Verification of linear (in)dependence in finite precision arithmetic

Rohn, Jiří

2012

Institute of Computer Science
Academy of Sciences of the Czech Republic

Verification of linear (in)dependence in finite precision arithmetic

Jiří Rohn
http://uivtx.cs.cas.cz/~rohn

Technical report No. V-1156

02.02.2012

Pod Vodárenskou věží 2, 182 07 Prague 8, phone: +420 266 051 111, fax: +420 286 585 789,
e-mail:rohn@cs.cas.cz

Institute of Computer Science
Academy of Sciences of the Czech Republic

Verification of linear (in)dependence in finite precision arithmetic

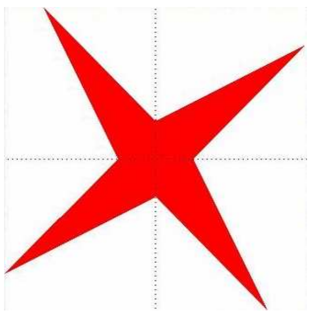
Jiří Rohn
http://uivtx.cs.cas.cz/~rohn

Technical report No. V-1156

02.02.2012

Abstract:

We present the theoretical background of the VERSOFT's file `zd.m` for verification of linear dependence/independence of columns of a matrix by means of finite precision arithmetic.[1]



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

[1] Above: logo of interval computations and related areas (depiction of the solution set of the system $[2,4]x_1 + [-2,1]x_2 = [-2,2]$, $[-1,2]x_1 + [2,4]x_2 = [-2,2]$ (Barth and Nuding [1])).

1 Introduction

In this report 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 `has linearly independent columns`

or

A `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 2 we start with 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 dependence, a verified enclosure of a null vector $x \neq 0$ satisfying $Ax = 0$, and in Theorem 5 we bring a verified description of the whole of the null space $\mathcal{N}(A)$. The last Theorem 6 shows how to find a linearly dependent column which can be deleted while preserving the range space $\mathcal{R}(A)$ intact.

2 Pseudoinverse

As is well known [3], for each matrix $A \in \mathbb{R}^{m \times n}$ there exists exactly one matrix $A^\dagger \in \mathbb{R}^{n \times m}$ satisfying

$$
\begin{aligned}
AA^\dagger A &= A, && (2.1)\\
A^\dagger AA^\dagger &= A^\dagger, && (2.2)\\
(A^\dagger A)^T &= A^\dagger A, && (2.3)\\
(AA^\dagger)^T &= AA^\dagger. && (2.4)
\end{aligned}
$$

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[2]

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

An $n \times m$ interval matrix $\mathbf{B} = [\underline{B}, \overline{B}] = \{\, B \mid \underline{B} \leqslant B \leqslant \overline{B} \,\}$ is said to be an *enclosure* of $A^\dagger$ if $A^\dagger \in \mathbf{B}$ holds, and a *verified enclosure* of $A^\dagger$ if $\underline{B}, \overline{B} \in \mathbb{F}^{n \times m}$ and $A^\dagger \in \mathbf{B}$ holds true.

[2] As it can be easily proved by verifying (2.1)-(2.4).

3 Auxiliary result

I suppose that the following theorem is known; but since I have not found it in standard textbooks, I provide its proof here.

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 for a given $A \in \mathbb{R}^{m\times n}$ there exist a matrix $R \in \mathbb{R}^{n\times m}$ such that*

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

holds in some consistent matrix norm[3]. Then A has linearly independent columns.

Proof. We have

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

and since $\|I - RA\| < 1$, the matrix $RA \in \mathbb{R}^{n\times n}$ is nonsingular ([2], 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 self-explanatory. 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. In the INTLAB file `zd.m` on pp. 6-7 this is done in the following part:

```
I=eye(n,n);
R=pinv(A);
R=infsup(R,R);
G=I-R*A; % intval quantity
n1=norm(G,1);
ni=norm(G,'inf');
```

[3] I.e., satisfying $\|CD\| \leqslant \|C\| \cdot \|D\|$ for each C, $D \in \mathbb{R}^{n\times n}$.

```
if min(n1.sup,ni.sup)<1 % full column rank of A verified
    fcr=1; % verified full column rank
    setround(gr); return
end
```

Since `R` is made a matrix of type intval by `R=infsup(R,R)`, the following quantities `G`, `n1`, `ni` are also of type intval[4], hence if `min(n1.sup,ni.sup)<1`, then either `n1.sup<1` or `ni.sup<1` so that the inclusion isotony of interval arithmetic operations implies that either $\|I - RA\|_1 < 1$ or $\|I - RA\|_\infty < 1$ is verified, hence the columns of A are verified linearly independent in view of Theorem 2. In this case the variable `fcr` (Full Column Rank) is set to 1.

5 Verification of linear dependence

At this point I must confess that during construction of VERSOFT [5], which lasted several years, I was looking for a long time in vain for a tool which would enable us to deliver a verified confirmation of linear dependence. The result below is the single one I found (and I do not know another one till today).

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

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

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 (not exactly known) matrix $A^\dagger$ belongs to $\mathbf{B}$, we have, according to Theorem 1,

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

hence

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

which contradicts the fact 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 $\mathbf{B}$ of $A^\dagger$; second, to compute $\mathbf{C} = I - \mathbf{B}A$ 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 program `verpinv.m` [4] whose syntax is `[X,E]=verpinv(A)`. Here `X` is a verified enclosure of `A` and `E` is an error message (if applicable).

In the `zd.m` file on pp. 6-7 this part looks a follows; our interval matrices $\mathbf{B}$, $\mathbf{C}$ are denoted there by `X`, `B`, respectively, and the variable `fcr` is set to 0 if linear dependence is verified.

[4] Following the "basic interval arithmetic property": an operation always uses interval arithmetic if at least one of the operands is of type intval.

```
[X,Everpinv]=verpinv(A);
if isnan(X.inf(1,1))
    E=Everpinv; % no verified result
    setround(gr); return
end
% pseudoinverse computed
B=I-X*A; % B=I-pinv(A)*A % A is column rank deficient iff B is nonzero
if any(any(B.inf>0))||any(any(B.sup<0)) % B is verified nonzero
    fcr=0; % verified column rank defective
end
```

6 Null space

If A has linearly dependent columns, then $Ax = 0$ for some $x \neq 0$. Such an x cannot 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*

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

is verified to enclose a point vector x satisfying $Ax = 0$ and $x_i \neq 0$.

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

This result was not included into the `zd.m` file as it had not been known to the author at the time.

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 $C \in \mathbf{C}$ such that*

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

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

7 Range space

Here we consider the range space of A,

$$\mathcal{R}(A) = \{\, Ax \mid x \in \mathbb{R}^n \,\}.$$

Theorem 6. *Under assumptions and notation of Theorem 3, let $\tilde{A}$ denote the $m \times (n-1)$ matrix formed from A by deleting its ith column. Then*

$$\mathcal{R}(\tilde{A}) = \mathcal{R}(A).$$

Proof. According to Theorem 4 there exists an x satisfying $Ax = 0$ and $x_i \neq 0$. Hence from

$$Ax = \sum_{j=1}^{n} x_j A_{\bullet j} = 0$$

we have

$$A_{\bullet i} = -(\sum_{j=1}^{i-1} x_j A_{\bullet j} + \sum_{j=i+1}^{n} x_j A_{\bullet j})/x_i, \tag{7.1}$$

so that the columns of $\tilde{A}$ span $\mathcal{R}(A)$. □

By repeating this process, we can construct a verified basis of $\mathcal{R}(A)$.

8 The file zd.m

```
function [fcr,E]=zd(A)
%    ZD      Verified full column rank of a rectangular real matrix.
%
%    This is an INTLAB file. It requires to have INTLAB installed under
%    MATLAB to function properly.
%
%    For a rectangular real matrix A,
%        fcr=zd(A)
%    either verifies full column rank of A, or verifies column rank
%    deficiency of A, or fails (yields no verified result):
%
%    fcr= 1      A is verified to have full column rank (i.e.,
%                columns of A are linearly independent),
%    fcr= 0      A is verified not to have full column rank (i.e.,
%                columns of A are linearly dependent),
%    fcr=-1      no verified result.
%
%    For full row rank, apply ZD to A'.
%
%    See also PINV, VERPINV.

%    Copyright 2008 Jiri Rohn.
%
%    Full column rank is verified by showing that
%        norm(eye(size(A,2))-pinv(A)*A,p)<1
%    for p=1 or p='inf'. Column rank deficiency is proved by showing that
%    the matrix
%        B=eye(size(A,2))-pinv(A)*A
%    is verified to be nonzero.
%
%    WARRANTY
%
%    Because the program is licensed free of charge, there is
%    no warranty for the program, to the extent permitted by applicable
%    law. Except when otherwise stated in writing the copyright holder
%    and/or other parties provide the program "as is" without warranty
%    of any kind, either expressed or implied, including, but not
%    limited to, the implied warranties of merchantability and fitness
%    for a particular purpose. The entire risk as to the quality and
%    performance of the program is with you. Should the program prove
%    defective, you assume the cost of all necessary servicing, repair
%    or correction.
%
```

```
%    History
%
%    2007-11-02   first version
%    2008-03-12   version for posting
%    2008-04-05   column rank deficiency part added; E added
%    2008-05-30   renamed as ZD, p-coded, called by VERFULLCOLRANK
%
gr=getround;
setround(0);
[m,n]=size(A);
fcr=-1;
E.error='verfullcolrank: none';
E.where='NaN';
E.value='NaN';
if ~(nargin==1&&nargout<=2&&~isintval(A))
    E.error='verfullcolrank: wrong data';
    setround(gr); return
end
I=eye(n,n);
R=pinv(A);
R=infsup(R,R);
G=I-R*A; % intval quantity
n1=norm(G,1);
ni=norm(G,'inf');
if min(n1.sup,ni.sup)<1 % full column rank of A verified
    fcr=1; % verified full column rank
    setround(gr); return
end
[X,Everpinv]=verpinv(A);
if isnan(X.inf(1,1))
    E=Everpinv; % no verified result
    setround(gr); return
end
% pseudoinverse computed
B=I-X*A; % B=I-pinv(A)*A % A is column rank deficient iff B is nonzero
if any(any(B.inf>0))||any(any(B.sup<0)) % B is verified nonzero
    fcr=0; % verified column rank defective
end
setround(gr);
```

9 Dedication

Dedicated to Z. D.

Bibliography

[1] W. Barth and E. Nuding, *Optimale Lösung von Intervallgleichungssystemen*, Computing, 12 (1974), pp. 117–125. 1

[2] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, 1985. 2

[3] R. Penrose, *A generalized inverse for matrices*, Proc. Camb. Philos. Soc., 51 (1955), pp. 406–413. 1

[4] J. Rohn, *VERPINV: Verified pseudoinverse of a real matrix*, 2008. http://uivtx.cs.cas.cz/~rohn/matlab/verpinv.html. 3

[5] J. Rohn, *VERSOFT: Verification software in MATLAB/INTLAB*, 2009. http://uivtx.cs.cas.cz/~rohn/matlab. 3