Gauge积分在HOL4中的形式化

谷伟卿[1] 施智平[1] 关 永[1] 张 杰[2] 赵春娜[1] 叶世伟[3]
(首都师范大学信息工程学院高可靠嵌入式系统技术北京市工程研究中心 北京 100048)[1]
(北京化工大学信息科学与技术学院 北京 100029)[2]
(中国科学院研究生院信息科学与工程学院 北京 100049)[3]

摘 要 积分是许多数学理论的基础,如实数分析、信号与系统中微分方程的求解等等。Gauge积分是黎曼积分在闭区间上的推广,应用更加方便。将Gauge积分的运算性质在HOL4(Higher-Order Logic 4)中形式化,包括积分的线性运算性质、积分不等式、分部积分、积分分裂定理、子区间的可积性、对特殊函数的积分的形式化及积分极限定理、柯西可积准则,并根据相关性质对反相积分器进行了验证。

关键词 形式化验证,定理证明,Gauge积分,HOL4,积分器
中图法分类号 TP301.2 **文献标识码** A

Formalization of Gauge Integration Theory in HOL4

GU Wei-qing[1] SHI Zhi-ping[1] GUAN Yong[1] ZHANG Jie[2] ZHAO Chun-na[1] YE Shi-wei[3]
(Beijing Engineering Research Center of High Reliable Embedded System, College of Information Engineering, Capital Normal University, Beijing 100048, China)[1]
(College of Information Science & Technology, Beijing University of Chemical Technology, Beijing 100029, China)[2]
(College of Information Science and Engineering, Graduate University of Chinese Academy of Sciences, Beijing 100049, China)[3]

Abstract Integral is one of the most important foundations in many subjects, such as real analysis, the differential equations in signals and systems and so on. Gauge integral is a generalization of the Riemann integral in which some situations are more useful than the Lebesgue integral. This paper formalized the operational properties which contain the linearity, ordering properties, integration by parts, the integral split theorem, integrability on a subinterval, integrability of special functions and limit theorem, cauchy-type integrability criterion of gauge integral in higher-order-logic 4 (HOL4), and then used them to verify an inverting integrator.

Keywords Formal verification, Theorem proving, Gauge integral, HOL4, Integrator

1 引言

软硬件系统广泛用于高铁、航空控制系统、医疗设备及工业控制系统中。这些系统的设计错误会带来巨大的人身财产损失,所以对其功能设计的正确性验证越来越受到重视。传统的验证方法包括模拟、测试和仿真,它们都是基于测试例方法,因而都是不完备的。

形式化验证根据某些形式规范或属性,使用数学的方法证明系统的正确性或非正确性,包括等价性验证、模型检测和定理证明[1]。其中定理证明用数学方法表达系统的规范和性质,从逻辑上判断设计的正确性,是最为严格和规范的方法,其结论的可信度也最高。定理证明系统基于已有的推理规则、公理和定理对要验证的系统进行建模和推理,定理证明系统包含的理论库越多,其建模和推理能力就越强。

积分是解决许多实际问题的数学工具,在几何、物理、经济等领域都有着非常广泛的应用,比如在几何学中用来求解平面图形的面积、平面曲线的弧长、旋转体的体积等,在物理学中可用来求变力沿直线做功、液体的侧压力、两物体之间的引力、求平均值和均方根,在经济中已知边际函数求总函数在某个范围的改变量。此外,积分在许多电路系统中也有重要应用,如在模拟控制系统中最常用的PID控制,它将偏差的比例(P)、积分(I)和微分(D)通过线性组合构成控制量,对被控对象进行控制。

本文第2节介绍相关工作;第3节介绍Gauge积分,及如何在HOL4中对积分的运算性质和相关定理进行形式化证明,包括积分的线性性质、积分不等式、分部积分法等性质及积分柯西可积准则等定理;第4节介绍积分器电路的形式化验证;最后总结全文。

到稿日期:2012-05-11 返修日期:2012-08-21 本文受国际科技合作计划(2010DFB10930,2011DFG13000),国家自然科学基金项目(61070049,61170304,61104035),北京市自然科学基金项目资助。

