Formalizing the Matrix Inversion Based on the Adjugate Matrix in HOL4

Liming Li, Zhiping Shi, Yong Guan, Jie Zhang, Hongxing Wei

▶ **To cite this version:**

Liming Li, Zhiping Shi, Yong Guan, Jie Zhang, Hongxing Wei. Formalizing the Matrix Inversion Based on the Adjugate Matrix in HOL4. 8th International Conference on Intelligent Information Processing (IIP), Oct 2014, Hangzhou, China. pp.178-186, 10.1007/978-3-662-44980-6_20 . hal-01383331

HAL Id: hal-01383331

https://inria.hal.science/hal-01383331v1

Submitted on 18 Oct 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Formalizing the Matrix Inversion Based on the Adjugate Matrix in HOL4

Liming LI[1], Zhiping SHI[1⋆], Yong GUAN[1], Jie ZHANG[2], and Hongxing WEI[3]

[1] Beijing Key Laboratory of Electronic System Reliability Technology, Capital Normal University, Beijing 100048, China
lilimінga@126.com, shizhiping@gmail.com
[2] College of Information Science & Technology, Beijing University of Chemical Technology, Beijing 100029, China
[3] School of Mechanical Engineering and Automation, Beihang University, Beijing 100083, China

Abstract. This paper presents the formalization of the matrix inversion based on the adjugate matrix in the HOL4 system. It is very complex and difficult to formalize the adjugate matrix, which is composed of matrix cofactors. Because HOL4 is based on a simple type theory, it is difficult to formally express the sub-matrices and cofactors of an n-by-n matrix. In this paper, special n-by-n matrices are constructed to replace the $(n-1)$-by-$(n-1)$ sub-matrices, in order to compute the cofactors, thereby, making it possible to formally construct aadjugate matrices. The Laplace's formula is proven and the matrix inversion based on the adjugate matrix is then inferred in HOL4. The paper also presents formal proofs of properties of the invertible matrix.

Keywords: Formal verification, Theorem proving, Matrix inversion, HOL4, Adjugate matrix

1 Introduction

Matrix theory is widely applied in many areas, and a great deal of research and development is currently being conducted on vector, matrix, and space transformation in some theorem provers. Yatsuka Nakamura et al. presented the formalization of a matrix of real elements, and Nobuyuki Tamura et al. described the determinant and inverse of a matrix of real elements in Mizar [4, 5]. Ioana Pasca formalized interval matrices and verified the conditions for their regularity in the COQ system [7, 8]. Steven Obua described in [6] how the vector and matrix can be formalized in Isabelle/HOL. John Harrision formalized the real vector type $\mathbb{R}^N$ for a variable N and verified many properties about the real matrix and Euclidean space in HOL-light [1, 2]. To the best of our knowledge, there is no explicit form of the inverse matrix in existing theorem provers.

⋆ Corresponding author.

We think that there are two main difficulties in formalizing the matrix inversion. First, it is not easy to describe $(n-1)$-ary space based on a simple type theory [9, 10], even though sets with an $n-1$ size can be generalized using the complement of one element subset [11, 12]. More importantly, $\mathbb{R}^{(n-1)\times(n-1)}$ and $\mathbb{R}^{n\times n}$ are different types, so it becomes very difficult to define the minor using the determinant of the sub-matrix. Accordingly, it is hard to explicate the inverse matrix using an analytic solution.

Indeed, it is very difficult to describe an $(n-1)$-ary square matrix in HOL4. However, the cofactors of a matrix can be defined using the determinant of an n-by-n rather than an $(n-1)$-by-$(n-1)$ matrix. Therefore, we constructed an n-by-n matrix, the determinant of which is equal to the cofactor. With such a method, the problem of the expression of the cofactor is solved. And then, the explicit form of the inverse matrix can be formalized using the adjugate matrix.

In this paper, we start from definitions of invertibility and the inverse matrix, and prove some important properties about the inverse matrix. Then, we systematically give formal definitions of the cofactor and the adjugate matrix, and formal proof of Laplace's formula. Finally, we formalize the matrix inversion and prove some major theorems about it.

