Annales Univ. Sci. Budapest., Sect. Comp. 25 (2005) 143-152

AN ALGORITHM CHECKING A NECESSARY CONDITION OF NUMBER SYSTEM CONSTRUCTIONS

P. Burcsi and A. Kovács (Budapest, Hungary)

Abstract. In this paper we investigate from an algorithmic point of view one of the three necessary conditions - the expansivity of the base - of the number system property.

1. Introduction

Let Λ be a lattice in $\mathbb{R}^n$, $M : \Lambda \to \Lambda$ be an operator such that $\det(M) \neq 0$ and let D be a finite subset of Λ containing 0.

Definition. The triple (Λ, M, D) is called a *number system* (or having the unique representation property) if every element x of Λ has a unique, finite representation of the form $x = \sum_{i=0}^{l} M^i d_i$, where $d_i \in D$ and $l \in \mathbb{N}$. The operator M is called the *base* or *radix*, D is the *digit set*.

Clearly, both Λ and $M\Lambda$ are abelian groups under addition. The order of the factor group $\Lambda/M\Lambda$ is $t = |\det M|$. Let A_j $(j = 1, \dots, t)$ denote the cosets of this group. If two elements are in the same residue class then we say that they are congruent modulo M. The following theorem was proved in [6].

Theorem 1. *If* (Λ, M, D) *is a number system then*

1. *D must be a full residue system modulo M,*

The research of first author was supported by the Hungarian National Foundation for Scientific Research under grant OTKA-T043657, Bolyai Stipendium and the fund of the Applied Number Theory Research Group of the Hungarian Academy of Sciences.

2. M must be expansive,
3. $\det(I - M) \neq \pm 1$.

For a given operator M and digit set D the complete residue system property of D modulo M was analysed in [4]. In order to check the expansivity of M the method of Lehmer-Schur [7] was suggested and used in [5]. In case of expansive operators we now present an alternative method.

2. Stability of linear systems

Consider the systems described by sets of linear differential equations, or linear difference equations of the form

$$\dot{x}(t) = A\,x(t), \quad t \geq 0,$$

and

$$x(k+1) = B\,x(k), \quad k = 0, 1, 2, \dots,$$

respectively, where $x(t)$ and $x(k)$ denote the n-dimensional state vector. These representations arise in control theory, where the fundamental question is the *stability* of the systems.

The origin of linear control systems emerged at the end of the XIX. century in connection of centrifugal regulator, theoretically treated by Maxwell, Hermite and Liapunov. They observed that the stability nature of equilibrium points depends upon the sign of the real parts of the eigenvalues of A. A continuous-time linear control system is said to be *asymptotically stable* if all the eigenvalues $\lambda_1, \dots, \lambda_n$ of A have negative real parts. In the discrete-time case it is equivalent with $|\mu_k| < 1, k = 1, \dots, n$, where $\mu_1, \dots, \mu_n$ are the eigenvalues of B. The correspondence between the continuous-time and discrete-time cases is obtained by substituting

$$\mathrm{Re}(\lambda_i) < 0 \Leftrightarrow |\mu_i| < 1$$

and this is achieved by the standard bilinear mapping

$$\lambda = \frac{\mu + 1}{\mu - 1}, \quad \mu = \frac{\lambda + 1}{\lambda - 1}. \tag{1}$$

It is equivalent to taking

$$A = (B + I)(B - I)^{-1}, \quad B = (A - I)^{-1}(A + I). \tag{2}$$

The asymptotic stability criterion means now that all the eigenvalues of B must lie inside the unit disc $|\mu| < 1$ in the complex plane. Obviously, in this case $B^k \to 0$ as $k \to \infty$ (convergence).

A direct method of testing a given system for asymptotic stability is to apply one of the standard numerical algorithms for determining the eigenvalues. But we are interested in checking the stability condition (1) without finding the eigenvalues exactly, (2) we are looking for a method in which the operator may contain symbolic coefficients. We consider the stability problem in terms of the characteristic polynomial of A or B.

Definition. The polynomial

$$p(z) = p_0 + p_1 z + p_2 z^2 + \ldots + p_n z^n \in \mathbb{R}[z] \tag{3}$$

is said to be ***stable*** if all its roots lie in the open left half of the complex plane. In the complementary case the polynomial is said to be ***unstable***.

Fortunately, the theory of polynomial stability is well-researched. Many people were involved in this area, including Routh, Stodola, Hurwitz etc., see [2, 3, 8]. Now, we describe a method which decides the stability of a given polynomial.

There is a simple necessary condition for a polynomial to be stable.

Theorem 2. [Stodola condition] *The polynomial $p(z)$ in (3) can only be stable if all its coefficients are of the same sign.*

Further we give a necessary and sufficient condition for stability. It is known that some real functions can be written in an m-terminating continued fraction of form

$$\cfrac{b_1}{1 + \cfrac{b_2 z}{1 + \cfrac{b_3 z}{\ddots \; \overline{1 + b_m z}}}}, \tag{4}$$

where b_k $(k = 1, 2, \ldots, m)$ are appropriate real numbers. If we consider the rational function

$$r(z) = \frac{c_0 + c_1 z + \cdots + c_s z^s}{d_0 + d_1 z + \cdots d_t z^t}$$

having an m-terminating continued fraction form, then it can be proved ([3]) that the numbers b_k in (4) satisfy the following recursion:

$$\begin{aligned} c_n^{(-1)} &:= d_n, \\ c_n^{(0)} &:= c_n, \\ b_{k+1} &:= \frac{c_0^{(k)}}{c_0^{(k-1)}}, \\ c_n^{k+1} &:= b_{k+1} c_{n+1}^{(k-1)} - c_{n+1}^{(k)}, \end{aligned}$$

where $k = 0, 1, \ldots$, $n = 0, 1, \ldots$ and $c_n = 0$ if $n > s$, $d_n = 0$ if $n > t$. The proof of the next theorem can be found in [3].

