Verification of Linear (In)Dependence in Finite Precision Arithmetic

Jiri Rohn

Dedicated to Professor Anatoly V. Lakeyev on the occasion of his 60th birthday.

Abstract. We present theoretical background for verification of linear dependence/independence of columns of a matrix by means of finite precision arithmetic.

Mathematics Subject Classification (2010). Primary 65G30; Secondary 65G50.

Keywords. Linear dependence, linear independence, pseudoinverse matrix, finite precision arithmetic, verification, MATLAB file.

1. Introduction

In this paper we are concerned with the problem of verification of linear (in)dependence of columns of a matrix by means of finite precision arithmetic. That means, given a matrix $A \in \mathbb{F}^{m\times n}$, where $\mathbb{F}$ is the set of floating-point numbers on a given computer, we wish to end up with statement

$$A \texttt{ has linearly independent columns}$$

or

$$A \texttt{ has linearly dependent columns}$$

and these assertions should hold as mathematical truths despite having been obtained by computation in finite precision arithmetic. The third possible statement is then

`No verified result`

meaning that the obtained result could not be verified in the above sense.

While verification of linear independence poses no problem (Theorem 2), verification of linear dependence is by no means easy. The clue to the solution of this problem consists in the use of a verified pseudoinverse which, in turn, requires use of a verified singular value decomposition. In the nutshell, the problem *can* be solved by finite precision means, but at the expense of employing heavy machinery.

In Section 3 we start with the characterization of linear independence of columns by means of the pseudoinverse matrix. This result is then employed in sufficient conditions for verified linear independence (Theorem 2) and dependence (Theorem 3). In Theorem 4 we show how to find, in case of linear dependence, a verified enclosure of a null vector of A, and in Theorem 5 we bring a verified description of the whole null space $\mathcal{N}(A)$.

This work was supported with institutional support RVO:67985807.

2. Pseudoinverse

As it is well known [5], for each matrix $A \in \mathbb{R}^{m\times n}$ there exists exactly one matrix $A^\dagger \in \mathbb{R}^{n\times m}$ satisfying

$$AA^\dagger A = A, \tag{2.1}$$
$$A^\dagger AA^\dagger = A^\dagger, \tag{2.2}$$
$$(A^\dagger A)^T = A^\dagger A, \tag{2.3}$$
$$(AA^\dagger)^T = AA^\dagger. \tag{2.4}$$

This matrix is called the *pseudoinverse* (or Moore-Penrose inverse) of A. If A has linearly independent columns, then $A^\dagger$ is given explicitly by

$$A^\dagger = (A^TA)^{-1}A^T. \tag{2.5}$$

The pseudoinverse of an $A \in \mathbb{R}^{m\times n}$ belongs to $\mathbb{R}^{n\times m}$, but it may not be exactly representable in $\mathbb{F}^{n\times m}$. To overcome this difficulty, we introduce the following notion. An $n \times m$ interval matrix $\boldsymbol{B} = [\underline{B}, \overline{B}] = \{\, B \mid \underline{B} \leqslant B \leqslant \overline{B}\,\}$, where inequalities are taken entrywise, is called a *verified enclosure* of $A^\dagger$ if $\underline{B}, \overline{B} \in \mathbb{F}^{n\times m}$ and $A^\dagger \in \boldsymbol{B}$ holds. Verified pseudoinverse will turn out to be our main tool for verification of linear dependence.

3. Auxiliary result

We suppose the following theorem to be known, but since we have not found it in standard textbooks, we provide its proof here. I denotes the identity matrix.

Theorem 1. A matrix $A \in \mathbb{R}^{m\times n}$ has linearly independent columns if and only if

$$A^\dagger A = I. \tag{3.1}$$

Proof. If A has linearly independent columns, then (2.5) gives $A^\dagger A = I$. Conversely, if (3.1) holds, then $Ax = 0$ implies $x = A^\dagger Ax = 0$, hence the columns of A are linearly independent. □

4. Verification of linear independence

Verification of linear independence is the easier of the two tasks. It is based on the following theorem.

Theorem 2. Let $A \in \mathbb{R}^{m\times n}$ be given. If there exists a matrix $R \in \mathbb{R}^{n\times m}$ such that

$$\|I - RA\|_1 < 1, \tag{4.1}$$

then A has linearly independent columns.

