函数矩阵及其微积分的高阶逻辑形式化

杨秀梅[1] 关 永[1] 施智平[1] 吴爱轩[1] 张倩颖[1] 张 杰[2]
(首都师范大学信息工程学院轻型工业机器人与安全验证北京市重点实验室 北京 100048)[1]
(北京化工大学信息科学与技术学院 北京 100029)[2]

摘 要 函数矩阵广泛应用于动态系统的建模与分析。传统的函数矩阵分析主要采用纸笔演算、数值计算和符号推导的方法,这些方法不能保证提供精确或正确的结果。高阶逻辑定理证明作为一种高可靠的形式化验证方法,可以克服以上不足。在高阶逻辑定理证明器HOL4中对函数向量和函数矩阵相关理论进行形式化,内容包括函数向量和函数矩阵及其连续性、微分、积分的形式化定义和相关性质的逻辑推理证明。为示范函数矩阵形式化的应用,最后给出机器人运动学中旋转矩阵微分公式的形式化验证。

关键词 函数矩阵,微积分性质,形式化验证,高阶逻辑定理证明
中图法分类号 TP301 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.11.005

Higher-order Logic Formalization of Function Matrix and its Calculus

YANG Xiu-mei[1] GUAN Yong[1] SHI Zhi-ping[1] WU Ai-xuan[1] ZHANG Qian-ying[1] ZHANG Jie[2]
(Beijing Key Laboratory of Light Industrial Robot and Safety Verification, 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]

Abstract Function matrix is widely employed in the modeling and analysis of dynamic system. Paper-pencil calculations, numerical calculations and symbolic algebra methods, which are used in traditional analysis of function matrix, cannot guarantee to provide accurate or correct results. Higher-order logic theorem proving, as a kind of highly reliable formal verification method, can overcome the above shortcomings. This paper formalized the related theories of function vector and function matrix in the higher-order logic theorem prover HOL4. Formal contents include the formal definitions and proving of function vector and function matrix, and their properties of continuity, differential and integral. The formal verification of the differential equation of rotation matrix in the robotic kinematics was given to illustrate the application of the formalization.

Keywords Function matrix, Calculus, Formal verification, Higher-order logic theorem proving

1 引言

函数矩阵理论广泛应用于动态系统的分析中,如控制系统[1-3]、能源系统[4,5]、机器人系统等。传统上对函数矩阵的分析主要采用纸笔演算以及基于计算机的数值计算或符号推导的方法。就现代社会中复杂的工程系统来说,纸笔演算很容易出现人为错误。数值方法[6]中浮点数的天然缺陷,加之运算次数受计算机内存资源的限制,使得数值分析法无法得到精确值。符号推导主要依赖于支持符号运算的计算机代数系统,它虽然避免了数值方法不精确的问题,但是这些代数系统中大量的程序并未经过完备的验证,难免存在错误。因此对于很多正确性和可靠性要求极高的动态系统,比如安全攸关的医学治疗机器人系统,传统方法并不能满足其可靠性和精确性要求。

形式化验证是一种高可靠的精确验证技术,近年来越来越多地被应用到众多关键系统的验证中,如自主机器人的安全区域算法的验证[7]、片上系统内存序列重组问题的验证[8]等。高阶逻辑定理证明是形式化验证方法中的一种,它用数学逻辑公式来表达所要验证的系统模型及其属性,具有很强的表达能力,能够形式化表示任何一种能被数学模型表示的系统。它以公认的逻辑公理和推理规则为基础构建形式化分析和证明过程,每个新加入定理证明器中的定理都经过严格

到稿日期:2015-09-10 返修日期:2016-01-29 本文受国际科技合作计划(2011DFG13000),国家自然科学基金项目(61170304,61472468,61572331),北京市科委项目(Z141100002014001),北京市教委科研基地建设项目(TJSHG201310028014),北京市属高等学校创新团队建设与教师职业发展计划项目(IDHT20150507)资助。

杨秀梅(1989-),女,硕士生,主要研究方向为形式化验证,E-mail:yangxml1991@sina.com;关 永(1966-),男,博士,教授,博士生导师,主要研究方向为电子系统健康状态预测与管理、形式化验证、高可靠嵌入式系统;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;吴爱轩(1990-),男,博士生,主要研究方向为形式化验证;张倩颖(1986-),女,博士,讲师,主要研究方向为形式化验证、实时操作系统;张 杰(1967-),女,硕士,副教授,主要研究方向为形式化验证。

证明，具有较高的可靠性和完备的正确性。然而定理证明系统的建模和推理能力依赖于应用领域的相关数学理论的形式化模型。因而，函数矩阵的形式化是使用定理证明技术形式化验证动态系统的基础，对其具有重要的理论意义和应用价值。