谷伟卿(1987—),女,硕士生,主要研究方向为定理证明、形式化验证;**施智平**(1974—),男,博士,副研究员,主要研究方向为定理证明、形式化验证、基于内容的图像/视频检索、机器学习、人工智能,E-mail:shizhiping@gmail.com;**关 永**(1966—),男,博士,教授,主要研究方向为定理证明、形式化验证、电子系统健康状态预测、高可靠嵌入式系统与智能信息处理。

2 相关工作

积分的应用非常广泛，许多定理证明验证系统已经实现了积分的形式化定理库。Isabelle/Isar 定理证明器中有勒贝格积分的定理库[2]，Isabelle/HOL 中有 Gauge 积分定理库[3]。L. Cruz-Filipe 在其博士论文中提到在 Coq 中建立了实数的结构化理论[4]，其中包括连续函数、微分、积分和超越函数。Ricky W. Butler 在 PVS 定理证明器中实现了黎曼积分的形式化[5]。John Harrison 在 HOL Light 中对 Gauge 积分的定义、运算性质等做了较完整的形式化。剑桥大学的 HOL4 系统中有勒贝格积分的形式化，但其主要用于概率中积分的计算，并且其概念是定义在测度的概念上，所以用勒贝格积分对一般的函数进行计算会比较复杂。HOL4 定理证明器中虽然有 Gauge 积分的定义[6]、积分的唯一性和微积分基本定理(Ⅰ)，但没有给出其他性质及定理的形式化。

积分的定义形式有多种，如牛顿积分、黎曼积分、勒贝格积分等。Gauge 积分最先由 Kurzweil 提出，但在后来的发展中，尤其是证明勒贝格型的收敛定理时，主要由 Henstock 完成，并称为“广义的黎曼积分”或“Kurzweil-Henstock gauge 积分”。Gauge 积分比勒贝格积分更加具有一般性[7]。Gauge 积分的定义比勒贝格积分的定义简单，因为它不需要先解释 $\sum$ 代数和测度，它的简单源于充分利用了区间 $[a,b]$ 的特性，这并不是所有测度空间共有的属性[8]。Harrison[6] 曾详细介绍了 Gauge 积分相比于其他积分的优势。

本文在 HOL4 中已有的 Gauge 积分定义基础上给出完整的 Gauge 积分形式化理论。HOL4 是 HOL 系统发展的最新版本，集成了之前版本的所有优点，拥有丰富的定理库，且在软硬件验证[11]及通信协议[9,10,12]的验证等方面都取得了令人瞩目的成果。

3 积分在 HOL4 中的形式化

Gauge 积分是黎曼积分和勒贝格积分在闭区间上的推广与拓展，且能够清楚地表达微分和积分的关系，即对所有 $x\in[a,b]$，f 都有导数 $f'(x)$ 使得微积分基本定理式(1)成立。

$$\int_a^b f'(x)\mathrm{d}x = f(b)-f(a) \tag{1}$$

其他定义形式都存在一些函数无法满足微积分基本定理的情况。

Gauge 积分的具体定义[7]为：P 是区间 $[a,b]$ 上给定的一个标签分割，用式(2)表示：

$$a=u_0<u_1<\cdots<u_n=b, t_i\in[u_{i-1},u_i] \tag{2}$$

一个正函数 $\delta:[a,b]\to(0,\infty)$ 为一个测度，当 $\forall i.\ t_i-\delta(t_i)<u_{i-1}\leqslant u_i<t_i+\delta(t_i)$ 时，称 P 是 δ 精细的。对一个标签分割 P 和一个 $[a,b]$ 上的实函数 f，定义其黎曼并用式(3)表示为：

$$\sum_P f=\sum_{i=1}^{n}(u_i-u_{i-1})f(t_i) \tag{3}$$

对给定的函数 $f:[a,b]\to R$，I 是一个确定的实数，若对任意给定的正数 ϵ 存在一个测度 δ，使得对 $[a,b]$ 上任意 δ 精细的分割 P 有式(4)成立，