Proof. We have

$$RA = I - (I - RA)$$

and since $\|I - RA\|_1 < 1$, the matrix $RA \in \mathbb{R}^{n\times n}$ is nonsingular ([4], Corollary 5.6.16). Hence if $Ax = 0$, then $RAx = 0$ and nonsingularity of RA implies $x = 0$ which shows that the columns of A are linearly independent. □

The choice of R in (4.1) is obvious. Since $I - A^\dagger A = 0$ in case of linear independence (Theorem 1), we choose

```
R=pinv(A)
```

(the *computed* pseudoinverse of A). But in order that the result (linear independence) be verified we must have the inequality (4.1) verified. This is done by computing the left-hand side of (4.1) in interval arithmetic with outward rounding [1] as shown in the subfunction `ind` of the MATLAB/INTLAB function `lindep` in Section 9.

5. Verification of linear dependence

The method for verifying linear dependence described in the following Theorem 3 seems to be the only one known so far.

Theorem 3. Let $A \in \mathbb{R}^{m\times n}$ and let $\boldsymbol{B}$ be a verified enclosure of $A^\dagger$ such that the interval matrix

$$\boldsymbol{C} = I - \boldsymbol{B}A = [\underline{C}, \overline{C}]$$

satisfies $\underline{C}_{ij} > 0$ or $\overline{C}_{ij} < 0$ for some i, j. Then A has linearly dependent columns.

Proof. Assume to the contrary that the columns of A are linearly independent. Since the matrix $A^\dagger$ belongs to $\boldsymbol{B}$, we have, according to Theorem 1,

$$0 = I - A^\dagger A \in I - \boldsymbol{B}A = \boldsymbol{C} = [\underline{C}, \overline{C}],$$

hence

$$\underline{C} \leqslant 0 \leqslant \overline{C}$$

which contradicts the assumption that $\underline{C}_{ij} > 0$ or $\overline{C}_{ij} < 0$ for some i, j. □

Thus, to verify linear dependence of the columns of A by means of Theorem 3, we must perform three steps: first, to find a verified enclosure $\boldsymbol{B}$ of $A^\dagger$; second, to compute $\boldsymbol{C} = I - \boldsymbol{B}A$ in interval arithmetic; and third, to check whether $\underline{C}_{ij} > 0$ or $\overline{C}_{ij} < 0$ holds for some i, j. Of these three, the last two steps are trivial; so the most important part consists in finding a verified enclosure of $A^\dagger$. This is done by VERSOFT's [7] program `verpinv.m` [6] whose syntax is `B=verpinv(A)`. However, this program is still far from perfect as it sometimes fails; Section 6 below offers some explanation of this behavior. It has been observed that failure occurs often when $\text{rank}(A) \leqslant n - 2$. Thus, to avoid these situations, we proceed as follows. First we find by means of standard RREF procedure a basis D of the range space of A, verify its full column rank according to Theorem 2, and then we check linear dependence of columns of $[D\ A_{\bullet j}]$ for nonbasic columns $A_{\bullet j}$ by Theorem 3. This idea is embedded into the subfunction `dep` of the function `lindep` described in Section 9.

6. Premature termination of `verpinv`

The VERSOFT file `verpinv` available from [6] uses three methods for computing verified pseudoinverse performed in the interval arithmetic: the formula (2.5), Greville's algorithm [3] and singular value decomposition [2]. Unfortunately, all three may fail, causing the failure of the `lindep` procedure: the formula (2.5) fails when A has linearly dependent columns, and each of the other two methods contains a statement of the form

```
if a>0
    statement1
else
    statement2
end
```

where a is a nonnegative scalar obtained in the course of previous computation. If a is a real number, then this statement is perfectly feasible. However, if a is a real interval, say $a = [0, 10^{-14}]$, then the verification program cannot decide which case occurs and the computation breaks down. This is a common curse of verification programs where to the two classic types of output "A possesses the property P" and "A does not possess the property P" we must add the third type "no verified result".

7. Examples

A randomly generated $m \times n$ matrix with $m \geqslant n$ is likely to have linearly independent columns:

```
>> m=200; n=100; rand('state',1); A=2*rand(m,n)-1; l=lindep(A)
l =
     1
```

On the other hand, if $m < n$, then the columns are linearly dependent:

```
>> m=100; n=200; rand('state',2); A=2*rand(m,n)-1; l=lindep(A)
l =
     0
```

Next consider matrices constructed by the statement

```
>> A=(reshape(1:n^2,n,n))'
```

i.e., satisfying $A(i, j) = (i-1)n + j$ for each i, j. Their structure can be clearly seen from the particular case of $n = 5$:

```
>> n=5; A=(reshape(1:n^2,n,n))'
A =
     1     2     3     4     5
     6     7     8     9    10
    11    12    13    14    15
    16    17    18    19    20
    21    22    23    24    25
```

These matrices satisfy $\mathrm{rank}(A) = 2$ for each $n \geqslant 2$. The file `lindep.m` rightly verifies linear dependence of columns for each n with $3 \leqslant n \leqslant 12$:

```
>> n=12; A=(reshape(1:n^2,n,n))'; l=lindep(A)
l =
     0
```

but it fails for $n = 13$:

```
>> n=13; A=(reshape(1:n^2,n,n))'; l=lindep(A)
l =
    -1
```

Results of this type emphasize the necessity of further improvements in computation of verified pseudoinverse, something this author has not been able to do so far.