2 Formalization of the invertible matrix

2.1 Definition of invertibility and the inverse matrix

Nonsingular linear transformation and its inverse transform have been applied in many important areas. The matrix is the operator of the space transform. General linear groups are such groups, the objects of which are all nonsingular matrices of a given size and the operation is matrix multiplication, since every element in a group has to be invertible. The multiplicative inverse of a nonsingular matrix is the inverse matrix.

In linear algebra an n-by-n (square) matrix $\mathbf{A}$ is called invertible (it is also called non-singular or nondegenerate) if there exists an n-by-n matrix $\mathbf{A'}$ such that

$$\mathbf{A}\mathbf{A'} = \mathbf{A'}\mathbf{A} = \mathbf{E}_n \tag{1}$$

where $\mathbf{E}_n$ denotes the n-by-n identity matrix and the multiplication used is ordinary matrix multiplication. If this is the case, then the matrix $\mathbf{A'}$ is uniquely determined by $\mathbf{A}$ and is called the inverse of $\mathbf{A}$, denoted by $\mathbf{A}^{-1}$.

Here, two definitions are involved. One is the invertibility of the matrix, and the other is the inverse matrix. Non-square matrices (m-by-n matrices for which $m \neq n$) have no inverses. However, in some cases, such an m-by-n matrix may have a left inverse or right inverse. Without loss of generality, the definitions are defined as followed in HOL4.

Definition 1. *invertible_def:*

$$invertible(\mathbf{A} : \mathbb{R}^{m\times n}) := \exists \mathbf{A'}(: \mathbb{R}^{n\times m}).\ \mathbf{A}\mathbf{A'} = \mathbf{E} \wedge \mathbf{A'}\mathbf{A} = \mathbf{E}$$

where the type of $\mathbf{A}$ is $\mathbb{R}^{m\times n}$ denotes matrix $\mathbf{A}$ is the m-by-n real matrix, similar to the following. The first $\mathbf{E}$ denotes the m-by-m identity matrix and the second $\mathbf{E}$ denotes the n-by-n identity matrix, the same as below.

Definition 2. *MATRIX_INV_DEF:*

$$(\mathbf{A} : R^{m\times n})^{-1} := \varepsilon\mathbf{A}'(:\mathbb{R}^{n\times m}).\ \mathbf{A}\mathbf{A}' = \mathbf{E} \wedge \mathbf{A}'\mathbf{A} = \mathbf{E}$$

there is an ε-term in the definition, $\varepsilon\mathbf{A}'(:\mathbb{R}^{n\times m}).\ \mathbf{A}\mathbf{A}' = \mathbf{E} \wedge \mathbf{A}'\mathbf{A} = \mathbf{E}$ denotes an $\mathbf{A}'$ such that $\mathbf{A}\mathbf{A}' = \mathbf{E} \wedge \mathbf{A}'\mathbf{A} = \mathbf{E}$.

2.2 Formalization and proof of important properties

In accordance with the definition of the invertibility of a matrix, it is easy to prove the following two theorems.

Theorem 1. *MATRIX_INV:*

$$\forall\mathbf{A}(:\mathbb{R}^{n\times n}).\ \mathit{invertible}(\mathbf{A}) \Rightarrow \mathbf{A}\mathbf{A}^{-1} = \mathbf{E} \wedge \mathbf{A}^{-1}\mathbf{A} = \mathbf{E}$$

Theorem 2. *INVERTIBLE_MATRIX_INV:*

$$\forall\mathbf{A}(:\mathbb{R}^{m\times n}).\ \mathit{invertible}(\mathbf{A}) \Rightarrow \mathit{invertible}(\mathbf{A}^{-1})$$

Furthermore, the following properties hold for an invertible matrix $\mathbf{A}$.