$$\left|\sum_P f-I\right|<\varepsilon \tag{4}$$

则称函数 f 在 $[a,b]$ 上是 Gauge 可积的。

HOL4 中已有 Gauge 积分的形式化定义[6]，形如式(5)：

$$\int_a^b f(x)\mathrm{d}x = k \tag{5}$$

的形式化表示为 $Dint(a,b)\,f\,k$，意思是定义 f 在区间 $[a,b]$ 上的积分是 k，具体定义形式如下：

```
Dint (a,b) f k=
∀e. 0 < e==>
  ∃g. gauge (λx. a <=x∧x <=b) g∧
    ∀D p. tdiv (a,b) (D,p)∧fine g(D,p)==>
      abs (rsum (D,p) f−k)<e:thm
```

其中：

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

表示 division(a,b)D 为区间 $[a,b]$ 上的一个分割 D。

tdiv(a,b)(D,p)<=>division(a,b)D∧∀n. D n<=p n∧p n<=D(SUCn)

表示在相邻的两个分割点之间任取一值 $p\,n$。

dsize D=@N.(∀n. n<N==>D n<D(SUCn))∧∀n. n>=N==>(D n=D N)

表示分割 D 将区间分割为 N 份。

Gauge 和 fine 表示为：g 为在一个集合(在实际中一般是区间)E 上的一个测度值，形式化如下：

|−∀E g. gauge E g<=>∀x. E x==>0<g x

|−∀g D p. fine g(D,p)<=>∀n. n<dsizeD==>D(SUC n)−D n<g(p n)

我们通过该定义首先给出可积分和积分值两个定义。

定义 1(可积分)　函数若在闭区间上可积，则等价于存在一个数为该函数在该闭区间上的积分值：

integrable=|− ∀a b f. integrable (a,b) f <=> ∃i. Dint (a,b) f i

定义 2(积分值)

integral=|−∀a b f. integral(a,b)f=@ i. Dint(a,b)f i

对在区间 $[a,b]$ 上任意可积函数 f 都存在一个积分值 $\int_a^b f(x)\mathrm{d}x$，使得式(6)成立。

$$\left|\sum_{i=1}^{n} f(\xi_i)\Delta x_i-\int_a^b f(x)\mathrm{d}x\right|<e \tag{6}$$

下面证明几种定义之间的关系。

定理 1(INTEGRABLE_DINT)

|−∀f a b. integrable (a,b) f==> Dint (a,b) f (integral (a,b) f)

定理 2)DINT_INTEGRAL)

|−∀f a b i. a <=b∧Dint (a,b) f i==> (integral (a,b) f=i)

通过这些定义对积分的运算性质进行形式化，如表 1 所列。

接下来证明积分分裂定理，性质描述如下。

性质 1　f 在 $[a,c]$ 上可积⇔$\forall b\in(a,c)$，f 在 $[a,b]$ 与 $[b,c]$ 上都可积，且

$$\int_a^b f(x)\mathrm{d}x+\int_b^c f(x)\mathrm{d}x=\int_a^c f(x)\mathrm{d}x \tag{7}$$

形式化如下：

DINT_COMBINE=

|- ∀ f a b c i j.

a<=b∧b<=c∧Dint (a,b) f i∧Dint(b,c)f j==>Dint(a,c)f(i+j)

