x* − *f y*) < *e*.

3. Verifying a Summing Inverting Integrator

In order to illustrate the usefulness of the proposed approach, we use our formalization to analyze a summing integrator. Integration circuits are widely used in electronic circuits; they are often used for waveform transformation, amplifier offset voltage elimination, integral compensation in feedback control, and so on. In this section, we use the formalization above to verify a summing inverting integrator. Figure 1 shows the basic summing inverting integral circuit.

The relation between output and input voltage can be present as the following formula:

$$v_o(x) = -\frac{1}{C}\int_0^x \left[\frac{v_{i1}(t)}{R_1} + \frac{v_{i2}(t)}{R_2}\right] dt. \tag{27}$$

We assumed the integral constant $-1/R_1C = m$, $-1/R_2C = n$, then formula 1 can be simplified as the following formula:

$$v_0(x) = \int_0^x (m * v_{i1}(t) + n * v_{i2}(t))\, dt. \tag{28}$$

When $V_{i1}(t) = \cos t$, $V_{i2}(t) = \sin t$, we can get

$$\begin{aligned} V_o(x) &= \int_0^x (m * \cos t + n * \sin t)\, dt \\ &= m * \sin x + n * (\cos 0 - \cos x). \end{aligned} \tag{29}$$

Formula (29) can be formalized in HOL4 as follows:

```
SUMMING_INTEGRATOR:
|-!x. 0 <= x ==> (integral(0, x) (\t.(m * cos t) + (n *
sin t)) = m * sin x + n * (cos 0 - cos x)).
```

The detailed formalization and proof are shown in Algorithm 1.

In this proof, we employ the linear property of integral DINT_LINEAR to divide the integral of the addition of two functions into the addition of two integrals of the two functions; then we prove the two integrals, respectively. For instantiating the input variable V_{i1} and V_{i2}, the derivative of negative cosine is proved in advance:

$$\frac{d}{dt}(-\cos t)\bigg|_{t=x} = \sin x, \tag{30}$$

```
val DIFF_NEG_COS = store_thm("DIFF_NEG_
COS"),
"!x. ((\t.- cos t) diffl sin(x)) (x)",
GEN_TAC THEN SUBGOAL_THEN"sin x = - sin x
" ASSUME_TAC THENL
[REWRITE_TAC[REAL_NEGNEG],ALL_TAC]
THEN
ONCE_ASM_REWRITE_TAC[] THEN
MATCH_MP_TAC DIFF_NEG THEN REWRITE_
TAC[DIFF_COS]).
```

4. Conclusion

In this paper, we presented a higher-order logic formalization of the gauge integral. The major properties of the gauge integral, including the linearity, boundedness, monotonicity, integration by parts, and Cauchy-type integrability criterion, were formalized and proven in HOL4, and then a formal proving of an inverting integrator was presented. The proposed integral theorem library has been accepted by HOL4 authority and will appear in HOL4 Kananaskis-9.

Acknowledgments

The authors thank Professor Jin Shengzhen and Dr. John Harrison for their helpful suggestions and thank Dr. Michael Norrish for reviewing their gauge integral theorem library. This work was supported by the International Cooperation Program on Science and Technology (2010DFB10930 and 2011DFG13000), the National Natural Science Foundation of China (60873006, 61070049, 61170304, and 61104035), the Natural Science Foundation of the City of Beijing (4122017), the S&R Key Program of the Beijing Municipal Education Commission (KZ201210028036), the Open Project Program of State Key Laboratory of Computer Architecture, and the Open Project Program of Guangxi Key Laboratory of Trusted Software.

References

[1] C. Kern and M. R. Greenstreet:, "Formal verification in hardware design: a survey," *ACM Transactions on Design Automation of Electronic Systems*, vol. 4, no. 2, pp. 123–193, 1999.

[2] Stefan Richter, "Formalizing integration theory with an application to probabilistic algorithms," in *Proceedings of the 17th International Conference on Theorem Proving in Higher Order Logics (TPHOLs '04)*, K. Slind, A. Bunker, and G. Gepalakrishnan, Eds., vol. 3223 of *Lecture Notes in Computer Science*, pp. 271–286, Springer, Park City, Utah, USA, September 2004.

[3] J. D. Fleuriot, "On the mechanization of real analysis in Isabelle/HOL," in *Theorem Proving in Higher Order Logics*, pp. 145–161, 2000.

[4] L. Cruz-Filipe, *Constructive real analysis: a type-theoretical formalization and applications [Ph.D. thesis]*, University of Nijmegen, 2004.

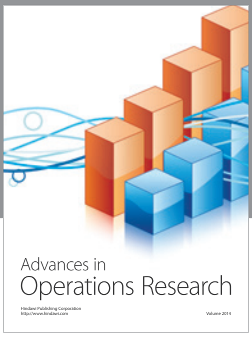
[5] R. W. Butler, "Formalization of the integral calculus in the PVS theorem prover," *Journal of Formalized Reasoning*, vol. 2, no. 1, pp. 1–26, 2009.