Theorem 3. *MATRIX_RMUL_EQ:*

$$\forall\mathbf{A}(:\mathbb{R}^{m\times n})\ (\mathbf{X}\ \mathbf{Y})(:\mathbb{R}^{n\times p}).\ \mathit{invertible}(\mathbf{A}) \Rightarrow (\mathbf{X} = \mathbf{Y} \Leftrightarrow \mathbf{A}\mathbf{X} = \mathbf{A}\mathbf{Y})$$

Theorem 4. *MATRIX_LMUL_EQ:*

$$\forall\mathbf{A}(:\mathbb{R}^{m\times n})\ (\mathbf{X}\ \mathbf{Y})(:\mathbb{R}^{p\times m}).\ \mathit{invertible}(\mathbf{A}) \Rightarrow (\mathbf{X} = \mathbf{Y} \Leftrightarrow \mathbf{X}\mathbf{A} = \mathbf{Y}\mathbf{A})$$

The above theorems are succinct and symmetrical, but they are less conveniently expended in the practical proof. They can be changed into the following two theorems:

Theorem 5. *MATRIX_EQ_LMUL_IMP:*

$$\forall\mathbf{A}(:R^{m\times n})\ (\mathbf{X}\ \mathbf{Y})(:\mathbb{R}^{n\times p}).\ \mathit{invertible}(\mathbf{A}) \wedge \mathbf{A}\mathbf{X} = \mathbf{A}\mathbf{Y} \Rightarrow \mathbf{X} = \mathbf{Y}$$

Theorem 6. *MATRIX_EQ_RMUL_IMP:*

$$\forall\mathbf{A}(:\mathbb{R}^{m\times n})\ (\mathbf{X}\ \mathbf{Y})(:\mathbb{R}^{p\times m}).\ \mathit{invertible}(\mathbf{A}) \wedge \mathbf{X}\mathbf{A} = \mathbf{Y}\mathbf{A} \Rightarrow \mathbf{X} = \mathbf{Y}$$

Thus, it can be proved that the inverse of an invertible matrix's inverse is itself.

Theorem 7. *MATRIX_INV_INV:*

$$\forall \mathbf{A}(:\mathbb{R}^{m\times n}).\ invertible(\mathbf{A}) \Rightarrow (\mathbf{A}^{-1})^{-1} = \mathbf{A}$$

The nature of an invertible transformation can be described as follows:

Theorem 8. *MATRIX_INV_TRAN_UNIQ:*

$$\forall \mathbf{A}(:\mathbb{R}^{m\times n})\ (\mathbf{x}\ \mathbf{y})(:\mathbb{R}^{n}).\ invertible(\mathbf{A}) \wedge \mathbf{Ax} = \mathbf{y} \Rightarrow \mathbf{x} = \mathbf{A}^{-1}\mathbf{y}$$

here, the type of $\mathbf{x}$ and $\mathbf{y}$ is $\mathbb{R}^n$ denotes they are both n-ary real vectors.

The following theorems can be proven:

Theorem 9. *MATRIX_MUL_LINV_UNIQ:*

$$\forall \mathbf{A}(:\mathbb{R}^{m\times n})\ (\mathbf{X}\ \mathbf{Y})(:\mathbb{R}^{n\times p}).\ invertible(\mathbf{A}) \wedge \mathbf{AX} = \mathbf{Y} \Rightarrow \mathbf{X} = \mathbf{A}^{-1}\mathbf{Y}$$

Theorem 10. *MATRIX_MUL_RINV_UNIQ:*

$$\forall \mathbf{A}(:\mathbb{R}^{m\times n})\ (\mathbf{X}\ \mathbf{Y})(:\mathbb{R}^{p\times m}).\ invertible(\mathbf{A}) \wedge \mathbf{XA} = \mathbf{Y} \Rightarrow \mathbf{X} = \mathbf{YA}^{-1}$$

Similarly, the following theorems hold for the square matrix $\mathbf{A}$:

Theorem 11. *MATRIX_LINV_UNIQ:*

$$\forall(\mathbf{A}\ \mathbf{B})(:\mathbb{R}^{n\times n}).\ \mathbf{AB} = \mathbf{E} \Rightarrow \mathbf{A} = \mathbf{B}^{-1}$$