HOL4 系统[9]是目前最通用的定理证明器之一，其庞大的定理库（如超越函数库、limTheory 库等）使得它已具有很强的建模推理能力，加上新增的实数矩阵定理库[10]，为函数矩阵及其性质的形式化奠定了坚实的基础。实际上，刘振科等人[11]曾在 HOL4 中形式化过函数矩阵理论。然而其函数矩阵的数据类型被定义为 $(real\rightarrow real)'m'n$（$m,n$ 分别为函数矩阵的行数和列数），这种类型虽然表征了函数矩阵的每一个元素都是类型为 $real\rightarrow real$ 的函数，但是并不能表征出函数矩阵的自变量。当函数矩阵中含有多个自变量而只要求对其中一个变量进行微积分时，上述类型无法直接表示。另外，上述类型对于 HOL4 系统来说是一个全新的类型，与普通实数矩阵没有建立联系，不能利用实数矩阵已有的运算性质，因此需要形式化很多类似普通实数矩阵的基本运算性质。在 HOL4 系统已有比较完备的实数矩阵理论库[10]的情况下，这样做显然比较冗余。为弥补上述不足，本文提出将函数矩阵的数据类型形式化定义为 $real\rightarrow real'm'n$。这看似微小的不同，使得函数矩阵理论形式化的应用更加便捷和广泛，主要体现如下：假设 fm 是类型为 $real\rightarrow real'm'n$ 的函数矩阵，$fm(x)$ 便表示以 x 为自变量的函数矩阵。$fm(x)$ 作为一个整体，其返回类型是 $real'm'n$，这正是普通实数矩阵的类型，函数矩阵本身的加、减、乘等基本运算性质便无须再形式化定义和证明，可以通过 $fm(x)$ 的形式直接使用普通实数矩阵库中相应定理进行推理演算。另一方面，本文形式化的函数矩阵微积分理论不仅可以方便地应用于只含有一个实数变量的函数矩阵的微积分，当函数矩阵中含有多个实变量时，也可以简便地对其中任何一个变量进行微积分运算。

本文第 2 节在高阶逻辑定理证明器中建立了函数矩阵和函数向量类型及其连续性的形式化模型；第 3 节给出了函数向量和函数矩阵的微分定义及性质的形式化；第 4 节在 HOL4 中形式化了函数向量和函数矩阵的积分及其性质；第 5 节以机器人旋转矩阵的微分公式的验证为例，展示了本文函数矩阵形式化的实际应用；最后总结全文。

2 函数矩阵及其连续性

以实变量 x 的函数为元素的矩阵，如

$$A(x)=\begin{pmatrix} a_{11}(x) & \cdots & a_{1n}(x) \\ \vdots & \ddots & \vdots \\ a_{m1}(x) & \cdots & a_{mn}(x) \end{pmatrix}$$

称为函数矩阵[12]，其中 $a_{ij}(x)$ 为该矩阵的元素。函数矩阵 $A(x)$ 在数学上表示从一个实数 x 到一个实数矩阵的映射。在 HOL4 中，用“$\alpha\rightarrow\beta$”来表示映射或函数的类型。根据本文思想，将函数矩阵的类型形式化定义为 $Hol\_type: real\rightarrow real'm'n$。其中 $real$ 表示实数类型，$real'm'n$ 表示 m 行 n 列的实数矩阵。

2.1 函数矩阵的连续性

众所周知，实函数连续性的讨论是函数的微积分理论的基础，对于函数矩阵，其连续性一样重要。接下来将形式化分析函数矩阵的连续性。

定义 1 若函数矩阵 $A(x)$ 的每个元素 $a_{ij}(x)$ 在 x_0 点都连续，则称函数矩阵 $A(x)$ 在 x_0 点连续。其形式化定义为：

Val fmatrix_contl_def = |− ∀ *FM x*. *fmatrix_contl FM x*

〈=〉∀ *ij*. *i*<*dimindex*(:'*m*) ∧ *j*<*dimindex*(:'*n*)

==>((λ*x*. *FM*(*x*)'*i*'*j*) *contl x*)

上述定义中，*FM* 表示类型为 *real*−>*real*['*n*]['*m*] 的函数矩阵，*x* 是类型为 *real* 的实数；*dimindex*(:'*m*) 和 *dimindex*(:'*n*) 分别表示维数 *m* 和 *n*；*contl* 是 HOL4 中函数连续的形式化表示，这里用 *fmatrix_contl* 形式化表示函数矩阵的连续，(*fmatrix_cont*(*FMx*)) 表示 *FM* 在 *x* 处连续。

容易得知，函数矩阵的连续具有函数连续的类似性质。表 1 列出函数矩阵的连续性相关性质的形式化。这些性质的形式化验证确保了函数矩阵连续性形式化定义的正确性。

表 1 函数矩阵连续性质的相关引理

性质描述	HOL4 形式化
1. 常数矩阵是连续的	|− ∀ A x. fmatrix_contl(λx. A) x
2. 若函数矩阵 FA、FB 都在 x 处连续，则(FA+FB)也在 x 处连续	|− ∀ FA FB x. (fmatrix_contl FAx) ∧ (fmatrix_contl FB x) ==>(fmatrix_contl(λx. FA(x)+FB(x)) x)
3. 若函数矩阵 FA、FB 都在 x 处连续，则(FA×FB)也在 x 处连续	|− ∀ FA FB x. (fmatrix_contlFAx) ∧ (fmatrix_contl FB x) ==>(fmatrix_contl(λx. FA(x) * *FB(x)) x)
4. 若函数矩阵 FA 在 x 处连续，则~FA 也在 x 处连续	|− ∀ FA x. (fmatrix_contl FA x) ==> (fmatrix_contl(λx. ~FA(x)) x)
5. 若函数矩阵 FA 和函数 f 都在 x 处连续，则 FA 在 f(x)处也连续	|− ∀ FA f x. (fmatrix_contl FA x) ∧ (f contl x) ==>(fmatrix_contl(λx. FA(f x)) x)

