连续傅里叶变换基础理论的高阶逻辑形式化

吕兴利[1] 施智平[1] 李晓娟[1] 关 永[1] 叶世伟[2] 张 杰[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]
(中国科学院研究生院信息科学与工程学院 北京 100049)[2]
(北京化工大学信息科学与技术学院 北京 100029)[3]

摘 要 连续傅里叶变换(CFT)在数学和工程技术领域都有着广泛应用。利用高阶逻辑定理证明器HOL4,实现了对连续傅里叶变换定义及其常用运算性质的形式化,包括线性、频移、反转性、积分、时域一阶微分及高阶微分运算性质,为采用形式化方法分析相关系统奠定了基础。最后利用定理证明的方法对电阻电感电容(RLC)串联谐振电路的频率响应特性进行了验证,说明了CFT形式化的初步应用。

关键词 形式化方法,定理证明,连续傅里叶变换,HOL4,频率响应
中图法分类号 TP301.2 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.4.004

Higher-order Logic Formalization of Basic Theory of Continuous Fourier Transform

LV Xing-li[1] SHI Zhi-ping[1] LI Xiao-juan[1] GUAN Yong[1] YE Shi-wei[2] ZHANG Jie[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 and Engineering, Graduate University of Chinese Academy of Sciences, Beijing 100049, China)[2]
(College of Information Science & Technology, Beijing University of Chemical Technology, Beijing 100029, China)[3]

Abstract Continuous Fourier transform (CFT) is widely used in the fields of mathematics and engineering. The definition of CFT and its operational properties were formalized in the higher-order logic theorem prover HOL4, including linearity, frequency shifting, reversion, integration, first-order differention and higher-order differention, which lays the foundation for analyzing related systems by formal methods. Finally, the frequency response of resistance inductance capacitance(RLC) series resonant circuit was verified by the theorem proving method, which illustrates a preliminary application of formalized CFT.

Keywords Formal methods, Theorem proving, Continuous Fourier transform, HOL4, Frequency response

1 引言

随着计算机技术及其应用的飞速发展,人们设计的系统日益复杂化。如何保证这些复杂系统的正确性已是一个亟需解决的问题,尤其是在航空航天、高铁、医疗等一些安全性要求较高的领域,微小的错误都可能给人们的生命和财产造成巨大的威胁。

形式化验证是保证系统正确性的一条十分重要的途径,它建立在严格完备的数学基础上,采用精确语义的数学推理方法,克服了传统验证技术如模拟、仿真、测试等不能对复杂系统进行穷尽测试的缺点[1]。形式化验证技术在高可信软硬件系统中,正发挥着越来越重要的作用,关注度日益提高。形式化验证技术分为两种方法:模型检验、定理证明。其中定理证明是指将系统的设计规范或性质以及所设计的实际系统分别表示成数学逻辑表达式,并运用数学定理来证明这两个逻辑表达式之间是否存在蕴含或等价的关系,证明过程主要借助于定理证明器。HOL4[2,3]是目前最常用的定理证明器之一,应用非常广泛,在软硬件验证[4,5]和通信协议验证[6,7]方面已经取得了令人瞩目的成果。

在工程数学中,为了把复杂的运算转换为较简单的运算,人们通常采用变换的方法来达到目的[8]。连续傅里叶变换[9,10](Continuous Fourier Transform, CFT)是一个特殊的积分变换,它能把满足一定条件的某函数类A表示成以指数函数为核函数的另一函数类B[8],而指数函数是微分算子的特征函数,从而使得CFT不仅可以把时域的微分运算变换为频域的乘积运算,函数在时域的卷积变为函数在频域的乘积,

到稿日期:2014-05-30 返修日期:2014-08-06 本文受国际科技合作计划(2010DFB10930,2011DFG13000),国家自然科学基金项目(60873006,61070049,61170304,61104035,61373034,61303014),北京市自然科学基金暨北京市教委重点项目(4122017,KZ201210028036),北京市优秀人才培养项目,北京市属高校青年拔尖人才培育计划资助。

吕兴利(1989—),女,硕士生,主要研究方向为形式化验证;施智平(1974—),男,博士,副研究员,CCF会员,主要研究方向为形式化验证与视觉信息处理,E-mail:shizhiping@gmail.com;李晓娟(1968—),女,博士,教授,主要研究方向为形式化验证、计算机网络;关 永(1966—),男,博士,教授,博士生导师,主要研究方向为形式化验证、高可靠嵌入式系统;叶世伟(1968—),男,博士,副教授,主要研究方向为智能信息处理;张 杰(1967—),女,硕士,副教授,主要研究方向为形式化验证。

而且使得 CFT 是分析函数光滑性的强有力工具，这些固有的特性注定了 CFT 在数学和工程技术中的应用越来越广泛。但是，由于 CFT 的应用存在一定的约束条件，而在工程应用中人们常常对函数是否满足这些条件不加以判断，便直接应用 CFT 的相关性质，因此很多情况下仅是进行 CFT 的形式演算，然后将得到的结果作为中间结果进行进一步处理，最后看最终的结果能否满足需求。这样做的后果是：有时得到的结果是正确的，而有时是错误的。如何从严格数学意义上保证应用 CFT 结果的正确性，而不是寄希望于不确定的可能性上，这就需要对 CFT 进行严格的逻辑形式化。目前没有文献讨论关于 CFT 的形式化理论，本文基于定理证明器 HOL4 实现连续傅里叶变换定义及其常用运算性质的形式化，包括线性、频移、反转性、积分和一阶微分及高阶微分运算性质，为采用形式化方法分析相关系统奠定基础；最后利用定理证明的方法对电阻电感电容(RLC)串联谐振电路的频率响应特性进行了验证，说明本文 CFT 定理库的应用。本文工作主要基于 HOL4 中的 realTheory 库[12]、limTheory 库、integration 库[13]、GAMMA 函数库[14]等。文中如无特别说明，傅里叶变换均指连续傅里叶变换。

本文第 2 节对傅里叶变换的定义进行形式化；第 3 节利用傅里叶变换的定义对傅里叶变换的相关性质进行形式化；第 4 节对 RLC 串联谐振电路的频率响应进行验证；最后总结全文。

2 傅里叶变换定义的形式化

满足一定条件的非周期信号 $f(t)$ 可以使用傅里叶变换公式将其表示为复指数函数的连续和，傅里叶变换公式如下所示：

$$F(\omega)=\mathscr{F}[f(t)]=\int_{-\infty}^{\infty} f(t)\mathrm{e}^{-j\omega t}\,\mathrm{d}t \tag{1}$$

式(1)称为 $f(t)$ 的正变换，也称分析公式，该公式中的广义积分是柯西主值意义下的积分，即 $\int_{-\infty}^{\infty} f(t)\,\mathrm{d}t=\lim_{b\to\infty}\int_{-b}^{b} f(t)\,\mathrm{d}t$，因此傅里叶变换可重新定义为：

$$F(\omega)=\lim_{b\to\infty}\int_{-b}^{b} f(t)\mathrm{e}^{-i\omega t}\,\mathrm{d}t \tag{2}$$

式中，傅里叶积分是一个关于复变函数的积分，为了对傅里叶变换的定义进行形式化，要先对复变函数的积分进行形式化。

定义 1 complex_integral_def

```
|- ∀a b f. complex_integral (a,b) f = (integral (a,b) (RE o f), integral (a,b) (IM o f))
```

其中，a,b 为实数，f 是 $R\to C$ 的函数，RE 的返回值是复数的实部，IM 的返回值是复数的虚部。该定义将复变函数的积分转化成了其对应的实部和虚部两个实变函数的积分，而关于实变函数的积分在 HOL4 中已经有相当完善的定理库，为我们后续证明傅里叶变换的性质及一些引理提供了方便。

根据式(2)及上面复变函数积分的定义，对傅里叶变换的定义进行形式化：

定义 2 CFT_def

```
|- ∀omega f.
   CFT omega f  <=>
   (lim(λb. RE(complex_integral (-&b,&b) (λt. f t * exp (i * (-omega * t))))),
   lim (λb. IM(complex_integral (-&b,&b) (λt. f t * exp (i * (-omega * t))))))
```

其中，lim 的返回值是当 $b\to\infty$ 时函数的极限，该定义的返回值是关于 omega 的复变函数，且为了便于推广，该定义中 f 的类型是 $R\to C$ 的函数。

3 傅里叶变换性质的形式化

本节将对傅里叶变换的一些重要性质进行形式化证明，验证傅里叶变换定义的正确性，便于用形式化方法分析实际的物理系统，如通信系统、控制系统等。

以下所有性质的证明，都以 $f(t)$ 的傅里叶变换存在为前提，即 $\mathscr{F}[f(t)]=F(\omega)$。根据复变函数的欧拉公式，式(2)中的被积函数 $f(t)\mathrm{e}^{-i\omega t}=f(t)\cos\omega t-if(t)\sin\omega t$，因此如果函数 $f(t)$ 的傅里叶变换存在，则等价于实部 $f(t)\cos\omega t$ 和虚部 $f(t)$ 分别在正负无穷上可积且收敛。傅里叶变换存在的形式化定义如下：

定义 3 CFT_EXISTS_def

```
|- ∀f.
   CFT_EXISTS f <=> ∀omega. (∀b. integrable (-&b,&b) (λt. f t * cos (omega * t)) ∧ integrable (-&b,&b) (λt. -f t * sin (omega * t))) ∧ (∃l. (λb. integral (-&b,&b) (λt. f t * cos (omega * t))) --> l) ∧ ∃k. (λb. integral (-&b,&b) (λt. -f t * sin (omega * t))) --> k
```

为了后续证明的需要，根据傅里叶变换存在的定义，可以证明下面的引理。

引理 1(CFT_EXISTS_CMUL) 若函数 $f(t)$ 的傅里叶变换存在，则任意乘以一个实数 c 后其傅里叶变换仍存在。

```
|- ∀f c. CFT_EXISTS f ==> CFT_EXISTS (λt. c * f t)
```

引理 2(CFT_EXISTS_ADD) 若函数 $f(t)$ 和 $g(t)$ 的傅里叶变换存在，则 $f(t)+g(t)$ 的傅里叶变换也存在。

```
|- ∀f g. CFT_EXISTS f ∧ CFT_EXISTS g ==> CFT_EXISTS (λt. f t+g t)
```

3.1 线性性质

线性性质是傅里叶变换最常用的性质之一，它表明：

$$\mathscr{F}[mf_1(t)+nf_2(t)]=m\mathscr{F}[f_1(t)]+n\mathscr{F}[f_2(t)] \tag{3}$$

其中，m 和 n 均为常实数，这个性质包含齐次性和可加性，为了简化证明过程，首先分别给出齐次性和可加性引理，然后给出线性性质的形式化。

引理 3(CFT_Homogeneous_Property) 齐次性表明若 $f(t)$ 乘以常实数 m，则其傅里叶变换也乘以 m，即 $\mathscr{F}[mf(t)]=m\mathscr{F}[f(t)]$。

```
|- ∀f m. CFT_EXISTS f ==> (CFT omega (λt. complex_of_real (m * f t)) = m * CFT omega (λt. complex_of_real (f t)))
```

引理 4(CFT_Additive_Property) 可加性即为几个函数和的傅里叶变换等于各个函数傅里叶变换的和，即

$$\mathscr{F}[f_1(t)+f_2(t)]=\mathscr{F}[f_1(t)]+\mathscr{F}[f_2(t)]$$

```
|- ∀f1 f2. CFT_EXISTS f1 ∧ CFT_EXISTS f2 ==> (CFT omega (λt. complex_of_real (f1 t+f2 t)) = CFT omega (λt. complex_of_real (f1 t))+CFT omega (λt. complex_of_real (f2 t)))
```

这两个引理的证明主要用到傅里叶变换的定义以及积分和极限的运算性质。线性性质的形式化如下：

性质 1 CFT_Linear_Property

|- ∀ *f1 f2 m n*

CFT_EXISTS f1 ∧ *CFT_EXISTS f2* ==>

(*CFT omega* (λt. *complex_of_real* ((*m* * *f1*(*t*)) + (*n* * *f2*(*t*)))) = *m* * *CFT omega* (λt. *complex_of_real*(*f1*(*t*))) + *n* * *CFT*(*omega*) (λt. *complex_of_real*(*f2*(*t*))))

证明过程大致为利用 SUBGOAL 策略先证明一个子目标即函数 $f_1(t)$和 $f_2(t)$乘以一个常实数后其傅里叶变换存在，利用 ASM_SIMP_TAC 策略重写假设条件和引理 1 即可使子目标得证，最后利用 RW_TAC 策略重写引理 3 和引理 4 便可使最终目标得证。

3.2 反转性质

函数 $f(t)$在时域反转，其傅里叶变换也反转，即

$$\mathcal{F}[f(-t)]=F(-\omega) \tag{4}$$

函数可以使用换元积分法求出其积分值。用 $t=-x$ 把原来的变量 t 代换成新变量 x 时，积分限也要换成相应于新变量 x 的积分限，不难发现此时变量 x 对应的积分上限小于下限，在这种情况下现有的积分库中的定理不能直接使用，因为按定积分的定义，记号 $\int_a^b f(t)\,dt$ 只有当 $a<b$ 时才有意义，而当 $a=b$ 时或 $a>b$ 时没有意义，但为了方便，一般有 2 个规定：

规定 1　当 $a=b$ 时，令 $\int_a^a f(t)dt=0$；

规定 2　当 $a>b$ 时，令 $\int_a^b f(t)dt=-\int_b^a f(t)dt$。

规定 1 在 HOL4 中已有证明，这里不再详细叙述，对规定 2 进行如下的形式化：

定义 4 INTEGRAL_BOUND_SYM

|- ∀ *a b f*.

INTEGRAL_BOUND_SYM (*a*,*b*) *f* <=>

if a≤*b then integral* (*a*,*b*) *f* = *integral* (*a*,*b*) *f*

else integral (*a*,*b*) *f* = *integral* (*b*,*a*) (λt. −*f t*)

接下来的难点就是对换元积分法的证明，它可以表述为：若函数 f 在$[a,b]$可积，g 在$[c,d]$上严格单调且连续可微，且满足

$$g(c)=a,g(d)=b,a\leqslant g(t)\leqslant b,t\in[c,d]$$

则有定积分换元公式 $\int_a^b f(t)dx=\int_a^b f(g(t))g'(t)dt$，设 $F(x)$是 $f(x)$在$[a,b]$上的一个原函数[15]。其形式化如下：

定理 1 INTEGRATION_BY_SUBST

|- ∀ *F f g g' a b c d*. *a*≤*b* ∧ *integrable* (*a*,*b*) *f* ∧ (∀ *x*. *a*≤*x* ∧ *x*≤*b* ==> (*F diffl f x*) *x*) ∧ (∀ *t*. *c*≤*t* ∧ *t*≤*d* ∨ *d*≤*t* ∧ *t*≤*c* ==> (*g diffl g' t*) *t* ∧ *a*≤*gt* ∧ *gt*≤*b* ∧ *contmono g*) ∧ (*gc*=*a*) ∧ (*gd*=*b*) ∧ (∀ *a b f*. *INTEGRAL_BOUND_SYM* (*a*,*b*) *f*) ==> (*integral* (*a*,*b*) *f* = *integral* (*c*,*d*) (λt. *f* (*g t*) * *g' t*))

在对这条性质进行证明时，需要将 c 和 d 之间大小关系分为 $d<c$ 和 $c\leqslant d$ 两种情况进行讨论。当 $d<c$ 时，用定义 4 交换积分上下限。这两种情况的证明主要借助复合函数的求导法则 DIFF_CHAIN、积分库中的牛顿莱布尼兹公式 FTC1 及积分的一些运算性质，再结合一系列的数学推导就可使目标得证。

为了便于反转性质的证明，利用换元积分法证明一个引理，其数学表达式为 $\int_a^b f(-t)dt=\int_{-b}^{-a} f(t)dt$，形式化如下：

引理 5 CFT_Reversion_lemma

|- ∀ *a b f H*.

a≤*b* ∧ *integrable* (*a*,*b*) (λt. *f* (−*t*)) ∧ *integrable* (−*b*,−*a*) (λt. *f t*) ∧ (∀ *a b f*. *INTEGRAL_BOUND_SYM* (*a*,*b*) *f*) ∧ (∀ *x*. −*b*≤*x* ∧ *x*≤−*a* ==> (*H diffl f x*) *x*) ==> (*integral* (*a*,*b*) (λt. *f* (−*t*)) = *integral* (−*b*,−*a*) (λt. *f t*))

对傅里叶变换的反转性质进行如下的形式化：

性质 2 CFT_Reversion

|- ∀ *omega f*.

CFT_EXISTS f ∧ *CFT_EXISTS* (λt. *f* (−*t*)) ∧ (∀ *x*. (*H1 diffl* (λt. *f t* * cos (*omega* * *t*)) *x*) *x* ∧ (*H2 diffl* (λt. *f t* * sin (*omega* * *t*)) *x*) *x*) ∧ (∀ *a b f*. *INTEGRAL_BOUND_SYM* (*a*,*b*) *f*) ==> (*CFT omega* (λt. *complex_of_real* (*f* (−*t*))) = *CFT* (−*omega*) (λt. *complex_of_real* (*f t*)))

在该定理的假设条件中，前两个是假设函数 $f(t)$和 $f(-t)$的傅里叶变换存在，接下来的两个是假设实部和虚部的原函数分别为 $H1(t)$和 $H2(t)$。根据复数库中的相关定义及定理将原始目标分成其对应的实部和虚部分别进行证明，并且用实部和虚部的积分对引理 5 进行实例化，选用适当的策略并结合 limTheory 库和 integration 库中的定理可使目标得证。

3.3 频移性质

当函数 $f(t)$ 乘以一个复指数函数 $e^{\pm j\omega_0 t}$ 后，将会使其傅里叶变换左右平移，该性质如下：

$$\mathcal{F}[f(t)e^{j\omega_0 t}]=F(\omega-\omega_0) \tag{5}$$

其中，ω_0 为常实数，在信号的调制和解调过程中该性质具有非常重要的作用，调制时它可以将低频信号搬移到高频信号，从而减少噪声的干扰；解调时，采用相同的载波信号将调制信号搬移到原来的频谱。该性质的形式化如下：

性质 3 CFT_Frequency_ Shift_Property

|- ∀ *f omega*0. *CFT_EXISTS f* ==>

(*CFT omega* (λt. *f t* * exp (*i* * *omega*0 * *t*)) = *CFT* (*omega*−*omega*0) (λt. *complex_of_real* (*f t*)))

该性质的证明相对比较简单，先重写傅里叶变换的定义，然后再根据复数库中模的左乘、右乘等一些基本运算性质，便可完成最终目标的证明。当复指数函数形如 $e^{-j\omega_0 t}$ 时，其证明过程类似。

3.4 时域微分性质

假设在任意一点 x 处，函数 $f(t)$可导且导函数是 $f'(t)$，函数 $f(t)$及其导函数 $f'(t)$的傅里叶变换都存在，且当 $|t|\to\infty$ 时函数 $f(t)$的极限为 0，则

$$\mathcal{F}[f'(t)]=i\omega F(\omega) \tag{6}$$

对该性质的证明以及后面对高阶导数的证明，要借助表 1 所列的几个引理，对一阶微分性质进行如下的形式化：

性质 4 CFT_DIFF

|- ∀ *f f' omega*.

(∀ *x*. (*f diffl f' x*) *x*) ∧ *CFT_EXISTS f* ∧ *CFT_EXISTS f'* ∧ (λn. *f*(&*n*)) −−>0 ∧ (λn. *f* (−&*n*)) −−>0 ==> (*CFT omega* (λt. *complex_of_real* (*f' t*)) = (0,*omega*) * *CFT omega* (λt. *complex_of_real* (*f t*)))

表 1　时域微分性质引理

	引理名称	引理描述	在 HOL4 中的表述形式
6	LEM_COS_0	若 f(x)趋于正无穷时的函数值为 0，则 f(x) coswt 趋于无穷时的值为 0	|-∀f omega. (λn. f (&n)) −−> 0 ==> (λn. f (&n) * cos (omega * &n))−−> 0
7	LEM_NEG_COS_0	若 f(x)趋于负无穷时的函数值为 0，则 f(x) coswt 趋于负无穷时的值为 0	|-∀f omega. (λn. f (−&n)) −−> 0 ==> (λn. f (−&n) * cos (omega * &n)) −−> 0
8	DIFFERENTIABLE_DERIV	函数 f(x)在点 x 处可微和在点 x 处有导数值等价	|- ∀f x. f differentiable x <=> (f diffl deriv f x) x
9	DIFFL_DERIV	函数在 x 处的导数值为 k，那么 deriv 在 x 处的返回值为 k	|-∀f x k. (f diffl k) x==> (deriv f x=k)
10	N_ORDER_DERIV_1	根据高阶导数的定义，当 n=1 时就是函数在 x 处的一阶导数	|-∀f x. n_order_deriv 1 f x =deriv f x
11	N_ORDER_DERIV_LEM1	函数的 n 阶导数的一阶求导等于函数的 n+1 阶导数	|-∀f x. n_order_deriv(SUC n) f x=deriv (\x. n_order_deriv n f x) x

要证明此定理成立，可以转化为证明等式两边的实部和虚部分别对应相等成立。根据复数库中的一些定义及定理将原始目标化简成两个子目标即：$\int_{-\infty}^{+\infty} f'(t)\cos\omega t\mathrm{d}t=\omega\int_{-\infty}^{+\infty} f(t)\sin\omega t\mathrm{d}t$和$\int_{-\infty}^{+\infty} -f'(t)\sin\omega t\mathrm{d}t=\omega\int_{-\infty}^{+\infty} f(t)\cos\omega t\mathrm{d}t$。