8. Null space

If A has linearly dependent columns, then $Ax = 0$ for some $x \neq 0$. Such an x may not be expressed exactly in floating point in general, but a verified enclosure of it can be found.

Theorem 4. Under assumptions and notation of Theorem 3 the interval vector

$$\boldsymbol{x} = \boldsymbol{C}_{\bullet j}$$

encloses a point vector $x \neq 0$ satisfying $Ax = 0$.

Proof. Define $x = (I - A^{\dagger}A)_{\bullet j} = (I - A^{\dagger}A)e_j$. Then $x \in (I - \boldsymbol{B}A)_{\bullet j} = \boldsymbol{C}_{\bullet j} = \boldsymbol{x}$, $Ax = (A - AA^{\dagger}A)e_j = 0$ by (2.1), and $x_i \neq 0$ because $x_i \in [\underline{C}_{ij}, \overline{C}_{ij}]$ and $0 \notin [\underline{C}_{ij}, \overline{C}_{ij}]$. $\square$

We can even give a certain description of the whole null space

$$\mathcal{N}(A) = \{\, x \mid Ax = 0 \,\}.$$

Theorem 5. Under assumptions and notation of Theorem 3 there exists a point matrix $C \in \boldsymbol{C}$ such that

$$\mathcal{N}(A) = \{\, Cy \mid y \in \mathbb{R}^n \,\}.$$

Proof. By Greville's description [3], $\mathcal{N}(A) = \{\, (I - A^\dagger A)y \mid y \in \mathbb{R}^n \,\}$. Here for $C = I - A^\dagger A$ we have $C \in I - \boldsymbol{B}A = \boldsymbol{C}$, and we are done. □

9. The MATLAB file `lindep.m`

Here we list the MATLAB/INTLAB file `lindep.m` employed in previous computations.

```
function l=lindep(A) % Linear INDEPendence, LINear DEPendence
% l= 1: columns of A are verified linearly independent,
% l= 0: columns of A are verified linearly dependent,
% l=-1: no verified result.
% Requires INTLAB and VERSOFT to be installed under MATLAB.
l=ind(A); if l==1, return, end
l=dep(A); if l==0, return, end
l=-1;
function lind=ind(A) % linear INDependence
I=eye(size(A,2));
R=pinv(A); R=infsup(R,R);
G=I-R*A; n1=norm(G,1);
if n1.sup<1, lind=1; return, end
lind=-1;
function lind=dep(A) % linear DEPendence
lind=-1; [AR,K]=rref(A); if isempty(K), return, end
D=A(:,K); if ind(D)==-1, return, end
I=eye(length(K)+1);
for j=1:size(A,2)
    if ~any(K==j)
        B=verpinv([D A(:,j)]); if isnan(B.inf(1,1)), return, end
        C=I-B*[D A(:,j)];
        if any(any(C.inf>0))||any(any(C.sup<0)), lind=0; return, end
    end
end
```

Acknowledgment

The author wishes to thank two anonymous referees for their comments.

References

[1] G. Alefeld and J. Herzberger, *Introduction to Interval Computations*, Academic Press, New York, 1983.

[2] G. H. Golub and C. F. van Loan, *Matrix Computations*, The Johns Hopkins University Press, Baltimore, 1996.

[3] T. N. E. Greville, *The pseudoinverse of a rectangular or singular matrix and its application to the solution of systems of linear equations*, SIAM Review, 1 (1959), pp. 38–43.

[4] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, 1985.

[5] R. Penrose, *A generalized inverse for matrices*, Proc. Camb. Philos. Soc., 51 (1955), pp. 406–413.

[6] J. Rohn, *VERPINV: Verified pseudoinverse of a real matrix*, 2008. `http://uivtx.cs.cas.cz/~rohn/matlab/verpinv.html`.

[7] J. Rohn, *VERSOFT: Verification software in MATLAB/INTLAB*, 2009. http://uivtx.cs.cas.cz/∼rohn/matlab.

Jiri Rohn
Institute of Computer Science
Pod vodarenskou vezi 2
CZ-18207 Prague
Czech Republic
e-mail: rohn@cs.cas.cz