2.2 函数向量及其连续性

以实变量 x 的函数为元素的向量，如

$$V(x)=(a_1(x),a_2(x),\cdots,a_n(x))$$

称为函数向量，其中 $a_i(x)$ 为函数向量的元素。函数向量 $V(x)$ 可以看成一个实数 x 到实数向量的映射。类似函数矩阵的类型定义，函数向量在 HOL4 中的形式化类型是 *Hol_type*: *real*→*real'n*，其中 *real'n* 表示 *n* 维向量。

定义 2 与函数矩阵类似，若函数向量的每个元素在某一点都连续，则称函数向量在这一点是连续的。其形式化定义为：

Val fvector_contl_def = |− ∀ *FV x*. *fvector_contl FV x* 〈=〉∀ *i*. *i*<*dimindex*(:'*n*)==>((λ*x*. *FV*(*x*)'*i*) *contl x*)

其中，*FV* 表示类型为 *real*−>*real*['*n*] 的函数向量；*x* 为类型为 *real* 的实数；*dimindex*(:'*n*) 表示函数向量的维数是 *n*。(*fvector_contlFV x*) 形式化表示函数向量 *FV* 在 *x* 处连续。

函数向量的连续性质也与函数矩阵类似，已在 HOL4 中形式化验证过，这里不再一一赘述。

3 函数矩阵的微分

若函数矩阵或函数向量的每个元素都是可微的，则称函数矩阵或函数向量也是可微的。本节将讨论函数向量和函数矩阵的微分及其运算性质的形式化。在 HOL4 中对运算性质的形式化证明或验证的过程是：先将需要证明的性质按照

HOL4 的形式化规则描述成一个个逻辑命题，再将这些命题当成需要证明的形式化目标，在 HOL4 中找到该目标的一个证明过程。由于篇幅限制，文中只对较复杂、难理解的性质的证明给出步骤，其余的只给出已验证性质的形式化验证目标。

3.1 函数向量微分的形式化

3.1.1 函数向量导数的定义

定义 3 设函数向量 $V(x)=(a_i(x))_n(i=1,2,\cdots,n)$，如果所有的元素 $a_i(x)$ 都是变量 x 的可微函数，则称函数向量 $V(x)$ 可微。其形式化定义为：

Val fvector_differentiable_def = |- ∀FV x. FV fvector_differentiable x <=> ∀i. i<dimindex(:'n) ==> ((λx. FV(x)' i) differentiable x)

其中，*FV* 表示类型为 *real->real['n]* 的函数向量，*x* 是类型为 *real* 的实数。HOL4 中，*differentiable* 表示实数函数可微，这里用 *fvector_differentiable* 形式化表示函数向量可微。

定义 4 若函数向量 $V(x)$ 可微，则称

$$V'(x)=\frac{\mathrm{d}}{\mathrm{d}x}V(x)=(\frac{\mathrm{d}}{\mathrm{d}x}a_i(x))_n \tag{1}$$

为函数向量 $V(x)$ 对变量 x 的导数。利用 limTheory 库中实数函数导数的定义可将函数向量导数的定义形式化为：

Val fvector_diffl_def = |- ∀FVV x. (FV fvector_diffl V)(x) <=> ∀i. i<dimindex(:'n) ==> ((λx. FV(x)'i) diffl (V'i))(x)

其中，*FV* 表示类型为 *real->real['n]* 的函数向量，*V* 是类型为 *real['n]* 的向量，*x* 是类型为 *real* 的实数。*diffl* 是 HOL4 中函数求导的中缀表示符。这里形式化定义 *fvector_diffl* 为函数向量求导的中缀表示符，*(FV fvector_diffl V) x* 表示 *FV* 在 *x* 处的导数为向量 *V*。

3.1.2 函数向量的导数性质

函数向量导数的运算性质有很多，下面将主要给出几条简单且常用的性质的形式化，如表 2 所列，这些性质都已经在 HOL4 系统中证明。无特别说明时，下面的形式化中 *FV*，*FV1* 和 *FV2* 表示函数向量，*V*，*V1* 和 *V2* 表示导数向量或常向量。

表 2 函数向量导数性质的相关引理

性质描述	HOL4 形式化
常数向量导数为 0 向量	|- ∀ V x. ((λx. V) fvector_diffl(VECTOR_0))(x)
函数向量导数的唯一性	|- ∀ FV x V1 V2. (FV fvector_diffl V1)(x) ∧ (FV fvector_diffl V2)(x) ==> (V1=V2)
$\frac{\mathrm{d}}{\mathrm{d}x}(cV(x))=cV'(x)$	|- ∀ V c x FV. (FV fvector_diffl V)(x) ==> ((λx. c * FV(x)) fvector_diffl(c * V))(x)
$\frac{\mathrm{d}}{\mathrm{d}x}(\sim V(x))=\sim V'(x)$	|- ∀ FV x V. (FV fvector_diffl V)(x) ==> ((λx. ~FV(x)) fvector_diffl(~V))(x)
$\frac{\mathrm{d}}{\mathrm{d}x}(V_1(x)\pm V_2(x))=V'_1(x)\pm V'_2(x)$	|- ∀ FV1 FV2 x V1 V2. ((FV1 fvector_diffl V1)x) ∧ ((FV2 fvector_diffl V2)(x)) ==> (((λx. FV1(x)±FV2(x)) fvector_diffl(V1±V2))(x))

3.2 函数矩阵微分的形式化

3.2.1 函数矩阵导数的定义

定义 5 设函数矩阵 $A(x)=(a_{ij}(x))_{m\times n}(i=1,2,\cdots,m;j=1,2,\cdots,n)$，如果所有的元素 $a_{ij}(x)$ 都是变量 x 的可微函数，则称函数矩阵 $A(x)$ 可微。其形式化定义为：

Val fmatrix_differentiable_def = |- ∀ FM x. FM-fmatrix_differentiable x <=> ∀i j. i<dimindex(:'m) ∧ j<dimindex(:'n) ==> ((λx. FM(x)'i'j) differentiable x)

其中，*FM* 表示类型为 *real->real['n]['m]* 的函数矩阵，*x* 是类型为 *real* 的实数。这里用 *fmatrix_differentiable* 形式化表示函数矩阵可微。

定义 6 若函数矩阵 $A(x)$ 可微，则称

$$A'(x)=\frac{\mathrm{d}}{\mathrm{d}x}A(x)=(\frac{\mathrm{d}}{\mathrm{d}x}a_{ij}(x))_{m\times n} \tag{2}$$

为函数矩阵 $A(x)$ 对变量 x 的导数。同函数向量导数的形式化定义类似，函数矩阵导数形式化定义为：

Val fmatrix_diffl_def = |- ∀ FMA x. (FM fmatrix_diffl A)(x) <=> ∀i j. i<dimindex(:'m) ∧ j<dimindex(:'n) ==> ((λx. FM(x)'i'j) diffl(A'i'j))(x)

其中，*FM* 表示类型为 *real->real['n]['m]* 的函数矩阵，*A* 是类型为 *real['n]['m]* 的矩阵。这里形式化定义 *(FM fmatrix_diffl A) x* 表示 *FM* 在 *x* 处的导数为矩阵 *A*。

3.2.2 函数矩阵导数的性质

根据上述函数矩阵导数的形式化定义，下面将给出函数矩阵导数的相关重要性质的形式化。无特别说明时，下面的形式化中 *FM*，*FA* 和 *FB* 表示函数矩阵，*M*，*A* 和 *B* 表示导数矩阵或常矩阵。*c* 和 *k* 为常系数，*f* 为实数函数。

性质 1 函数矩阵在 *x* 处可导，则在 *x* 处一定连续。

|- ∀fm m x. ((fm fmatrix_diffl m)(x)) ==> (fmatrix_contl fm x)

性质 2 常数矩阵的导数为零矩阵。

|- ∀Ax. ((λx. A) fmatrix_diffl(MAT 0))(x)

性质 3

$$\frac{\mathrm{d}}{\mathrm{d}x}(cA(x))=c\frac{\mathrm{d}}{\mathrm{d}x}A(x) \tag{3}$$

*|- ∀FMM c x. ((FM fmatrix_diffl M)(x)) ==> (((λx. c * FM(x)) fmatrix_diffl(c * M))(x))*

性质 4

$$\frac{\mathrm{d}}{\mathrm{d}x}(A(x)\pm B(x))=\frac{\mathrm{d}}{\mathrm{d}x}A(x)\pm\frac{\mathrm{d}}{\mathrm{d}x}B(x) \tag{4}$$

|- ∀FA FB x A B. ((FA fmatrix_diffl A)(x)) ∧ ((FB fmatrix_diffl B)(x)) ==> (((λx. FA(x)±FB(x)) fmatrix_diffl(A±B))(x))

性质 5 函数矩阵导数的唯一性。

|- ∀FM x A B. (FM fmatrix_diffl A)(x) ∧ (FM fmatrix_diffl B)(x) ==> (A=B)

性质 6 相等的两函数矩阵在同一处的导数也相等。

|- ∀FA FB A x. (FA=FB) ∧ (FA fmatrix_diffl A) x ==> (FB fmatrix_diffl A)x

性质 7

$$\frac{\mathrm{d}}{\mathrm{d}x}(A_1(x)+\cdots+A_n(x))=\frac{\mathrm{d}}{\mathrm{d}x}A_1(x)+\cdots+\frac{\mathrm{d}}{\mathrm{d}x}A_n(x) \tag{5}$$

|- ∀m x FMM. (∀r. 0<= r ∧ r<m ==> (((λx. FM r x) fmatrix_diffl(M r))(x))) ==> (((λx. (MSUM

(count m)(λm. FM m x))) fmatrix_diffl(MSUM(count m)(λr. M r))) x)

上述性质的形式化中，FM是带有编号的函数矩阵，其类型为num->real->real['n]['m]。M类型为num-> real['n]['m]，(M r)表示第 r 个函数矩阵(FM r x)在 x 处的导数矩阵。MSUM形式化表示多个矩阵依次求和。

性质 8

$$\frac{d}{dx}(k_1A_1(x)+\cdots+k_nA_n(x))=k_1\frac{d}{dx}A_1(x)+\cdots+k_n\frac{d}{dx}A_n(x)_1 \quad (6)$$

|- ∀m x FM M c. (∀r. 0 <= r ∧ r<m ==>(((λx. FM r x) fmatrix_diffl(M r))(x)))==>(((λx. (MSUM (count m) (λm. (c m) * (FM m x)))) fmatrix_diffl (MSUM(count m)(λr. (c r) * (M r)))) x)

性质 8 与性质 7 类似，只是每个函数矩阵都乘了一个常系数。

性质 9

$$\frac{d}{dx}(f(x)\times A(x))=f'(x)\times A(x)+f(x)\times\frac{d}{dx}A(x) \quad (7)$$

|- ∀FM M flx. ((f diffl l)x) ∧ ((FM fmatrix_diffl M) x)==>(((λx. f(x) * FM(x)) fmatrix_diffl(l * FM(x)+f(x) * M))x)

性质 10

$$\frac{d}{dx}(A(x)\times B)=(\frac{d}{dx}A(x))\times B \quad (8)$$

|- ∀FA AB x. ((FA fmatrix_diffl A)(x))==> (((λx. (FA(x)) * * B) fmatrix_diffl(A ** B))(x))

性质 11

$$\frac{d}{dx}(A(x)\times B(x))=(\frac{d}{dx}A(x))\times B(x)+A(x)\times\frac{d}{dx}B(x) \quad (9)$$

|- ∀FA FB AB x. ((FA fmatrix_diffl A)(x)) ∧ ((FB fmatrix_diffl B)(x))==>(((λx. (FA(x)) ** (FB (x))) fmatrix_diffl(A ** FB(x)+(FA(x)) ** B))(x))

性质 12

$$\frac{d}{dx}(A(f(x)))=(\frac{d}{du}A(u))\cdot f'(x) \quad (10)$$

|- ∀FMM flx. ((FM fmatrix_diffl M)(f x)) ∧ ((fdiffl l)x)==>(((λx. FM(f(x))) fmatrix_diffl (M * l))(x))

性质 13

$$\frac{d}{dx}A^{-1}(x)=-A^{-1}(x)\times\frac{dA(x)}{dx}\times A^{-1}(x) \quad (11)$$

|- ∀ FMM x. ((FM fmatrix_diffl M) x) ∧ (fmatrix_differentiable(λx. MATRIX_INV(FM(x)))==> (((λx. MATRIX_INV(FM(x))) fmatrix_diffl (-MATRIX_INV(FM(x)) ** M ** MATRIX_INV(FM(x))))x)

性质 13 的形式化验证稍显复杂，它先使用逆矩阵的性质定理 MATRIX_INV 证得 $A(x)\times A^{-1}(x)=I$(I 为单位矩阵)；再利用上述函数矩阵的导数性质 6 和式(11)，可得 $A(x)\times\frac{d}{dx}A^{-1}(x)=-\frac{dA(x)}{dx}\times A^{-1}(x)$；最后使用矩阵定理库中相关定理对目标等式两边同时左乘 $A^{-1}(x)$，可证得目标。

3.3 函数向量和函数矩阵的混合运算导数性质

在实际动态系统的应用中，函数向量和函数矩阵的导数运算并不总是单一使用的，有时也需要函数向量和函数矩阵的混合运算的导数性质。这里给出两个最主要的混合运算的导数性质的形式化。

性质 14

$$\frac{d}{dx}(V(x)\times A(x))=V'(x)\times A(x)+V(x)\times A'(x) \quad (12)$$

|- ∀V FV FM Mx. ((FV fvector_diffl V)(x)) ∧ ((FM fmatrix_diffl M)(x))==>(((λx. FV(x) ** FM (x))fvector_diffl(V ** FM(x)+FV(x) ** M))x)

性质 15

$$\frac{d}{dx}(A(x)\times V(x))=A'(x)\times V(x)+A(x)\times V'(x) \quad (13)$$

|- ∀V FV FM Mx. ((FV fvector_diffl V)(x)) ∧ ((FM fmatrix_diffl M)(x))==>(((λx. FM(x) ** FV (x)) fvector_diffl(M ** FV(x)+FM(x) ** V))x)

函数向量和函数矩阵导数的性质是其实际应用的理论前提。本节导数性质的形式化验证不仅为实际使用函数向量和函数矩阵导数运算性质进行关键系统的形式化验证减少了大量人工干预，还确保了函数向量和函数矩阵微分和导数的形式化定义的正确性。

4 函数矩阵的积分

4.1 函数向量的积分的形式化

4.1.1 函数向量积分的定义

定义 7 设函数向量 $V(x)=(a_i(x))_n(i=1,2,\cdots,n)$，如果所有的元素 $a_i(x)$ 都在某一区间 $[a,b]$ 上 $(a\leqslant b)$ 存在积分，则称函数向量 $V(x)$ 在此区间上可积。其形式化定义为：

Val fvector_integrable_def=|- ∀ FV a b x. fvector_integrable(a,b) FV <=> ∀i. (a<=b) ∧ (i<dimindex(:'n)) ==> ∃V:real['n]. Dint(a,b)(λx:real. FV(x) ' i)(V'i)

其中，FV 表示类型为 real->real['n] 的函数向量，a 和 b 表示积分区间的边界值。HOL4 中，Dint(a,b) f k 形式化表示 f 在区间 [a,b] 上的积分为 k，integrable 表示实数函数可积。这里用 fvector_integrable 形式化表示函数向量可积。

定义 8 若函数向量 $V(x)$ 在区间 $[a,b]$ $(a\leqslant b)$ 上可积，则称

$$\int_a^b V(x)dx=(\int_a^b a_i(x)dx)_n, i=1,2,\cdots,n \quad (14)$$

为函数向量 $V(x)$ 在区间 $[a,b]$ 上的积分。根据 Gauge 积分库[13]中实数函数积分的定义可将函数向量积分的定义形式化为：

Val fvector_integral_def= |- ∀a b FV x. fvector_integral(a,b) FV= @V. ∀i. a<= b ∧ i<dimindex(:'n)==> Dint(a,b)(λx. FV(x)'i)(v'i)

其中，FV 表示类型为 real->real['n] 的函数向量，V 是 FV 在区间 [a,b] 上的积分。integral 在 HOL4 中表示函数积分，这里定义 fvector_integral(a,b) FV 形式化表示 FV 在区间 [a,b] 上的积分。

4.1.2 函数向量积分的性质

性质 16 零向量在任意区间上的积分都为零向量。

|－∀ a b x i. (a<=b) ∧ (i<dimindex(:'n)) ==> Dint(a,b)(λx. fv(x)'i)(v'i)

性质 17 若$\int_a^b V(x)\mathrm{d}x=v$,则$\int_a^b c\cdot V(x)dx=c\cdot v$。

|－∀ fv va b c:real x i. (a<=b) ∧ (i<dimindex(:'n)) ==>Dint(a,b)(λx. fv(x)'i)(v'i) ==>Dint(a,b)(λx. (c * fv(x))'i)(c * v'i)

性质 18 若$\int_a^b V_1(x)\mathrm{d}x=v_1$,并且$\int_a^b V_2(x)\mathrm{d}x=v_2$,则$\int_a^b (V_1(x)\pm V_2(x))\mathrm{d}x=v_1\pm v_2$。

|－∀ fv1 fv2 v1 v2 a b c:real x i. (a<=b) ∧ (i<dimindex(:'n)) ==> (Dint(a,b)(λx. fv1(x)'i)(v1'i)) ∧ (Dint(a,b)(λx. fv2(x)'i)(v2'i)) ==>Dint(a,b)(λx. (fv1(x)+fv2(x))'i)(v1'i+v2'i)

4.2 函数矩阵的积分的形式化

4.2.1 函数矩阵积分的定义

定义 9 设函数矩阵$A(x)=(a_{ij}(x))_{m\times n}(i=1,2,\cdots,m;j=1,2,\cdots,n)$,如果所有的元素$a_{ij}(x)$都在某一区间$[a,b]$上$(a\leqslant b)$存在积分,则称函数矩阵$A(x)$在此区间上可积。其形式化定义为:

Val fmatrix_integrable_def=|－∀ *FM a b. fmatrix_integrable(a,b) FM*(=) ∀ *i j.* (a<=b) ∧ (i<*dimindex*(:'m)) ∧ (j<*dimindex*(:'n)) ==> ∃*M. Dint*(a,b)(λx:*real. FM*(x)'i'j)(M'i'j)

其中,*FM*表示类型为*real*－>*real*['n]['m]的函数矩阵,*a* 和 *b* 是积分区间的边界值,*M* 为 *FM* 在区间$[a,b]$上的积分。*fmatrix_integrable*(*a*,*b*) *FM*形式化表示函数矩阵 *FM* 在区间$[a,b]$上可积。

定义 10 若函数矩阵 *FM* 在区间$[a,b](a\leqslant b)$上可积,则称

$$\int_a^b A(x)\mathrm{d}x=\left(\int_a^b a_{ij}(x)\mathrm{d}x\right)_{m\times n},i=1,2,\cdots,m,j=1,2,\cdots,n \tag{15}$$

为函数矩阵$A(x)$在区间$[a,b]$上的积分。同函数向量积分的定义类似,函数矩阵积分的定义被形式化为:

Val fmatrix_integral_def=|－∀ *a b FM. fmatrix_integral*(*a*,*b*) *FM*= @*M.* ∀ *i j.* (a<=b) ∧ (i<*dimindex*(:'m)) ∧ (j<*dimindex*(:'n)) ==> *Dint*(*a*,*b*)(λx:*real. FM*(x)'i'j)(M'i'j)

其中,*fmatrix_integral*(*a*,*b*) *FM*形式化表示函数矩阵 *FM* 在区间$[a,b]$上的积分。

4.2.2 函数矩阵积分的性质

性质 19 若函数矩阵$A(x)$在区间$[a,b]$上连续,则$A(x)$在$[a,b]$上可积。

|－∀ *FM a b x.* ((a<=b) ∧ (a<=x) ∧ (x<=b) ==> (*fmatrix_contl FM x*)) ==> (*fmatrix_integrable*(*a*,*b*) *FM*)

性质 20 若$\int_a^b A(x)\mathrm{d}x=A$,则$\int_a^b c\cdot A(x)\mathrm{d}x=c\cdot A$。

|－∀ *fmma b c.* (a<=b) ∧ (i<*dimindex*(:'m)) ∧ (j<*dimindex*(:'n)) ==> *Dint*(*a*,*b*)(λx. *fm*(x)'i'j)(m' i'j) ==>*Dint*(*a*,*b*)(λx. (c * *fm*(x))'i' j)(c * m'i' j)

性质 21 若$\int_a^b A(x)\mathrm{d}x=A$,并且$\int_a^b B(x)\mathrm{d}x=B$,则$\int_a^b (A(x)\pm B(x))\mathrm{d}x=A\pm B$。

|－∀ *FAFBAB a b.* (a<=b) ∧ (i<*dimindex*(:'m)) ∧ (j<*dimindex*(:'n)) ==> (*Dint*(*a*,*b*)(λx. *FA*(x)'i'j)(A'i' j)) ∧ (*Dint*(*a*,*b*)(λx. *FB*(x)'i' j)(B'i' j)) ==> *Dint*(*a*,*b*)(λx. (*FA*(x)+*FB*(x))'i' j)(A'i'j+B'i'j)

同函数向量和函数矩阵的微分运算性质的形式化证明类似,本节函数向量和函数矩阵的积分运算性质的形式化验证确保了相关形式化定义的正确性,同时也为以后直接使用提供了方便。

5 应用:旋转矩阵的导数

函数矩阵是动态系统分析的基础,本文提出的函数矩阵形式化理论实现为 HOL 系统的一个定理库,可作为动态系统形式化分析的基础。旋转运动是机器人等刚体机构最主要的运动形式,通常用旋转矩阵来描述。刚体旋转矩阵的导数在机器人等机构的运动学和动力学分析中应用广泛。为说明所实现的定理库的正确性和实用性,本节在 HOL 系统中用所实现的函数矩阵定理库表示刚体旋转矩阵及其微分公式,并给出微分公式的形式化证明。

设机器人连杆(视为刚体)绕固定轴做旋转运动,$\boldsymbol{\omega}(\boldsymbol{\omega}\in R^3)$表示旋转轴方向的单位矢量,$t(t\in R)$为旋转角度。以单位角速度绕$\boldsymbol{\omega}$轴旋转角度$t$的旋转矩阵表示为$\boldsymbol{R}(\boldsymbol{\omega},t)=\mathrm{e}^{t\hat{\boldsymbol{\omega}}}$,其中$\hat{\boldsymbol{\omega}}$表示 3 维列向量$\boldsymbol{\omega}$的反对称矩阵,满足$\hat{\boldsymbol{\omega}}^3=-\hat{\boldsymbol{\omega}}$。通常情况下为了表达方便,取$\|\boldsymbol{\omega}\|=1$($\boldsymbol{\omega}$范数为 1)。根据罗德里格斯(Rodrigues)公式:

$$\mathrm{e}^{t\hat{\boldsymbol{\omega}}}=I+\hat{\boldsymbol{\omega}}\sin t+\hat{\boldsymbol{\omega}}^2(1-\cos t)$$

则旋转矩阵的导数为:

$$\frac{\mathrm{d}(\mathrm{e}^{t\hat{\omega}})}{\mathrm{d}t}=\hat{\omega}-\mathrm{e}^{t\hat{\omega}} \tag{16}$$

对其进行形式化分析和验证的过程可分为两步。

(1)形式化表示作为验证目标的式(16),如下:

|－∀ *tx.* (*norm*(x)=&1) ==> ((λt. *matrix_exp*(t * (*VECTOR_2_SSM x*))) *fmatrix_diffl*((*VECTOR_2_SSM x*) ** *matrix_exp*(t * (*VECTOR_2_SSM x*))))(t)

其中,*t* 表示旋转角度,*x* 表示旋转轴方向的单位矢量,(*norm*(x)=&1)形式化表示矢量 *x* 的范数为 1,它是 Rodrigues 公式存在的前提条件。*matrix_exp*(*t* * (*VECTOR_2_SSM x*))形式化表示$\mathrm{e}^{t\hat{x}}$,其中(*VECTOR_2_SSM x*)形式化表示矢量 *x* 的反对称矩阵。

(2)形式化证明此目标:先使用 HOL4 的重写策略重写 Rodrigues 公式在 HOL4 中对应的形式化定理 SSM_MATRIX_EXP,将$\mathrm{e}^{t\hat{x}}$代入证明目标中;再利用函数矩阵导数的性质 2－性质 4 等对应的定理,以及超越函数库中相关三角函数微分的定理(例如 DIFF_EXP,DIFF_COS 等),形式化证明得出$\frac{\mathrm{d}(\mathrm{e}^{t\hat{\omega}})}{\mathrm{d}t}=\hat{\mathbf{e}}\cos t+\hat{\boldsymbol{\omega}}^2\sin t$;最后利用之前已形式化证明

的$\hat{\omega}^3=-\hat{\omega}$和相关的普通函数矩阵的性质定理证明$\hat{\omega}\cdot e^{t\hat{\omega}}$也等于$\hat{\omega}\cos t+\hat{\omega}^2\sin t$，便可得证目标。

本文提出的函数矩阵形式化方法也可以用于多变量函数矩阵对其中一个变量求偏导，这里给出含有两个实数变量 t_1 和 t_2 的函数矩阵($e^{t_1\hat{\omega}}\cdot e^{t_2\hat{\omega}}$)对 t_1 的导数的形式化验证。

$$\frac{d(e^{t_1\hat{\omega}}\cdot e^{t_2\hat{\omega}})}{d(t_1)}=\hat{\omega}\cdot e^{t_1\hat{\omega}}\cdot e^{t_2\hat{\omega}} \tag{17}$$