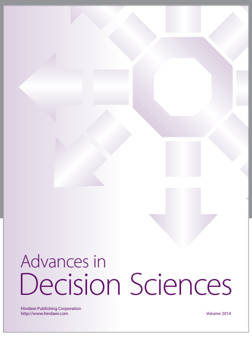
[6] T. Mhamdi, O. Hasan, and S. Tahar, "On the formalization of the Lebesgue integration theory in HOL," in *Interacitve Theorem Proving*, vol. 6172 of *Lecture Notes in Computer Science*, pp. 387–402, Springer, 2010.

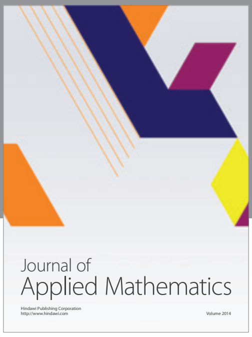
[7] J. Harrison, *Theorem Proving with the Real Numbers*, Springer, Heidelberg, Germany, 1998.

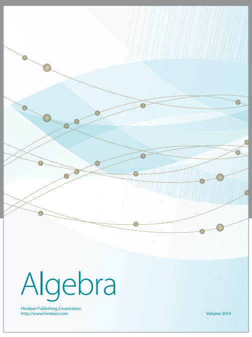
[8] C. Swartz, *Introduction to Gauge Integrals*, World Scientific, Singapore, 2001.

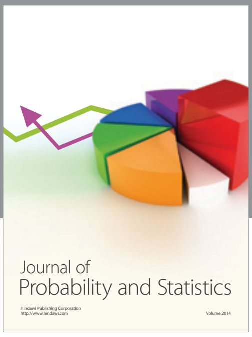
[9] R. A. Gordon, *The Integrals of Lebesgue, Denjoy, Perron, and Henstock*, vol. 4 of *Graduate Studies in Mathematics*, American Mathematical Society, Providence, RI, USA, 1994.


Advances in
Operations Research

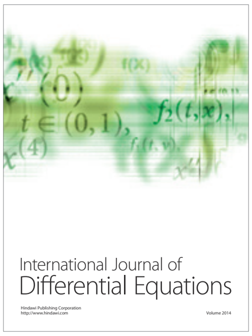

Advances in
Decision Sciences


Journal of
Applied Mathematics

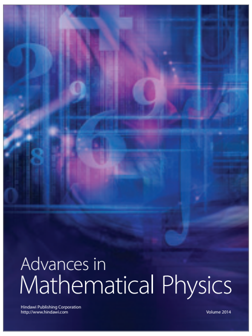

Algebra

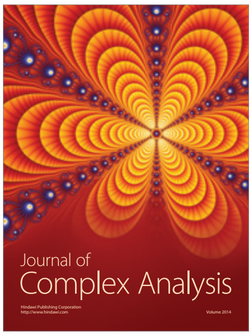

Journal of
Probability and Statistics

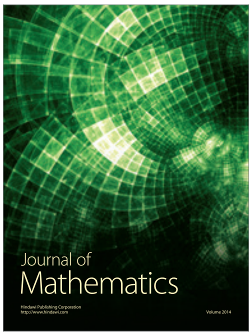
The Scientific
World Journal

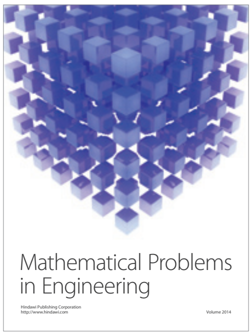

International Journal of
Differential Equations

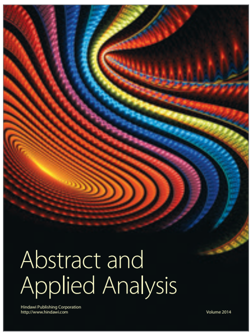
International Journal of
Combinatorics

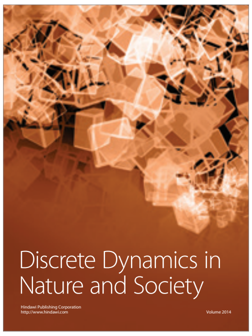

Advances in
Mathematical Physics

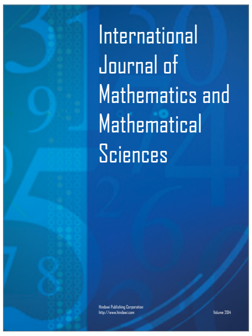

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

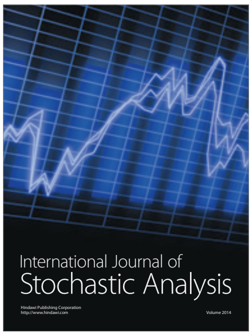

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization