实数二项式系数在HOL4中的形式化

师丽坤[1] 赵春娜[1] 关 永[1] 施智平[1] 李晓娟[1] 叶世伟[2]
(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]

摘 要 定理证明是一种形式化方法,在高可靠性系统验证中起着越来越重要的作用。分数阶微积分是高可靠性系统分析的基础,实数二项式系数是分数阶微积分定义的重要组成部分。在高阶逻辑定理库中还没有实数二项式系数的形式化。提出实数二项式系数高阶逻辑形式化方法。首先研究阶乘幂在HOL4中的形式化,然后利用阶乘幂的高阶逻辑形式分析实数二项式系数,最后将实数二项式系数应用于分数阶微积分的形式化。分数阶微积分的形式化分析表明了实数二项式系数及其运算性质形式化的正确性和有效性。

关键词 实数二项式系数,高阶逻辑,定理证明,HOL4,分数阶微积分

中图法分类号 TP319 **文献标识码** A

Formalization of Real Binomial Coefficient in HOL4

SHI Li-kun[1] ZHAO Chun-na[1] GUAN Yong[1] SHI Zhi-ping[1] LI Xiao-juan[1] YE Shi-wei[2]
(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, Chinese Academy of Sciences, Beijing 100049, China)[2]

Abstract The theorem proving is a formal method and plays an important role in the verification of safety-critical system. The fractional calculus is the basis of the complex system's analysis. The real binomial coefficient is an important part of the fractional calculus GL definition. Currently, there is not the formalization of real binomial coefficient in higher-order-logic theorem library. This paper presented the formalization of the real binomial coefficients. The factorial power was firstly formalized in HOL4. And the real binomial coefficient was formalized using the formalization of factorial power. The paper also presented the formal verification of the fractional calculus. At the same time it illustrateed the practical effectiveness and utilization of our approach.

Keywords Real binomial coefficient, High order logic, Theorem proof, HOL4, Fractional calculus

1 引言

近些年,软硬件的设计错误造成的人身财产损失对社会的影响越来越大,尤其是高铁、航空、医疗等高安全领域,因此系统的可靠性受到人们的高度重视。形式化验证作为验证软硬件的正确性和可靠性的有效方法成为一个研究热点[1]。

形式化的数学系统由符号以及使用这些符号的规则共同组成。形式化方法是将概念或方法经过高度抽象后使用一定的数学模型进行表示,通过推演计算来研究数学模型,进而证明系统的正确性和可靠性,主要包括等价性验证、模型检测和定理证明3种技术[2]。HOL4是一个常用的交互式定理证明器,它利用定理证明的方法验证系统的正确性,并且已有很多成功的应用[9]。HOL4基于定理库中已有的推理规则、公理和定理对要验证的系统进行高阶逻辑建模和推理。定理证明系统拥有越丰富的定理库,建模推理能力就越强[10]。

分数阶微积分是解决许多高可靠系统的数学工具,如图像处理[12]、控制[11]、流体力学[13]等领域都有着非常广泛的应用。实数二项式系数是二项式系数在实数域的推广[3],它是分数阶微积分GL定义中的重要组成部分[4]。分数阶微积分和分数阶系统的形式化分析是以实数二项式系数形式化为基础的。目前在HOL4定理库中没有实数二项式系数的高阶逻辑形式化。只有拥有实数二项式系数的高阶逻辑表达式才能建立分数阶微积分的高阶逻辑模型。本文主要研究实数二项式系数在HOL4定理证明器中的形式化方法。

本文第2节提出基于实数二项式系数形式化分析框架结构;第3节介绍实数二项式系数及在高阶逻辑定理证明器HOL4中的形式化;第4节用第2节提出的方法验证分数阶微积分,证明该形式化方法的正确性和有效性;最后总结全文。

到稿日期:2013-04-21 返修日期:2013-06-21 本文受国际科技合作计划(2010DFB10930,2011DFG13000),国家自然科学基金项目(60873006,61070049,61170304,61104035,61174145,61201378),北京市自然科学基金、北京市优秀人才项目(4122017,KZ201210028036,KM201010028021,2012D005016000011)资助。

师丽坤(1988—),男,硕士生,主要研究方向为定理证明,形式化验证;**赵春娜**(1978—),女,博士,副教授,主要研究方向为定理证明、形式化验证、分数阶系统建模与控制,E-mail:chunnazhao@163.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 形式化框架结构图

基于实数二项式系数对分数阶微积分的高阶逻辑形式化的框架图如图 1 所示。图中灰色部分是本文的主要研究内容。它们是在定理证明器中构建分数阶微积分形式化分析框架的基础。该框架的输入是分数阶微积分的数学模型以及需要验证的性质，也就是图 1 中曲底矩形部分。

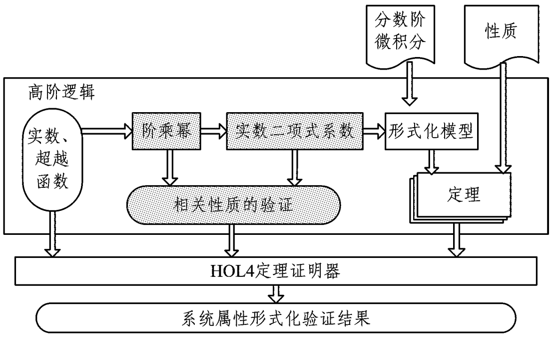

图 1 基于实数二项式系数的形式化框架

分数阶微积分形式化分析的第一步是用高阶逻辑构造形式化模型。完成第一步需要有高阶逻辑形式的实数二项式系数。实数二项式系数的形式化需要阶乘幂和实数的相关数学理论。Harrison 已经完成实数的形式化[5]。本文在 Harrison 的工作基础上对阶乘幂和实数二项式系数进行形式化，并将其用于构造分数阶微积分的高阶逻辑形式。第二步利用第一步构造的高阶逻辑模型去形式化分析分数阶微积分，即将分数阶微积分的性质表达为高阶逻辑函数。第三步用定理证明器对以上的高阶逻辑函数进行形式化验证。分数阶微积分性质的验证过程需要用到实数二项式系数的相关性质。为了验证分数阶微积分性质，本文验证了实数二项式系数和阶乘幂的一些重要性质。最后，框架的输出是经过证明的高阶逻辑定理。定理的正确证明为分数阶系统应用奠定了基础，同时也验证了实数二项式系数及其性质的形式化是正确的。

3 形式化

这部分主要是在实数库的基础上，提出阶乘幂和实数二项式系数的高阶逻辑形式化以及相关性质的验证。

3.1 阶乘幂的形式化

在普通代数学中代数多项式使用普通幂的积和式，即变量 x 的 n 次普通幂就是 x 自乘 n 次后的积。专门研究数与形的连续状态的渐变规律性的微积分比较适宜于处理普通幂。但是自然界还有许多离散状态阶梯式变化的量，需要考虑阶乘幂以及阶乘幂多项式[14]。下面给出两类阶乘幂的定义。

上升阶乘幂：

$$(x)^{[n]}=x(x+1)(x+2)\cdots(x+n-1) \tag{1}$$

下降阶乘幂：

$$(x)_n=x(x-1)(x-2)\cdots(x-n+1) \tag{2}$$

并且约定：

$$(x)^{[0]}=(x)_0=1 \tag{3}$$

上升阶乘幂和下降阶乘幂的 n 次幂和 $n+1$ 次幂之间拥有紧密的联系，使用递归的方法定义它们，可以令定义的描述简洁而且易于理解。其中，上升阶乘幂的递归调用函数是：

$$(x)^{[n+1]}=(x+n)*(x)^{[n]}$$

下降阶乘幂的递归调用函数是：

$$(x)_{n+1}=(x-n)*(x)_n$$

它们的终止条件是零次幂时等于 1，如式(3)所示。在 HOL4 中是通过合取的方式将终止条件和递归调用函数两个条件放在一起，即阶乘幂中这两个条件必须同时成立。对阶乘幂的形式化如下：

定义 1 上升阶乘幂

|- (!x. x fact_pow_asc 0=1) ∧ !x n. x fact_pow_asc SUC n=(x+&n) * x fact_pow_asc n

定义 2 下降阶乘幂

|- (!x. x fact_pow_des 0=1) ∧ !x n. x fact_pow_des SUC n=(x-&n) * x fact_pow_des n

下面对阶乘幂的一些重要性质进行验证，主要结果如表 1 所列，其中 x 为实数，m、n 为整数。

表 1 阶乘幂的相关性质

<table>
<tr><th></th><th>性质名称</th><th>HOL4 中形式化</th><th>数学表达式</th></tr>
<tr><td>1</td><td>FACT_POW_DES_FACT</td><td>|- !n m. n <= m ==> (&m fact_pow_des n= &FACT m/&FACT (m-n))</td><td>$(m)_n=\frac{m!}{(m-n)!}$ $(n<=m)$</td></tr>
<tr><td>2</td><td>FACT_POW_ASC _FACT</td><td>|- !n m. n <= m ==> (&m fact_pow_asc n= &FACT (m+n-1)/ &FACT (n-1))</td><td>$(m)^{[n]}=\frac{(m+n-1)!}{(n-1)!}$ $(n<=m)$</td></tr>
<tr><td>3</td><td>FACT_POW_DES _ NEG _ ASC</td><td>|- !m n. -m fact_pow_asc n=-1 pow n * m fact_pow_des n</td><td>$(-m)^{[n]}=(-1)^n(m)_n$</td></tr>
<tr><td>4</td><td>FACT_POW_DES_N_FACT</td><td>|- !n. &n fact_pow_des n =&FACT n</td><td>$(n)_n=n!$</td></tr>
<tr><td>5</td><td>FACT_POW_ASC_1_FACT</td><td>|- !n. 1 fact_pow_asc n= &FACT n</td><td>$(1)^{[n]}=n!$</td></tr>
<tr><td>6</td><td>FACT_POW_ASC_DES</td><td>|- !x n. x fact_pow_asc n =(x+&n-1) fact_pow_des n</td><td>$(x)^{[n]}=(x+n-1)_n$</td></tr>
<tr><td>7</td><td>FACT_POW_DES_ASC</td><td>|- !x n. x fact_pow_des n =(x-&n+1) fact_pow_asc n</td><td>$(x)_n=(x-n+1)^{[n]}$</td></tr>
</table>

表中第 1 条和第 2 条性质分别验证了下降阶乘幂和上升阶乘幂与阶乘的关系。它们是阶乘幂的重要性质，阶乘幂的其它性质和实数二项式系数的一些性质是基于这两条性质进行验证的。它们的验证难点在于数学归纳法的正确使用，与手工验证不同，它们的变换必须符合 HOL4 的逻辑规则，逻辑拥有完备性，这也同时保证了证明的百分百正确。第 3 条性质验证了当 x 取整数时(表 1 中用 m 表示)上升阶乘幂与下降阶乘幂的特殊关系。第 4 条和第 5 条分别是下降阶乘幂和上升阶乘幂的特殊情况，它们的验证为后面很多性质的验证提供了方便。第 6 条和第 7 条是阶乘幂之间两种转化，它们的证明主要也用到数学归纳法，这两条定理虽然相似，但是把它们分为不同形式定理为以后证明过程中的定理调用提供了方便。

阶乘幂定义中递归方法的引入和阶乘幂性质证明时数学归纳法在高阶逻辑中的高效应用是阶乘幂形式化的关键。阶乘幂在很多领域都有应用，如差分计算[14]和我们下面将要形式化的实数二项式系数。

3.2 实数二项式系数的形式化

整数二项式系数在数学上是二项式定理中的系数族。它的结果是一个正整数，且能以两个非负整数作为参数，这两个

参数通常以 n 和 k 代表，可将二项式系数写作 $\binom{n}{k}$[6]。把二项式系数 n 扩展为任意的数进行推广[7]，可得：

设 k 是非负整数，x 是任意实数，令

$$\binom{x}{k}=\frac{x(x-1)\cdots(x-k+1)}{k!}=\frac{(x)_k}{k!} \tag{4}$$

称 $\binom{x}{k}$ 为实数二项式系数。

在整数二项式系数中，当 $k>n$ 时 $\binom{n}{k}=0$，可以理解为从 n 个东西中取 k 个。在 $k>n$ 情况下，表明所取个数已超过总数，无法取到，即从 n 中取 k 的情况为零。实数二项式系数 $\binom{x}{k}(x\in R,k\in N)$ 和整数二项式系数有些不同。在 $x<k$ 条件下，当 x 等于自然数时，$x(x-1)\cdots(x-(k-1))$ 会出现 0 项，如 $\binom{2}{4}=\frac{2*1*0*(-1)}{4!}=0$；当 x 不是自然数时，$x(x-1)\cdots(x-(k-1))$ 不会出现 0 项，如 $\binom{2.5}{4}=\frac{2.5*1.5*0.5*(-0.5)}{4!}\neq 0$。在 $x>k$ 条件下，如果 x 等于自然数，实数二项式系数和整数二项式系数具有相同结果。可见整数二项式系数是实数二项式系数的一种特殊情况。