Theorem 12. *MATRIX_RINV_UNIQ:*

$$\forall(\mathbf{A}\ \mathbf{B})(:\mathbb{R}^{n\times n}).\ \mathbf{AB} = \mathbf{E} \Rightarrow \mathbf{B} = \mathbf{A}^{-1}$$

The above theorems are all related to the inverse matrix, but do not indicate the explicit form of the inverse matrix. However, in practical applications it is very necessary to explicate the inverse matrix. For example, for non-singular linear transformations, their inverse transforms are always needed. In order to solve such problems, the explicit form of the inverse matrix must be formalized. There are many methods for achieving matrix inversion and an analytical solution is applied in this paper.

3 Formalizing the explicit form of the inverse matrix

Writing the adjugate matrix is an efficient way of calculating the inverse of small matrices. To determine the inverse, we calculate a matrix of cofactors:

$$\mathbf{A}^{-1} = \frac{\begin{bmatrix} \mathbf{A}_{00} & \mathbf{A}_{10} & \cdots & \mathbf{A}_{(n-1)0} \\ \mathbf{A}_{01} & \mathbf{A}_{11} & \cdots & \mathbf{A}_{(n-1)1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{0n} & \mathbf{A}_{1n} & \cdots & \mathbf{A}_{(n-1)(n-1)} \end{bmatrix}}{|\mathbf{A}|} \tag{2}$$

where $|\mathbf{A}|$ is the determinant of $\mathbf{A}$, and $\mathbf{A_{ij}}$ is the cofactor of the corresponding subscript elements of matrix $\mathbf{A}$.

3.1 Formalizing determinant

The determinant of an n-by-n matrix $\mathbf{A}$ is defined with the **Leibniz** formula.

Definition 3. *DET_DEF:*

$$DET(\mathbf{A} : \mathbb{R}^{n\times n}) := \sum_{p\in S_n} SIGN(p) \prod_{i=0}^{n-1} a_{i,p(i)}$$

It is denoted as $|\mathbf{A}|$. Here, the sum is computed over all permutations p of the set $\{0, 1, \cdots, n-1\}$. The signature of a permutation p is denoted as $SIGN(p)$ and defined as $+1$ if p is even and -1 if p is odd. $a_{i,p(i)}$ is the i-th row and the $p(i)$-th column element of the matrix $\mathbf{A}$.

Cramer's rule is an explicit formula for the solution of a system of linear equations with as many equations as unknowns. The formula is valid whenever the system has a unique solution. It expresses the solution in terms of the determinants of the (square) coefficient matrix and of matrices obtained from it by replacing one column by the vector of the right-hand sides of the equations. Its formalization is as follows:

Theorem 13. *CRAMER:*

$$\begin{array}{l}\forall \mathbf{A} : \mathbb{R}^{n\times n}\ \mathbf{x}\ \mathbf{b}.\\ |\mathbf{A}| \neq 0 \Rightarrow\\ \mathbf{Ax} = \mathbf{b} \Leftrightarrow \mathbf{x} = \frac{[|\mathbf{b},\mathbf{a}_1,\cdots,\mathbf{a}_{n-1}|,\cdots,|\mathbf{a}_0,\cdots,\mathbf{a}_{j-1},\mathbf{b},\mathbf{a}_{j+1},\cdots,\mathbf{a}_{n-1}|,\cdots,|\mathbf{a}_0,\cdots,\mathbf{a}_{n-2},\mathbf{b}|]}{|A|}\end{array}$$

here, $\mathbf{a}_i$ is the the i-th column vector of the matrix $\mathbf{A}$. This theorem is presented with some ellipsis for comprehensibility. Its formal description in HOL4 is as follows.

```
!A:real['n]['n]  x  b.
   ~(DET(A) = &0)
     ==> ((A ** x = b) <=>
     (x =
FCP k. DET(FCP i j. if j = k then b ' i else A ' i ' j) / DET(A)))
```