表1 积分的运算性质

积分运算性质	HOL4 形式化
对常数的积分 $\int_a^b c\,dx = c*(b-a)$	∀a b c. Dint (a,b) (λx. c) (c * (b−a))
对0积分等于0 $\int_a^b 0\,dx = 0$	∀a b. Dint (a,b) (λx. 0) 0
$\int_a^b f(x)dx = i \Rightarrow \int_a^b (-f(x))dx = -i$	∀f a b i. Dint (a,b) f i==> Dint (a,b) (λ x. −f x) (−i)
$\int_a^b f(x)dx = i \Rightarrow \int_a^b c*f(x)dx = c*i$	∀f a b c i. Dint (a,b) f i==> Dint (a,b) (λ x. c * f x) (c * i)
$\int_a^b f(x)dx = i \wedge \int_a^b g(x)dx = j \Rightarrow \int_a^b (f(x)+g(x))dx = i+j$	∀f g a b i j. Dint (a,b) f i ∧ Dint (a,b) g j==> Dint (a,b) (λ x. f x+g x) (i+j)
$\int_a^b f(x)dx = i \wedge \int_a^b g(x)dx = j \Rightarrow \int_a^b (f(x)-g(x))dx = i-j$	∀f g a b i j. Dint (a,b) f i /\ Dint (a,b) g j==> Dint (a,b) (λ x. f x − g x) (i − j)
$\int_a^b f(x)dx = i \wedge \int_a^b g(x)dx = j \Rightarrow \int_a^b (m*f(x)+n*g(x))dx = m*i+n*j$	∀f g a b i j. Dint (a,b) f i ∧ Dint (a,b) g j==> Dint (a,b) (λ x. m * f x +n * g x) (m * i+n * j)
∀x∈[a,b] 且 f(x)、g(x) 在[a,b]上均可积，若 f(x)≤g(x)⇒ $\int_a^b f(x)dx \leqslant \int_a^b g(x)dx$	∀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
$\lvert \int_a^b f(x)dx \rvert \leqslant \int_a^b \lvert f(x) \rvert dx$	∀f a b i j. a<=b∧Dint (a,b) f i ∧ Dint (a,b) (λ x. abs (f x)) j==> abs i <=j
∀x∈[a,b]有 f(x)=g(x)⇒ $\int_a^b f(x)dx = \int_a^b g(x)dx$	∀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)
分部积分法：若 f(x)，g(x)为[a,b]上的连续可微函数，则有定积分分部积分公式 $\int_a^b f(x)g'(x)dx = f(b)*g(b) - f(a)*g(a) - \int_a^b f'(x)g(x)dx$	∀f g f' g' a b. a<=b ∧ (∀x. a<=x ∧ x<=b==> (f diffl f' x) x) ∧(∀ x. a<=x ∧ x<=b==> (g diffl g' x) x)==> Dint (a,b) (λx. f'x * g x+f x * g' x) (f b * g b−f a * g a)

积分分裂定理的证明非常复杂，需要很多引理来辅助证明，表2是需要事先证明的一些区间分割的性质。

在对这条性质进行证明时，需对已知条件 $a<=b \wedge b<=c$ 分类证明，当 $a=b$ 或 $b=c$ 时，证明过程比较简单。证明当 $a<b$ 且 $b<c$ 时，点 b 是连接两个测度区间的连接点，在对 b 点所在的区间测度及分割精细度证明时，需要用到以上的性质。由于此性质证明代码超过400行，不在此展示具体证明过程。证明过程描述如下。

当 $a<b$ 且 $b<c$ 时，将目标按定理展开得：

abs (sum (0,dsize d) (λn. f (p n) * (d (SUC n)−d n))− (i+j))<e

用 DIVISION_INTERMEDIATE 将目标转化为

abs (sum (0,m+n) (λn. f (p n) * (d (SUC n)−d n)) − (i+j))<e

首先，对 $n=0$ 和 $n\neq 0$ 两种情况分别进行证明。当 $n\neq 0$ 时，将目标改写为

abs (sum (0,m) (λn. f (p n) * (d (SUC n)−d n))+ (f (p m) * (d (SUC m)−d m)+sum (m+1,PRE n) (λn. f (p n) * (d (SUC n)−d n)))−(i+j))<e

证明 $p\,m=b$，证明目标改写为：

abs (sum (0,m) (λn. f (p n) * (d (SUC n)−d n))+ (f b * (d (SUC m) −d m)+sum (m+1,PRE n) (λn. f (p n) * (d (SUC n)−d n)))− (i+j))<e

用符号 s1 表示 sum (0,m) (λn. f (p n) * (d (SUC n) −d n))，用符号 s2 表示 sum (m+1,PRE n) (λn. f (p n) * (d (SUC n) −d n))。将证明目标化简为：

abs (s1+f b * (b−d m) −i) < e / 2 ∧ abs (s2+f b * (d (SUC m) − b) − j)<e/2

对不等式 abs (s1+f b * (b − d m) −i)<e/2 分别证明 $d\,m=b$ 与 $d\,m\neq b$ 的情况。同理，对 abs (s2+f b * (d (SUC m) −b) − j)<e/2 分别证明 d(SUC m)=b 与 d(SUC m)≠b 的情况，目标得证。

表2 区间分割相关的性质

引理名称	HOL4 表述形式
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)

性质2 对特殊函数的积分

DINT_DELTA_LEFT=|- ∀a b. Dint (a,b) (λx. if x=a then 1 else 0) 0

DINT_DELTA_RIGHT=|- ∀a b. Dint (a,b) (λx. if x=b then 1 else 0) 0

DINT_DELTA=|- ∀a b c. Dint (a,b) (λx. if x=c then 1 else 0) 0

DINT_POINT_SPIKE=

|- ∀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

性质3 子区间的可积性

INTEGRABLE_SUBINTERVAL=

|- ∀f a b c d. a <=c ∧ c <=d ∧ d <=b ∧ integrable (a,b) f==> integrable (c,d) f

在证明此性质之前，需要先证明

```
INTEGRABLE_SPLIT_SIDES=
  |- ∀f a b c.
    a <=c ∧ c <=b ∧ integrable (a,b) f==>
    ∃i. ∀e. 0 < e==>
      ∃g. gauge (λx. 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
```

定理 3(柯西积分准则)　一个可积函数对在该区间上的任意一种分割形式都收敛。

```
INTEGRABLE_CAUCHY:
∀f a b. integrable(a,b) f <=>
    ∀e. &0 < e
      ==> ∃g. gauge (λx. 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
```

定理 4(极限定理)

```
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
```

4　应用

积分电路的应用非常广泛，可以用于波形变换、放大电路失调电压的消除及反馈控制中的积分补偿等场合。

本节运用积分形式化定理库验证反向积分器的性质。标准反相积分电路如图 1 所示。

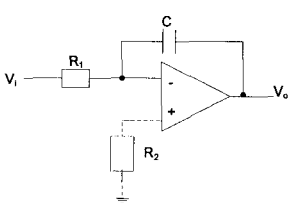

图 1　标准反相积分电路

图 1 所示的标准反相积分电路中，输入电压与输出电压满足积分的关系式(8)：

$$V_o(x)=-\frac{1}{R_1C}\int_0^x V_i(t)\mathrm{d}t \tag{8}$$

假设积分常数 $R_1C=1$，公式化简为：

$$V_o(x)=-\int_0^x V_i(t)\mathrm{d}t \tag{9}$$

当 $V_i(t)=\sin t$ 时，有

$$V_o(x)=-\int_0^x \sin t\mathrm{d}t=\cos x-\cos 0 \tag{10}$$

这一性质在 HOL4 中的形式化为：

INTEGRAL_NEG_SIN=|- ∀x. 0 <=x==> (integral (0,x) (λt. −sin t)=cosx−cos0)

证明过程如下：

```
val INTEGRAL_NEG_SIN=store_thm("INTEGRAL_NEG_
SIN",
  "! x. 0 <=x==> (integral(0,x) (\t. (−sin t))=cos x
−cos 0)"
  REPEAT STRIP_TAC THEN REWRITE_TAC[integral]
THEN
  SELECT_ELIM_TAC THEN CONJ_TAC THENL
  [EXISTS_TAC"cos x −cos 0" THEN
    HO_MATCH_MP_TAC FTC1 THEN
    ASM_SIMP_TAC arith_ss[DIFF_COS],
  RW_TAC std_ss[] THEN MATCH_MP_TAC DINT_
UNIQ THEN
  MAP_EVERY EXISTS_TAC["0:real","x:real",
    "(\t. −sin t):real->real"] THEN
  ASM_REWRITE_TAC[] THEN MATCH_MP_TAC
FTC1 THEN
  RW_TAC std_ss[] THEN ASM_SIMP_TAC arith_ss
[DIFF_COS]]);
```

当输入电压 $V_i(t)=-\cos t$ 时，有式(11)

$$V_o(x)=\int_0^x \cos t\mathrm{d}t=\sin x \tag{11}$$

在 HOL4 中的形式化表示为：

INTEGRAL_COS=|- ∀x. 0 <=x==> (integral (0,x) cos=sinx)

证明过程如下：

```
val INTEGRAL_COS=store_thm("INTEGRAL_COS",
  "! x. 0 <=x==> (integral(0,x) cos=sin x)",
  REPEAT STRIP_TAC THEN REWRITE_TAC[integral]
THEN
  SELECT_ELIM_TAC THEN CONJ_TAC THENL
  [EXISTS_TAC"sin x−sin 0" THEN MATCH_MP_TAC
   FTC1 THEN ASM_SIMP_TAC arith_ss[DIFF_SIN],
  RW_TAC std_ss[] THEN MATCH_MP_TAC DINT_
UNIQ THEN
  MAP_EVERY EXISTS_TAC["0:real","x:real","cos:re-
al->real"]
  THEN ASM_REWRITE_TAC[] THEN
SUBGOAL_THEN" sin x= sin x− sin 0" ASSUME_TAC
THENL
  [SIMP_TAC std_ss[SIN_0] THEN
  REAL_ARITH_TAC,ALL_TAC] THEN
  ONCE_ASM_REWRITE_TAC[] THEN MATCH_MP_
TAC FTC1 THEN RW_TAC std_ss[] THEN ASM_SIMP_
TAC arith_ss[DIFF_SIN]]);
```

(下转第 228 页)

其时间窗口不符合任何一辆车的时间窗口，因此将其排除；乘客 30 号搭载距离比较长，搭载需求从站点 6 至站点 61(见表 6)，同时需要跨越多辆车的运行区域，某一辆车如果搭乘该乘客会使得总的花费大幅度提高，导致该乘客不能搭乘。

图 4、图 5 是通过实验运行得到的 17 组解，通过运行迭代，得到最后的车辆-乘客路线总花费从最初的 30991 下降到 29773，搭乘率从一开始的 82.8%上升至 96.6%。

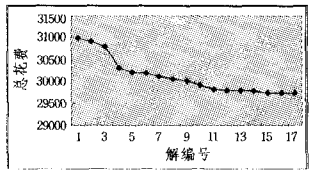

图 4　总花费

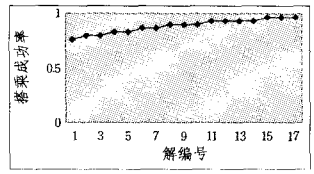

图 5　搭载成功率

由于乘客 29 的时间窗口不符合要求，因此本文在计算搭乘成功率时取底数为 30−1=29。

另外，乘客 30 的搭乘需求要跨越多个车辆运行区域，由于本文未涉及换乘概念，任何一辆车搭载之后都会大幅增加总花费，导致没有搭乘成功，最终只有 28 名乘客成功搭乘。最后 3 组解由于结果相同导致程序终止，经分析，符合实验要求，将最后 3 组解(3 组解相同)作为最优解输出。

结束语　本文通过详细的多车辆模型构建、相对贴近实际的实验及分析对目前关于车辆合乘匹配问题研究中存在的模型单一、适用性低等特点进行了改进，通过吸引粒子群算法结合先验聚类相关思想实现车辆-乘客之间的匹配、排序，同时通过匹配再优化策略对得到的结果进行再优化，避免了因为初次误匹配对后期实验结果产生重大影响。实验结果表明，该算法能以较高的效率和搭载成功率求解车辆合乘匹配问题。

由于针对车辆合乘问题的研究比较少，关于该问题的基础数据也比较少，因此在本文中基础数据生成过程需要较长时间，下一步将现实中的数据用于实验效果或许会更好。同时，根据实验结果，如果某乘客的搭载过程需要跨越多辆车的运行区域，则在考虑总花费的情况下会使得该需求长时间搭载不成功，此时可以考虑增加换乘概念，通过多辆车来接力搭乘该乘客。

参 考 文 献

[1] Lauri H. An adaptive insertion algorithm for the single-vehicle dial-a-ride problem with narrow time windows[J]. European Journal of Operational Research, 2011, 209(1): 11-22