因此，对原始目标的证明就可转化为对这两个子目标的证明。这两个子目标的证明主要基于分部积分公式，以第一个子目标为例，对等式左边使用分部积分法后得到：$\int_{-\infty}^{+\infty} -f'(t)\cos\omega t\mathrm{d}t=f(t)\cos\omega t|_{-\infty}^{+\infty}+\omega\int_{-\infty}^{+\infty} f(t)\sin\omega t\mathrm{d}t$，重写假设条件及引理 6 和引理 7 可使第一个子目标得证，第二个子目标的证明过程与第一个子目标相似。两个子目标都成立，很显然原始目标也成立。

更一般地，若 $f(\pm\infty)=f'(\pm\infty)=\cdots=f^{(k-1)}(\pm\infty)=f^{(n)}(\pm\infty)=0$，且对 $\forall k.\ k\leqslant n$，$f^{(k)}(t)$的傅里叶变换存在，则

$$\mathscr{F}[f^{(n)}(t)]=(i\omega)^n\mathscr{F}[f(t)] \tag{7}$$

即 n 阶导数的傅里叶变换等于函数的傅里叶变换乘以 $(i\omega)^n$ 因子。该性质的形式化要用到文献[14]中的两个定义，现做一下简单说明：

定义 5　n_order_deriv_def

|- (∀f x. n_order_deriv 0 f x=f x) ∧ ∀n f x. n_order_deriv (SUC n) f x=n_order_deriv n (λx. deriv f x) x

采用递归的方法对高阶导数的定义进行了形式化，其中 deriv f x 的返回值是函数 $f(x)$在 x 处的导数值，形式化定义如下：

定义 6　deriv_def

|- ∀f x. deriv f x=@k. (f diffl k) x

基于定义 5 和定义 6，可对傅里叶变换的 n 阶微分性质 CFT_DIFF_GENERAL 进行形式化，其证明过程如下所示：

```
val CFT_DIFF_GENERAL = store_thm("FT_DIFF_GENERAL",
(−−`!(f:real−>real)(omega:real)(n:num).
(!(m:num). m≤n==> FT_EXISTS(\t. n_order_deriv m f t)) ∧
(!m(x:real) . m≤n==> (\x. n_order_deriv m f x ) differentiable x
) ∧
(!(m:num). m≤n==> (\b. n_order_deriv m f (&b)) −−> 0)
∧
(!(m:num). m≤n==>(\b. n_order_deriv m f (−&b)) −−> 0)
==> (FT(omega:real)(\t. complex_of_real(n_order_deriv n f t))
= ((0, omega) pow n) * FT(omega:real) (\t. complex_of_real
(f(t))))'−−),
REPEAT STRIP_TAC THEN Induct_on'n:num' (*对 n 进行归纳*)
THENL[REWRITE_TAC[complex_pow_def] (*当 n=0 时*)
THEN REWRITE_TAC[n_order_deriv_def]
THEN REWRITE_TAC[COMPLEX_MUL_LID],
REPEAT DISCH_TAC (*当 n=SUC n 时*)
THEN W(C SUBGOAL_THEN ASSUME_TAC o funpow 2 (fst o
dest_imp) o snd) (*证明任意 n 阶以下导函数的傅里叶变换存在*)
THENL[REPEATSTRIP_TAC THEN
FIRST_ASSUM MATCH_MP_TAC THEN
RW_TAC std_ss[LESS_OR_EQ,LESS_EQ_IMP_LESS_SUC],
ASM_REWRITE_TAC[] THEN
W(C SUBGOAL_THEN ASSUME_TAC o funpow 2 (fst o dest_
imp) o snd) (*证明任意 n 阶以下导函数可微*)
THENL[REPEAT STRIP_TAC THEN FIRST_ASSUM MATCH_
MP_TAC
THENRW_TAC std_ss[LESS_OR_EQ, LESS_EQ_IMP_LESS_
SUC],
ASM_REWRITE_TAC[] THEN
W(C SUBGOAL_THEN ASSUME_TAC o funpow 2 (fst o dest_
imp) o snd) (*证明任意 n 阶以下导函数趋于正无穷时的极限为 0
*)
THENL[REPEAT STRIP_TAC THEN
FIRST_ASSUM MATCH_MP_TAC THEN
RW_TAC std_ss[LESS_OR_EQ,LESS_EQ_IMP_LESS_SUC] ,
ASM_REWRITE_TAC[] THEN
W(C SUBGOAL_THEN ASSUME_TAC o funpow 2 (fst o dest_
imp)o snd) (*证明任意 n 阶以下导函数趋于负无穷时的极限为 0
*)
THENL[REPEAT STRIP_TAC THEN FIRST_ASSUM MATCH_
MP_TAC
THEN RW_TACstd_ss[LESS_OR_EQ, LESS_EQ_IMP_LESS_
SUC],
ASM_REWRITE_TAC[] THEN DISCH_TAC THEN
REWRITE_TAC[complex_pow_def] (*重写 complex_pow 定义*)
THEN REWRITE_TAC[GSYM COMPLEX_MUL_ASSOC]
THEN FIRST_ASSUM(SUBST1_TAC o SYM)
THEN POP_ASSUM K_TAC THEN
HO_MATCH_MP_TAC CFT_DIFF (*匹配一阶微分性质*)
THEN POP_ASSUM (MP_TAC o Q.SPEC' n:num')
THEN REWRITE_TAC[LESS_EQ_REFL]
THEN DISCH_TAC THEN ASM_REWRITE_TAC[]
THEN FIRST_ASSUM (MP_TAC o Q.SPEC' n:num')
THEN REWRITE_TAC[LESS_EQ_REFL] THEN DISCH_TAC
THEN ASM_REWRITE_TAC[] THEN CONJ_TAC
THENL[ASSUM_LIST(fn thl => UNDISCH_TAC(concl(el 1
(rev thl)))) THEN DISCH_THEN(MP_TAC o SPEC"n:num")
THEN RW_TACstd_ss
[LESS_OR_EQ,LESS_EQ_IMP_LESS_SUC],CONJ_TAC THENL
[ASSUM_LIST(fn thl=>UNDISCH_TAC(concl(el 1 (rev thl))))
THEN DISCH_THEN(MP_TAC o SPEC"(SUC n):num")
THEN RW_TAC std_ss[LESS_EQ_REFL],
RW_TAC std_ss [N_ORDER_DERIV_LEM1] (*重写引理 11*)
THEN REWRITE_TAC[GSYM DIFFERENTIABLE_DERIV] (*
```

重写引理 8 *)
THEN FIRST_ASSUM MATCH_MP_TAC
THEN ASM_REWRITE_TAC[LESS_EQ_REFL]]]]]]]]);

高阶微分性质的证明采用对 n 进行归纳的方法：

1)当 $n=0$ 时，等式左边根据定义 4 可知 $f(t)$ 的 0 阶导数仍为它本身，等式右边根据 complex_pow 的定义可得 $(i\omega)^0=1$，左边等于右边显然成立；

2)当 $n=k+1$ 时，假设 $\mathscr{F}[f^{(k)}(t)]=(i\omega)^k\mathscr{F}[f(t)]$ 成立，因为 $\int_{-\infty}^{+\infty} f^{(k+1)}(t)e^{-i\omega t}dt=\int_{-\infty}^{+\infty} e^{-i\omega t}df^{(k)}t$，所以等式左边可以当作是对函数 $f^{(k)}t$ 的一阶微分求傅里叶变换，根据性质 4 可得 $\mathscr{F}[f^{(k+1)}(t)]=(i\omega)\mathscr{F}[f^k(t)]$，根据 complex_pow 的定义可得 $(i\omega)^{k+1}=(i\omega)*(i\omega)^k$，于是等式右边 $(i\omega)^{k+1}\mathscr{F}[f(t)]=(i\omega)*(i\omega)^k\mathscr{F}[f(t)]$，重写假设条件就可使目标得证。

3.5 时域积分性质

若 $F(0)=\int_{-\infty}^{+\infty} f(t)dt=0$，则

$$i\omega\mathscr{F}[\int_{-\infty}^{t} f(t)dt]=\mathscr{F}[f(t)] \tag{8}$$

该性质的形式化如下：

性质 5 CFT_INTEGRAL

|- ∀*f*. *CFT_EXISTS f* ∧*CFT_EXISTS* (λ*t*. *f_lim* (λ*b*. *integral* (−*abs b*,*t*) *f*)) ∧ (∀*x*. *f contl x*) ∧ (∀*a*. ∃*k*. (λ*b*. *integral* (−*abs b*,*a*) *f*) −−> *k*) ∧ (∀*a b*. *a*≤*b* ==> *integrable* (*a*,*b*) *f*) ∧ (*f_lim* (λ*b*. *integral* (−*abs b*,*abs b*) *f*) = 0) ∧ (λ*b*. (λ*t*. *f_lim* (λ*b*. *integral* (−*abs b*,*t*) *f*)) (*abs b*)) −−> 0 ∧ (λ*b*. (λ*t*. *f_lim* (λ*b*. *integral* (−*abs b*,*t*) *f*)) (−*abs b*)) −−> 0 ==> (*CFT* (λ*t*. *complex_of_real* (*f t*)) *omega* = (0,*omega*) * *CFT*(λ*t*. *complex_of_real* ((λ*t*. *lim* (λ*b*. *integral* (−*abs b*,*t*) *f*)) *t*)*omega*)

根据时域一阶微分性质：

$$\mathscr{F}[\frac{d}{dt}\int_{-\infty}^{t} f(x)dx]=i\omega\mathscr{F}[\int_{-\infty}^{t} f(x)dx]$$

因此如果 $\frac{d}{dt}\int_{-\infty}^{t} f(x)dx=f(t)$ 得证，那么即可证明原目标成立。对无穷积分的上变限求导问题是证明时域积分性质的难点之一。根据积分的结合性质存在实数 a，当 $a<t$ 时，$\int_{-\infty}^{t} f(x)dx=\int_{-\infty}^{a} f(x)dx+\int_{a}^{t} f(x)dx$，由导数的四则运算法则得：$\frac{d}{dt}\int_{-\infty}^{t} f(x)dx=\frac{d}{dt}\int_{-\infty}^{a} f(x)dx+\frac{d}{dt}\int_{a}^{t} f(x)dx$，该等式右边第一项的积分值是一个常数，导数值为 0，因此此时的问题变成了对 $\frac{d}{dt}\int_{a}^{t} f(x)dx=f(t)$ 的证明，这是关于定积分的变上限求导问题。关于它有一个非常重要的定理即原函数存在定理，其描述如下：若 g 在 $[a,b]$ 上连续，则 $\int_{a}^{t} g(x)dx$ 在 (a,b) 上处处可导，且 $\frac{d}{dt}\int_{a}^{t} g(x)dx=g(t)$[15]，该定理在导数和定积分之间建立关系。目前在微积分库中还没有涉及到变限积分的相关定义及定理，本文对原函数存在定理进行了形式化证明，其形式化如下：

定理 2 Fundamental_Theorem_Calculus

|- ∀*g a b*.
a≤*b* ∧ (∀*x*. *a*≤*x* ∧ *x*≤*b* ==> *g contl x*) ==> ∀*t*. *a*<*t* ∧ *t*<*b* ==> ((λ*x*. *integral* (*a*,*x*) *g*) *diffl g t*) *t*

该定理的证明过程比较繁琐，要处理的细节问题较多，需要表 2 所列的一些辅助引理来帮助证明，证明代码约有 300 行。

表 2 时域积分性质引理

	引理名称	引理描述	HOL4 表述形式
12	INTEGRAL_TRIANGLE	$\lvert\int_a^b f(x)dx\rvert\leqslant\int_a^b \lvert f(x)\rvert dx$	|- ∀f a b. a≤b ∧ integrable (a,b) f ∧ integrable (a,b) (\x. abs (f x)) ==> abs (integral (a,b) f) ≤ integral (a,b) (\x. abs (f x))
13	CONT_ABS	函数 f 在点 x 处连续，那么函数 f 的绝对值在 x 处亦连续	|- ∀f x. (\x. f x) contl x ==> (\x. abs (f x)) contl x
14	INTEGRAL_BOUND_EQ	积分上下限相等时，函数的积分值为 0：$\int_a^a f(x)dx=0$	|- ∀ f a. integral (a,a) f=0
15	FTC_LEM1	与一个小于 1 的数相乘，越乘越小	|- ∀ x1 x2 y1. 0≤x1 ∧ 0≤y1 ∧ x1<x2 ∧ y1<1 ==>x1 * y1<x2
16	FTC_LEM2	若 y≤z ∧ z≤y+x，则 ∃t. t∈[0,1]，使得 z=y+t * x	|- ∀ x y z t. 0 <x ∧ y≤z ∧ z ≤y+x==>∃t. 0 ≤t ∧ t≤ 1 ∧ (z=y+t * x)
17	FTC_LEM3	若 y≤z ∧ z≤y+x，则 ∃t. t∈[0,1]，使得 z=y+t * x	|- ∀ x y z t. 0<x ∧ y≤z ∧ z≤ y+x==>∃t. 0≤t ∧ t≤1 ∧ (z=y+t * x)

关于无穷积分变上限求导问题的形式化为：

定理 3 DIFFL_IMPROPER_INTEGRAL

|- ∀*f t k a*. *a* < *t* ∧ (*x*. *f contl x*) ∧ ((λ*b*. *integral* (−*abs b*,*a*) *f*) −−> *k*) ∧ (∀*a b*. *a*≤*b* ==> *integrable*(*a*,*b*) *f*) ==> ((λ*t*. (*lim*(λ. *integral*(−*abs b*,*t*) *f*))) *diffl f* (*t*))*t*;

该定理的证明代码有 300 多行，这里不再详细叙述。

4 应用

本节对串联谐振电路的频率响应进行形式化分析，示范基于 CFT 定理库的形式化分析与验证应用。图 1 所示是一个具有电动势 $f(t)$ 的 RLC 的电路，它是最基本的选频回路，有滤掉不需要的杂波、谐波和选出所需频率的作用。对谐振现象的研究有重要的实际意义：1)因为谐振现象有广泛的应用，如在无线电工程中，利用串联谐振可以获得较高的电压；在高电压技术中，利用串联谐振获得工频高电压，为变压器等电力设备做耐压测试，可以发现设备中危险的集中性缺陷；2)在某些情况下电路中发生谐振会破坏正常工作。对 RLC 串联电路进行设计时，可以通过分析其频率响应，然后恰当选择 R、L、C 值来达到选频及滤波的目的。

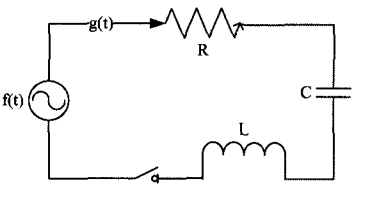

图 1 RLC 串联谐振电路

设 t 时刻回路中的电流是 $g(t)$，则根据基尔霍夫律 $g(t)$

和 $f(t)$满足如下的微积分方程：

$$L\frac{d^2g(t)}{dt}+R\frac{dg(t)}{dt}+\frac{1}{C}g(t)=\frac{df(t)}{dt} \tag{9}$$

对式(9)两边同时取傅里叶变换，可以得到该串联回路的频率响应：

$$H(\omega)=\frac{G(\omega)}{F(\omega)}=\frac{i\omega}{L(i\omega)^2+R(i\omega)+1/C} \tag{10}$$

本节的目的就是使用式(9)来验证其频率响应式(10)成立。对系统的频率响应形式化证明时，为了使目标看起来更加简洁，定义 COEFFI、F_omega、G_omega 分别代表 $L(i\omega)^2+R(i\omega)+1/C$、输入频率响应、输出频率响应。因为 COEFFI 中的前两项为复数，而 $1/C$ 为实数，所以相加时存在类型不一致的问题，在对其定义时应使用 complex_of_real 将实数 $1/C$变成复数类型。

定义 7 val COEFFI=(–'L * ((0,omega) pow 2)+R *(0,omega)+complex_of_real(inv C)'–)

定义 8 val F_omega= (–'CFT omega (\t. complex_of_real(f t))'–)

定义 9 val G_omega= (–'CFT omega (\t. complex_of_real(g t))'–)