3.2 Formalizing the cofactor and the adjugate matrix

The difficulty of defining minor. In classical mathematical theory, the minor M_{ij} is defined as the determinant of the $(n-1)\times(n-1)$-matrix that results from $\mathbf{A}$ by removing the i-th row and the j-th column. The expression $(-1)^{i+j}M_{ij}$ is known as cofactor A_{ij}. However, with this definition it is very difficult to formalize the minor in a theorem prover. For example, in HOL4 an n-ary real vector type $\mathbb{R}^n$ is formalized with $real[:'n]$, where $'n$ is a type variable, supposing that $dimindex(:'n) = n$, where n is a num type and $:'n$ is a set [3]. Although $dimindex(sub1(:'n)) = n-1$, it is still difficult to define an $(n-1)$-ary real vector type $\mathbb{R}^{n-1}$ in this way. Even if it could be expressed, $\mathbb{R}^n$ and $\mathbb{R}^{n-1}$ are

two different types, and so are $\mathbb{R}^{(n-1)\times(n-1)}$ and $\mathbb{R}^{n\times n}$. The type of determinant that was previously defined is $\mathbb{R}^{n\times n} \to \mathbb{R}$, but the type of the expected minor should be $\mathbb{R}^{(n-1)\times(n-1)} \to \mathbb{R}$. Therefore, it is also hard to define a minor with the determinant.

Defining the cofactor by contributing the *n*-by-*n* matrix. To Define the cofactor with the determinant of $\mathbb{R}^{n\times n} \to \mathbb{R}$, it is essential to construct a matrix with $\mathbb{R}^{n\times n}$ that is the same size as the original matrix $\mathbf{A}$. The following key point is to construct a matrix whose determinant is equal to the cofactor. When **Cramer**'s rule is formalized, $\mathbf{a}_j$ is replaced with $\mathbf{b}$ to obtain a new matrix. Similarly, the cofactor A_{ij} can be expressed by the determinant of an n-by-n matrix by replacing $\mathbf{a}_j$ with a standard basis $\mathbf{e}_i$ in matrix $\mathbf{A}$. In order to simplify the proof, a more concise matrix can be used to define the cofactor.

Definition 4. *COFACTOR_DEF:*

$$A_{ij} := DET \begin{bmatrix} a_{00} & \cdots & a_{0(j-1)} & 0 & a_{0(j+1)} & \cdots & a_{0(n-1)} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \iddots & \vdots \\ a_{(i-1)0} & \cdots & a_{(i-1)(j-1)} & 0 & a_{(i-1)(j+1)} & \cdots & a_{(i-1)(n-1)} \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ a_{(i+1)0} & \cdots & a_{(i+1)(j-1)} & 0 & a_{(i+1)(j+1)} & \cdots & a_{(i+1)(n-1)} \\ \vdots & \iddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{(n-1)0} & \cdots & a_{(n-1)(j-1)} & 0 & a_{(n-1)(j+1)} & \cdots & a_{(n-1)(n-1)} \end{bmatrix}$$

The type of definition above is $\mathbb{R}^{n\times n} \to \mathbb{N} \to \mathbb{N} \to \mathbb{R}$, which matches with the determinant defined previously. Therefore, the cofactor of the corresponding subscripts can be expressed, and its formal definition is described below:

```
val COFACTOR_DEF = Define
 `(COFACTOR:real['n]['n]-> num -> num -> real) A i j =
    DET ((FCP k l. if k = i then (if l = j then &1 else &0) else
            (if l = j then &0 else A ' k ' l)):real['n]['n])`;
```

Formalizing the adjugate matrix. The transpose of the matrix of cofactors is known as the adjugate matrix, i.e.,

Definition 5. *ADJUGATE_MATRIX_DEF:*
$ADJUGATE\_MATRIX(\mathbf{A} : \mathbb{R}^{n\times n}) := \{\mathbf{A}_{ij}\}^T$

noted as $\mathbf{A}^*$. In HOL4, it can be formally defined in the following way:

```
val ADJUGATE_MATRIX_DEF = Define
  `(ADJUGATE_MATRIX:real['n]['n]-> real['n]['n]) A =
                              TRANSP(FCP i j. COFACTOR A i j)`;
```