[2] Cordeau J-F, Laporte G. The dial-a-ride problem: models and algorithms[J]. Ann Oper Res, 2007, 4(1): 29-46

[3] 李相勇. 车辆路径问题模型及算法研究[D]. 上海：上海交通大学，2007

[4] 段凤华. 带软时间窗约束的开放式车辆路径问题及其应用[D]. 长沙：中南大学，2009

[5] Kennedy J, Eberhart R. Particle swarm optimization[A]// Proc IEEE Int Conf on Neural Networks[C]. Perth, 1995: 1942-1948

[6] 谢晓锋，等. 微粒群算法综述[J]. 控制与决策，2003，18(2)：129-134

[7] 魏明，靳文舟. 求解车辆路径问题的离散粒子群算法[J]. 计算机科学，2010，37(4)：187-191

[8] 蒋忠中，汪定伟. 物流配送车辆路径优化的模糊规划模型与算法[J]. 系统仿真学报，2006，18(11)：3301-3306

[9] 刘云忠，宣慧玉. 车辆路径问题的模型及算法研究综述[J]. 管理工程学报，2005，19(1)：124-130

[10] 李琳，等. 改进的蚁群算法求解带时间窗的车辆路径问题[J]. 控制与决策，2010，25(9)：1379-1383

[11] 黄敏芳. 物流配送车辆路径方案的智能生成方法研究[D]. 大连：大连理工大学，2008

[12] 吴耀华，张念志. 带时间窗车辆路径问题的改进粒子群算法研究[J]. 计算机工程与应用，2010，46(15)：230-234

(上接第 194 页)

结束语　本文基于高阶逻辑定理证明器 HOL4，实现了 Gauge 积分的运算性质和相关定理的形式化，以反相积分器的形式化验证为例证明了本文提出的定理库的有效性。本文的积分定理库可以在 HOL4 中直接加载使用，它为使用 HOL4 对积分相关的系统进行形式化分析和验证奠定了基础。

参 考 文 献

[1] 韩俊刚，杜慧敏. 数字硬件的形式化验证[M]. 北京：北京大学出版社，2001

[2] Richter S. Formalizing integration theory, with an application to probabilistic algorithms [D]. Technische Universitat Munchen, Department of Informatics, Germany, 2003

[3] Fleuriot J D. On the mechanization of real analysis in isabelle/hol[C]// Theorem Proving in Higher Order Logics: 13th International Conference, TPHOLs 2000, Lecture Notes in Computer Science. volume 1869, 2000

[4] Cruz-Filipe L. Constructive Real Analysis: a Type-Theoretical Formalization and Applications [D]. University of Nijmegen, April 2004

[5] Butler R W. Formalization of the Integral Calculus in the PVS Theorem Prover [J]. Journal of Formalized Reasoning, 2009, 2(1): 1-26

[6] Harrison J. Theorem Proving with the Real Numbers [R]. Technical Report number 408. University of Cambridge Computer Laboratory, December 1996

[7] Henstock-Kurzweil integral [EB/OL]. http://en.wikipedia.org/wiki/Henstock%E2%80%93Kurzweil_integral

[8] Gordon R A. The Integrals of Lebesgue, Denjoy, Perron, and Henstock [M]. American Mathematical Society, 1994: 150-169

[9] Abdullah N, Akbarpour B, Tahar S. Error Analysis and Verification of an IEEE 802.11 OFDM Modem using Theorem Proving [J]. Electronic Notes in Theoretical Computer Science, Elsevier B. V. Pub., 2009, 242(2): 3-30

[10] Abdullah A N M. Formal Analysis and Verification of an OFDM Modem Design [D]. Department of Electrical and Computer Engineering, Concordia University, Montreal, Quebec, Canada, February 2006

[11] Akbarpour B. Modeling and Verification of DSP Designs in HOL [D]. Department of Electrical and Computer Engineering, Concordia University, Montreal, Quebec, Canada, April 2005

[12] 李黎明，关永，吴敏华，等. 运用定理证明的形式化方法验证 SpaceWire 编码电路[J]. 小型微型计算机系统，2011，30(6)：1372-1376