将 RLC 串联电路频率响应形式化为如下。

定理 4 RLC_CFT_Response

|- ∀ *f g omega L R C.*

*0<L∧0<R∧0<C∧(∀m. m≤2==>FT_EXISTS (λt. n_order_deriv m g t))∧(∀mx. m≤2 ==> (λx. n_order_deriv m g x) differentiable x)∧(∀m. m≤2==> (λb. n_order_deriv m g (&b)) −−> 0)∧(∀m. m <= 2 ==>(λb. n_order_deriv m g (−&b))−−> 0)∧(∀m. m ≤ 1 ==> FT_EXISTS (λt. n_order_deriv m f t))∧(∀m x. m≤1==> (λx. n_order_deriv m f x) differentiable x)∧(∀m. m≤1==> (λb. n_order_deriv m f (&b)) −−> 0)∧(∀m. m ≤ 1 ==> (λb. n_order_deriv m f (−&b)) −−> 0)∧(∀t. L * (n_order_deriv 2 g t)+R * deriv(\x. g(x))t +(inv C) * g(t)=deriv(\x. f(x))t)∧^ COEFFI <> 0∧^ F_omega <> 0 ==>(^ G_omega/^ F_omega=(0,omega)/^ COEFFI)'*;

前 3 个假设条件是保证电感、电阻、电容大于零，接下来 4 个依次是假设函数 $g(t)$二阶可导，任意二阶以下的导函数的傅里叶变换存在且当$|t|\to\infty$时极限为 0，再接下来的 3 个是假设函数 $f(t)$的任意一阶以下导函数的傅里叶变换存在且$|t|\to\infty$时的极限为 0，接下来一个假设条件就是对式(9)的形式化描述，最后两个是假设式(10)中的分母不为 0，而结论是对式(10)的形式化描述。

证明时先根据复数库中的 COMPLEX_EQ_RDIV_EQ、complex_div 等一些运算性质将式(10)中的分式化为整式即

$$(L(i\omega)^2+R(i\omega)+1/C)G(\omega)=i\omega F(\omega) \tag{11}$$

根据高阶微分性质证明 $i\omega F(\omega)$等于函数 f 一阶导数的傅里叶变换，再根据微分性质及线性性质证明式(9)左侧的傅里叶变换等于式(11)的左侧，这两个目标得证后原目标变为 $\mathcal{F}(L\frac{d^2g(t)}{dt}+R\frac{dg(t)}{dt}+\frac{1}{C}g(t))=\mathcal{F}(\frac{df(t)}{dt})$的形式，重写假设条件，目标中左侧的部分被式(9)右侧的部分替代，很显然此时目标得证，证明过程中还要用到复数的许多运算性质以及关于定义 6 的一些引理。

形式化验证的结果和理论结果一致。由于定理证明方法的完备性，就所证明的性质而言，其结果是准确完备的。基于本文实现的 CFT 定理库，应用系统的验证过程相对简单，说明了形式化的傅里叶变换在分析现实应用中的有效性。

结束语 本文基于高阶逻辑定理证明器 HOL4，实现了对连续傅里叶变换的定义以及常用性质的形式化，并且证明了一个重要的定理即微积分基本定理，对换元积分法也给予了证明，利用傅里叶变换的线性及微分性质，对 RLC 串联电路的频率响应进行了分析。本文实现的连续傅里叶变换理论的形式化定理库为使用定理证明方法进行相关系统的形式化验证准备了条件。傅里叶变换的卷积定理以及时频域的能量守恒是其广泛应用的重要原因，因此下一步工作将在 HOL4 中完成傅里叶变换卷积定理和帕萨瓦尔定理的形式化以及更多应用的形式化验证。

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] Slind, Konrad, Norrish M. A brief overview of HOL4. Theorem Proving in Higher Order Logics[M]. Springer Berlin Heidelberg, 2008: 28-32

[3] http://hol.sourceforge.net/

[4] Akbarpour B. Modeling and Verification of DSP Designsin HOL [D]. Montreal, Quebec, Canada: Department of Electrical and Computer Engineering, Concordia University, Aprial 2005

[5] Harrison J, Théry L. Extending the HOL theorem prover with a computer algebra system to reason about the reals[M]// Higher Order Logic Theorem Proving and Its Applications. Springer Berlin Heidelberg, 1994: 174-184

[6] 张玉鹏，施智平，关永，等. SpaceWire 译码电路在 HOL4 中的形式化验证[J]. 小型微型计算机系统，2013，8：1959-1963

[7] Abdullah A N M, Akbarpour B, Tahar S. Formal analysis and verification of an OFDM modem design using HOL[C]// Formal Methods in Computer Aided Design, 2006(FMCAD'06). IEEE, 2006: 189-190

[8] 盖云英，包革军，等. 复变函数与积分变换[M]. 北京：科学出版社，2006

[9] 曾禹村，张宝俊，等. 信号与系统[M]. 北京：北京理工大学出版社，2008

[10] Bracewell R N. The Fourier transform and its applications[M]. New York, 1965

[11] Taqdees S H, Hasan O. Formalization of Laplace Transform Using the Multivariable Calculus Theory of HOL-Light[C]// Logic for Programming, Artificial Intelligence, and Reasoning. Springer Berlin Heidelberg. New York: McGraw-Hill, 1986, 2013: 744-758

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

[13] 谷伟卿，施智平，关永，等. Gauge 积分在 HOL4 中的形式化[J]. 计算机科学，2013，40(2)：191-194

[14] Siddique U, Hasan O. Formal analysis of fractional order systems in HOL[C]// Computer-Aided Design (FMCAD). IEEE, 2011: 163-170

[15] 华东师范大学数学系. 数学分析[M]. 北京：高等教育出版社，2006