3.3 Formalizing and proving Laplace's formula

The determinant of matrix $\mathbf{A}$ is expanded along an arbitrary row or column as follows:

Theorem 14. *LAPLACE_ROW:*

$$\forall \mathbf{A} : \mathbb{R}^{n\times n}\ k.\ k < n \Rightarrow |\mathbf{A}| = \sum_{j=0}^{n-1} a_{kj} A_{kj}$$

Theorem 15. *LAPLACE_COLUMN:*

$$\forall \mathbf{A} : \mathbb{R}^{n\times n}\ k.\ k < n \Rightarrow |\mathbf{A}| = \sum_{i=0}^{n-1} a_{ik} A_{ik}$$

Likewise, these corollaries can be proven.

Corollary 1. *LAPLACE_ROW_COROLLARY:*

$$\forall A(:\mathbb{R}^{n\times n})\ i\ j.\ i < n \wedge j < n \wedge i \neq j \Rightarrow \sum_{k=0}^{n-1} a_{ik} A_{jk} = 0$$

Corollary 2. *LAPLACE_COLUMN_COROLLARY:*

$$\forall A(:\mathbb{R}^{n\times n})\ i\ j.\ i < n \wedge j < n \wedge i \neq j \Rightarrow \sum_{k=0}^{n-1} a_{ki} A_{kj} = 0$$

3.4 Proving the explicit form of the inverse matrix

Using the definition of matrix multiplication, the following theorems can be proven.

Corollary 3. *LAPLACE_COROLLARY_LMUL:*

$$\forall \mathbf{A}(:\mathbb{R}^{n\times n}).\ \mathbf{A}\mathbf{A}^{*} = |\mathbf{A}|\mathbf{E}$$

Corollary 4. *LAPLACE_COROLLARY_RMUL:*

$$\forall \mathbf{A}(:\mathbb{R}^{n\times n}).\ \mathbf{A}^{*}\mathbf{A} = |\mathbf{A}|\mathbf{E}$$

A square matrix $\mathbf{A}$ is invertible if and only if its determinant is not 0.

Theorem 16. *INVERTIBLE_DET_NZ:*

$$\forall \mathbf{A}(:\mathbb{R}^{n\times n}).\ \mathit{invertible}(\mathbf{A}) \Leftrightarrow |\mathbf{A}| \neq 0$$

This theorem can be proven based on the definition of the inverse matrix and the properties of the determinant mentioned before.

Hence, the inversion of the invertible matrix can be explicated as follows:

Theorem 17. *MATRIX_INV_EXPLICIT:*

$$\forall \mathbf{A}(:\mathbb{R}^{n\times n}).\ invertible(\mathbf{A}) \Rightarrow \mathbf{A}^{-1} = \frac{\mathbf{A}^*}{|\mathbf{A}|}$$

Here is the formal proof in HOL4:
Moving the antecedent of the above goal into the assumptions and doing left multiplication with matrix $\mathbf{A}$ at both sides of the equation, the following form is obtained.

$$\frac{\mathbf{A}\mathbf{A}^{-1} = \frac{\mathbf{A}\mathbf{A}^*}{|\mathbf{A}|}}{invertible(\mathbf{A})} \tag{3}$$

It can be proven by rewriting $LAPLACE\_COROLLARY\_LMUL$ and $MATRIX\_INV$.

4 Inverse transforming and solving the matrix equation

After formalizing the matrix inversion, some questions about the inverse matrix can be expressed using its explicit form. As a consequence, the inverse of the nonsingular transformation can be formalized.