其验证目标在 HOL4 中的形式化描述为：

```
|- ∀ t1 t2 x. (norm(x)=&1)==>((λt1. matrix_exp
(t1 * (VECTOR_2_SSMx)) ** matrix_exp(t2 * (VECTOR_
2_SSM x)))fmatrix_diffl((VECTOR_2_SSM x) ** ma-
trix_exp(t1 * (VECTOR_2_SSM x)) ** matrix_exp(t2 *
(VECTOR_2_SSM x))))(t1)
```

含有两个实数变量的函数矩阵 M 只要以($\lambda t1.\ M$) 的形式便可以方便地表达出微分变量为 t_1，避免了类型形式化为 $(real\to real)'m'n$ 的函数矩阵混淆微分变量的问题。上述目标主要利用式(16) 的结果和函数矩阵导数性质 10 即可证明，其得证的结果显示如图 1 所示。

```
〉val it=
    Initial goal proved.      |-!t1 t2 x.
        〈norm x=1〉==〉
        〈〈\t1.
            matrix_exp 〈t1 * VECTOR_2_SMM x〉 **
            matrix_exp 〈t2 * VECTOR_2_SMM x〉 fmatrix_diffl
        〈VECTOR_2_SSM x ** matrix_exp 〈t1 * VECTOR_2_
         SSM x〉 ** matrix_exp 〈t2 * VECTO_2_SMM x〉〉〉 t1 :
         proof
```

图 1　证明结果

图 1 不仅显示了式(17)得以验证，同时也说明了式(16)已正确通过 HOL 系统的形式化验证，否则 HOL 无法使用式(16)证明式(17)。另外，式(16)和式(17)使用本文实现的定理库得以正确验证，也验证了本文实现的定理库的正确性和有效性。

结束语　本文提出类型为 $real\to real'm'n$ 的函数矩阵和类型为 $real\to real'n$ 的函数向量的高阶逻辑形式化，给出了函数矩阵和函数向量连续、微分及积分的定义、性质的形式化，并在 HOL4 中形成定理库，其可直接加载使用。本文提出的函数矩阵形式化方法可以继承实数矩阵形式化理论的大部分内容，从而避免了大量重复性工作。另一方面，函数矩阵和函数向量的连续、积分性质的高阶逻辑形式化是其他任何公开发表的文献中所未涉及的。这部分内容丰富和完善了函数矩阵和函数向量的形式化理论体系，拓宽了其形式化理论的应用范围。同时，本文较为完整和简洁的函数矩阵高阶逻辑形式化理论增强了 HOL4 高阶逻辑定理证明器在相关领域的建模和推理能力，对未来验证相关领域的关键系统具有重要意义。

参 考 文 献

[1] 胡寿松. 自动控制原理[M]. 北京：科学出版社，2008

[2] Huang Ke-jin, Qian Ji-xin, Sun You-xian, et al. A kind of theoretical derivation method of rectifying column transfer function matrix[J]. Journal of Zhejiang University, 1994, 28(3): 253-261 (in Chinese)
黄克谨，钱积新，孙优贤，等. 一种精馏塔传递函数矩阵的理论推导方法[J]. 浙江大学学报，1994，28(3)：253-261

[3] Shen Yu-ling. Multivariable control system analysis and design based on the equivalent transfer function[D]. Shanghai: Shanghai Jiaotong University, 2012(in Chinese)
沈玉玲. 基于等价传递函数的多变量控制系统分析与设计[D]. 上海：上海交通大学，2012

[4] Vladimir N, Sidorova Sergey M, et al. Discrete-analytic solution of unsteady-state heat conduction transfer problem based on a theory of matrix function [J]. Procedia Engineering, 2015, 111: 726-733

[5] Hu Liang, Gu Ming, Li Li. Proper orthogonal decomposition of the wind field based on the coherence function matrix [J]. Journal of Vibration Engineering, 2010, 23(1): 64-68(in Chinese)
胡亮，顾明，李黎. 基于相干函数矩阵的风场本征正交分解[J]. 振动工程学报，2010，23(1)：64-68

[6] Babolian E, Fattahzadeh F. Numerical solution of differential equations by using Chebyshev wavelet operational matrix of integration[J]. Applied Mathematics & Computation, 2007, 188: 417-426

[7] Taubig H, Frese U, Hertzberg C, et al. Guaranteeing functional safety: design for provability and computer-aided verification [J]. Autonomous Robots, 2012, 32(3): 303-331

[8] Hasan O, Tahar S, et al. Formal Reliability Analysis Using Theorem Proving [J]. IEEE Transactions on Computers, 2010, 59 (5): 579-592

[9] Gordon M, Melham T. Introduction to HOL: A Theorem Proving Environment for Higher-Order Logic [M]. Cambridge: Cambridge Univ. Press, 1993

[10] Shi Z, Zhang Y, Liu Z, et al. Formalization of Matrix Theory in HOL4[J]. Advances in Mechanical Engineering, 2014, 6: 1-16

[11] Shi Zhi-ping, Liu Zhen-ke, Guan Yong, et al. Formalization of Function Matrix Theory in HOL[J]. Advances in Mechanic Engineering, 2014, 3: 1-16

[12] 程云鹏，张凯院，徐仲. 矩阵论(第三版)[M]. 西安：西北工业大学出版社，2006

[13] Gu Wei-qing, Shi Zhi-ping, Guan Yong, et al. Formalization of Gauge Integration Theory in HOL4 [J]. Computer Science, 2013, 40(2): 191-194(in Chinese)
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