实数二项式系数是通过下降阶乘幂 fact_pow_des 和阶乘 FACT 定义的。在 HOL4 中根据式(4)的中间形式对实数二项式系数直接定义难度比较大，利用阶乘幂定义实数二项式系数可以降低定义难度。实数二项式系数在 HOL4 中的形式化如下：

定义 3 实数二项式系数

|- !x k. rbino_coe x k=x fact_pow_des k/&FACT k

下面对实数二项式系数的一些重要性质进行形式化，主要结果如表 2 所列，其中 x 为实数，n、k 为整数。我们从分析实数二项式系数性质开始，对其进行形式化验证。

表 2 实数二项式系数的相关性质

	性质名称	HOL4 中形式化	数学表达式
1	RBINO_COE_0	|- ! n k. n<k ==> (rbino_coe (&n) k=0)	$\binom{n}{k}=0\ (n<k)$
2	RBINO_COE_1	|- ! x. rbino_coe x 0=1	$\binom{x}{0}=1$
3	RBINO_COE_1_N	|- ! k. rbino_coe (&k) k=1	$\binom{x}{k}=1\ (x=k)$
4	RBINO_COE_FACT	|- ! n k. k <= n ==> (rbino_coe (&n) k=&FACT n/(&FACT k * &FACT (n-k)))	$\binom{n}{k}=\frac{n!}{k!\ (n-k)!}\ (k\leqslant n)$
5	RBINO_CEO_NEG	|- ! x k. rbino_coe (-x) k=(-1) pow k * rbino_coe (x+k-1) k	$\binom{-x}{k}=(-1)^k\binom{x+k-1}{k}$
6	RBINO_CEO_PASCAL	|- ! x k. 0 < k ==> (rbino_coe x k=rbino_coe (x-1) (k-1)+rbino_coe (x-1) (k))	$\binom{x}{k}=\binom{x-1}{k-1}+\binom{x-1}{k}$

表 2 中第 1 条即是对实数二项式系数的特例整数二项式系数的性质在 $k>n$ 情况下的形式化。第 2 条和第 3 条是实数二项式系数的两种特殊情况。第 2 条是当 k 等于 0 时，对于任意 x 实数二项式系数等于 1；第 3 条是当 x 等于 k 时，实数二项式系数等于 1，这两条性质的证明主要是对实数二项式系数、下降阶乘幂和阶乘 3 个定义的重写以及相关的数学推理。它们是实数二项式系数的经典性质，后面许多定理的证明需要用到这两条定理，尤其是在实际应用中。第 4 条表示了实数二项式系数与阶乘的关系。这里使用 n 而不是 x 是因为 n 代表自然数符合阶乘的要求。其中前提条件 k 小于等于 n 保证了 $n-k$ 阶乘的成立。第 5 条验证了实数二项式系数中 x 取反时所得结果，它的证明主要是用定义 3 对实数二项式进行展开，然后用到实数乘法的交换律、乘与除的关系等一些实数的推理。主要变换如下：

$$\begin{aligned}\binom{-x}{k}&=\frac{(-x)(-x-1)(-x-2)\cdots(-x-(k-1))}{k!}\\&=(-1)^k\frac{x(x+1)(x+2)\cdots(x+k-1)}{k!}\\&=(-1)^k\frac{(x+k-1)(x+k-2)(x+k-3)\cdots x}{k!}\\&=(-1)^k\binom{x+k-1}{k}\end{aligned}$$

第 6 条呈现了实数二项式系数的 Pascal 三角形法则。Pascal 法则是一个重要的递归等式。它是二项式系数向下化简的有力工具。在很多应用中，需要实数二项式系数的递归化简，并一直化简到表 2 中第 2 条定理的形式，然后再利用第 2 条定理得出结果。这些性质的证明不仅为下面的分数阶微积分的形式化提供了基础，同时还是对 HOL4 库的补充。

4 应用与验证

4.1 分数阶微积分 GL 定义的形式化

分数阶微积分理论研究几乎与整数阶微积分理论研究具有同样长的历史，但由于分数阶微积分的实际应用没有被发现而发展缓慢。直到 1983 年 Mandelbort[18] 首次指出自然界及许多科学技术领域中存在大量的分数维事实，分数阶微积分才重新获得了新的发展而成为当前国际上的一个热点研究领域。近些年分数阶微积分被广泛地应用于 $PI^{\alpha}D^{\alpha}$ 控制器[15]、信号处理[16]、地震分析[17] 等领域并取得了更好的效果。例如，分数阶加热炉模型要比整数阶的模型更加准确[8]。分数阶微积分是扩展传统微积分学的一种直接方式，即允许微分方程中对函数的导数阶次选择分数，而不仅是现有的整数。下面将利用高阶逻辑形式的实数二项式系数对分数阶微积分定义进行形式化，并且利用分数阶微积分的高阶逻辑定义对分数阶微积分的零阶性质进行验证。

分数阶微积分 GL 定义如下：

$${}_aD_t^v f(t)=\lim_{h\to 0}h^{-v}\sum_{j=0}^{[(t-a)/h]}(-1)^j\binom{v}{j}f(t-jh) \tag{5}$$

分数阶微积分 GL 定义通过操作算子 ${}_aD_t^v$ 把积分和微分统一在一起。其中 $\binom{v}{j}$ 是 v 为实数、j 为自然数的实数二项式系数。基于实数二项式系数的高阶逻辑定义对式(5)的形式化如下：

定义 4 分数阶微积分 GL 定义

|- ! f v a b x. frac_cal f v a b x=lim(\n. 2 rpow (&n * v) * (sum(0,SUC (flr((b-a) * (2 pow n)))) (\(m:num). ((~1) pow m * (rbino_coe v m) * f(x-(&m/(2

pow n)))))))`;
其中，f 是一个 real-real 类型的函数，v 为分数阶微积分阶数。a，b 分别为分数阶微积分下限和上限，式(5)中的上限是积分变量 t，相当于变上限积分，本文分数阶微积分的高阶逻辑定义中积分上限是 b，这样的定义是一个定积分，能更好地适用于现实的应用。lim 是求 n 趋于无穷时表达式的极限，rpow 是上标为实数的指数函数，rbino_coe 是第三部分定义的实数二项式系数。sum 是求和函数，其中 0 和 flr(($b-a$) * (2 pow n))分别是求和函数的下限和上限。flr 为对实数进行下取整，它将返回小于等于这个实数的最大整数，这个函数满足了求和函数 sum 的上下界是整数的要求。

当分数阶微积分的阶次为零，即没有对函数进行微分也没有进行积分时，返回函数本身，数学模型如式(6)所示：

$$ {}_0D_t^0 f(t) = f(t) \tag{6}$$

用分数阶微积分的高阶逻辑定义对上式进行高阶逻辑建模，可得：

定理 1 分数阶微积分零阶性

|- frac_cal f 0 a b x=f x

根据 HOL4 的推理规则，利用定义 4 重写定理 1 后，可以将定理 1 转换为式(7)：

lim(\n. 2 rpow 0 * sum (0,SUC (flr ((b−a) * 2 pow n))) (\m. −1 pow m * rbino_coe 0 m * f (x−&m/2 pow n)))=f x (7)

上式的证明需要用到实数二项式系数的性质 RBINO_COE_1 和 RBINO_COE_0(见表 2)以及求和函数 sum 两个引理。对实数二项式系数形式化定理的应用表明了实数二项式系数性质的有用性以及本文对实数二项式系数形式化的正确性。对上式的求和函数 sum 和求极限函数 lim 的处理是本定理证明的一个难点。在人们的习惯性思维及通常纸质上的推导过程中会先化简 sum 再处理 lim。但在 HOL4 中，如果从 sum 先入手，系统会对 n 出现不同的识别，sum 中的 n 为任意自然数，而 lim 的变量 n 是一个趋于无穷的数，它们的意义不一样，证明很难完成。本文的方法是先化简 lim，然后对 sum 化简，这样就可以确保计算机对 n 的识别是一致的。定理 1 的证明结果如图 2 所示。这条定理表明了零阶分数阶微积分返回原函数。

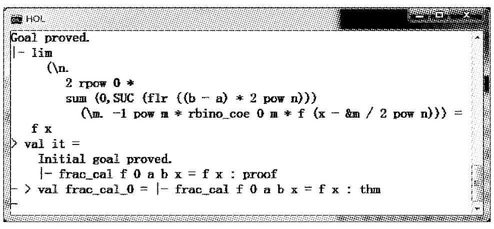

图 2 分数阶微积分 GL 定义零阶性的验证结果

图 2 中目标得证(Goal proved)表明等式(6)已经证明完毕，计算机可以根据 HOL4 的规则推出初始目标得证(Initial goal proved)，这是开始证明过程的反向推导。最后一行表明得证的等式以定理的形式存储到 HOL4 中，定理名称为 frac_cal_0。

分数阶微积分的形式化分析是对实数二项式系数的实际应用。由于形式化模型的特性继承了高阶逻辑定理证明的健壮性，因此可以保证分数阶微积分验证的高可靠性。

结束语 实数二项式系数的高阶逻辑形式化验证是实数二项式系数的一种新颖的分析方法。本文基于高阶逻辑定理证明器 HOL4，实现了实数二项式系数以及相关性质的形式化，这些形式化的性质被称作定理。它们可以用于证明分数阶微积分，分数阶微积分的形式化分析表明了实数二项式系数相关定理的有效性和实用性。

分数阶系统作为复杂系统，它的可靠性越来越受到人们的重视。实数二项式系数是分数阶微积分定义的重要组成部分。实数二项式系数和阶乘幂的形式化充实了 HOL4 的定理库，为分数阶系统的形式化分析提供了理论基础。本文研究的是实数二项式系数的形式化，也可以根据复数库研究复数域二项式系数的高阶逻辑形式化，提高验证复杂系统的能力。

参 考 文 献

[1] 王戟，李宣东. 形式化方法与工具专刊前言[J]. 软件学报，2011，22(6)：1121-1122

[2] 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

[3] 万哲先. 二项式系数和 Gauss 系数[J]. 数学通报，1994，10：1-6

[4] Podlubng I. Fractional Differential Equations[M]. Technical University of Kosice，Slovak Repubic，1999

[5] Harrison J. Theorem Proving with the Real Numbers [M]. Springer-Verlag，1998

[6] Graham，Knuth R L，Patashnik D E，et al. Concrete Mathematics：A Foundation for Computer Science[M]. 1994

[7] 万哲先. 介绍广义二项式系数[J]. 数学通报，2000(1)：34-37

[8] 赵春娜，李英顺，陆涛. 分数阶系统分析与设计[M]. 北京：国防工业出版社，2011

[9] Mhamdi T，Hasan O，Tahar S. On the Formalization of the Lebesgue Integration Theory in HOL[C]// Interactive Theorem Proving，volume 6172 of Lecture Notes in Computer Science. Springer，2010：387-402

[10] 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

[11] 王东风，王晓燕，韩璞. 锅炉-汽轮机系统的分数阶控制器设计[J]. 中国电机工程学报，2010 (5)：113-119

[12] 黄果，许黎，蒲亦非. 分数阶微积分在图像处理中的研究综述[J]. 计算机应用研究，2012，29(2)：414-420

[13] 殷德顺，任俊娟，和成亮，等. 基于分数阶微积分理论的软土应力-应变关系[J]. 岩石力学与工程学报，2009，28(A01)：2973-2979

[14] 孙建新. 阶乘幂多项式及其基本恒等式[J]. 绍兴文理学院学报，2004，24(7)：34-37

[15] Maione G，Lino P. New Tuning Rules for Fractional PI^{α} Controllers[J]. Nonlinear Dynamics，2007，49(1/2)：251-257

[16] 蒲亦菲. 分数阶微积分在现在信号分析与处理中应用的研究[D]. 成都：四川大学，2006

[17] Chang T-S，Singh M P. Seismic analysis of structures with a fractional derivative model of viscoelastic dampers[J]. Earthquake Engineering and Engineering Vibration，2002，1(2)：251-260

[18] Mandelbrot B B. The fractal geometry of nature[M]. San Francisco：Freeman，1982