Theorem 18. *TRAN_INV_EXPLICIT:*

$$\forall \mathbf{A}(:\mathbb{R}^{n\times n})\ \mathbf{x}\ \mathbf{y}(:\mathbb{R}^{n}).invertible(\mathbf{A}) \wedge \mathbf{A}\mathbf{x} = \mathbf{y} \Rightarrow \mathbf{x} = \frac{\mathbf{A}^*}{|\mathbf{A}|}\mathbf{y}$$

Solving the matrix equation with an invertible coefficient matrix is widely applied in robot, real-time simulations, and MIMO wireless communication. It can be represented in formal form as below:

Theorem 19. *MATRIX_MUL_LINV_EXPLICIT:*

$$\forall \mathbf{A}(:\mathbb{R}^{n\times n})\ (\mathbf{X}\ \mathbf{Y})(:\mathbb{R}^{n\times m}).invertible(\mathbf{A}) \wedge \mathbf{A}\mathbf{X} = \mathbf{Y} \Rightarrow \mathbf{X} = \frac{\mathbf{A}^*}{|\mathbf{A}|}\mathbf{Y}$$

It can be proven using $MATRIX\_INV\_EXPLICIT$ and $MATRIX\_MUL\_LINV\_UNIQ$.

5 Conclusions

To solve the problem of formalizing the cofactor, we proposed a method using the determinant of an n-by-n matrix to express the cofactor. Consequently, we formally described the explicit form of an inverse matrix using the adjugate matrix method, and proved some of the important properties. Our work enriched theories of HOL4 and is expected to extend the scope of application of HOL4.

Acknowledgements

First and foremost we thank Prof. Shengzhen Jin for the guidance and encouragement that he gave us. We also thank Dr. John Harrison for his many good suggestions.

This work was supported by the International S&T Cooperation Program of China (2010DFB10930, 2011DFG13000); the National Natural Science Foundation of China (60873006, 61070049, 61170304, 61104035); the Beijing Natural Science Foundation and S&R Key Program of BMEC(4122017, KZ201210028036). Support was also received from the Open Project section of State Key Laboratory of Computer Architecture and the Trusted Software section of the Guangxi Key Laboratory.

References

1. J. Harrison. A HOL theory of Euclidean space. In Theorem Proving in Higher Order Logics, (TPHOLs 2005). Lecture Notes in Computer Science 3603, 114-129.
2. C. Robert M. Solovay, R.D. Arthan, and J. Harrison. Some new results on decidability for elementary algebra and geometry. ArXiV preprint 0904.3482, submitted to the Annals of Pure and Applied Logic, 2009.
3. K. Slind and M. Norrish. A brief overview of HOL. In O. A. Mohamed, C. M. noz, and S. Tahar, editors, TPHOLs 2008, Vol 5170 of LNCS: 28-32, 2008.
4. Y. Nakamura, N. Tamura, and W. Chang. A Theory of Matrices of Real Elements. J. Formalized Mathematics 2006, Vol. 14, No. 1: 21-28.
5. N. Tamura and Y. Nakamura. Determinant and Inverse of Matrices of Real Elements. J. Formalized Mathematics 2007, Vol. 15, No. 3: 127-136
6. S. Obua. Proving bounds for real linear programs in Isabelle/HOL. In J. Hurd, editor, Theorem Proving in Higher Order Logics (TPHOLs 2005), Vol. 3603 of Lect. Notes in Comp. Sci.: 227-244. Springer-Verlag, 2005.
7. I. Pasca. Formal Proofs for Theoretical Properties of Newton′s Method. Rapport de recherché INRIA Sophia Antipolis, 28 pages. February 2010
8. I. Pasca. Formally Verified Conditions for Regularity of Interval Matrices. Intelligent Computer Mathematics, 2010-Springer.
9. P. B. Andrews. An Introduction to Mathematical Logic and Type Theory: To Truth Through Proof. Academic Press, 1986.
10. A. Church. A formulation of the Simple Theory of Types. Journal of Symbolic Logic, 5:56-68, 1940.
11. R. Diaconescu. Axiom of choice and complementation. Proceedings of the American Mathematical Society, 51:176-178, 1975.
12. M. J. C. Gordon. Representing a logic in the LCF metalanguage. In D. Neel, editor, Tools and notions for program construction: an advanced course, pp. 163-185. Cambridge University Press, 1982.