Theorem 3. *The polynomial (3) of degree n is stable if and only if the rational function*

$$h(z) = \frac{p_1 + p_3 z + p_5 z^2 + \cdots}{p_0 + p_2 z + p_4 z^2 + \cdots} = \frac{\sum_{k=0}^{\lfloor (n-1)/2 \rfloor} p_{2k+1} z^k}{\sum_{k=0}^{\lfloor n/2 \rfloor} p_{2k} z^k}$$

(the Hurwitz alternant of p) can be represented by an n-terminating continued fraction, in which every number b_k $(k = 1, 2, \ldots, n)$ is positive.

3. The algorithm

Back to our original problem let the operator $M : \Lambda \to \Lambda$ be given. Observe that a basis transformation in Λ does not change the number system property, hence number expansions can be examined without loss of generality on the lattice $\mathbb{Z}^n$. Therefore let

$$b^*(\mu) = b_0 + b_1 \mu + \cdots + b_n \mu^n \in \mathbb{Z}[\mu]$$

be the characteristic polynomial of M. Since $\det(M) \neq 0$, the inverse of M exists and the characteristic polynomial of M^{-1} is

$$b(\mu) = b_n + b_{n-1}\mu + \cdots + b_0 \mu^n \in \mathbb{Z}[\mu], \; b_0 > 0. \tag{5}$$

Applying the linear transformation (1) we got the polynomial

$$a(\lambda) = a_n + a_{n-1}\lambda + \cdots + a_0\lambda^n \in \mathbb{Z}[\lambda].$$

Now, using Theorem 2 and 3 the stability of $a(\lambda)$ can easily be decided.

Summarizing our results, the operator M is expansive if and only if $a(\lambda)$ is stable.

Instead of giving a pseudocode we present a code written in Maple [1] language. The input is a list of coefficients of the characteristic polynomial of M. If the input is numeric then the output is true or false, depending on the the expansivity of M, if the input contains symbolic coefficients then the output is a set of inequalities, in which the expansivity holds.

```
Is_expansive:=proc(L::list)
      local l,cfnu,cfde,deg,b,m,temp,i,symb,s;
      deg := nops(L)-1;
      l := [seq(coeff(collect(sum(L[i+1]*(x+1)^(deg-i)*(x-1)^i,
            i=0..deg),x),x,j),j=0..deg)];
      if signum(op(1,l)) = 0 #minus 1 is a root
          then RETURN(false); fi;
      symb := not type(L,list(numeric));
      if not symb then
          s := signum(op(1,l));
          if s < 0 then l:=-l; s:=-s; fi;
          for i from 2 to nops(l) do
              if signum(op(i,l)) <> s then RETURN(false); fi;
                #Stodola criteria violated
          od;
      if type(deg,even) then l := [op(l),0] fi;
      m := 1;
      cfde := [seq(l[2*i-1],i=1..(deg+2)/2)];
      cfnu := [seq(l[2*i],i=1..(deg+2)/2)];
      while ((cfnu[1] > 0 or symb) and m < deg+1) do
          b[m] := cfnu[1]/cfde[1];
          if cfnu[nops(cfnu)] = 0 and
              cfnu[nops(cfnu)] = cfde[nops(cfde)] then
                cfnu := [seq(cfnu[i],i=1..nops(cfnu)-1)];
```

[1] Maple is a trademark of Waterloo Maple Inc.

```
                cfde := [seq(cfde[i],i=1..nops(cfde)-1)]; fi;
          temp := cfnu;
          for i to nops(cfnu)-1 do
              cfnu[i] := b[m]*cfde[i+1]-cfnu[i+1] od;
          cfnu[nops(cfnu)] := 0;
          cfde := temp;
          m := m+1;
      od;
      if m < deg+1
          then RETURN(false);
          elif not symb then RETURN(true);
          else print('true, if the following expressions are
            all positive:  ');
              print(seq(op(1,op(i,entries(factor(simplify(b))))),
                  i=1..m-1)); fi;
end:
```

We remark that in the symbolic case the set of inequalities is not simplified automatically.

Let us see some examples.

(1) Let the characteristic polynomial of the operator M be

$$a(x) = -18 + 9x - 8x^2 + 4x^3 \in \mathbb{Z}[x]. \tag{6}$$

Now, `Is_expansive`($[-18, 9, -8, 4]$) works as follows. After the linear transformation the program computes the list $l = [-39, -43, -49, -13]$. Then, since the first element of l is negative, the program produces the list $l = [39, 43, 49, 13]$. Observing that all the element of l have the same sign, the Stodola criteria are not violated. Then, the program computes the continued fraction coefficients b_i, which are $b_1 = 43/39, b_2 = 1600/1677$, and $b_3 = 13/43$. Since all b_i-s are positive, the program returns with *true*, so the operator M is expansive.

(2) Let the characteristic polynomial of M be

$$a(x) = a_0 + a_1x + a_2x^2 + x^3 \in \mathbb{Z}[x].$$

The algorithm `Is_expansive`($[a_0, a_1, a_2, 1]$) gives the following:

$$true,\ if\ the\ following\ expressions\ are\ all\ positive:$$

$$\frac{3a_0 - a_1 - a_2 + 3}{a_0 - a_1 + a_2 - 1}, \frac{8(a_0^2 - a_0 a_2 + a_1 - 1)}{(a_0 - a_1 + a_2 - 1)(3a_0 - a_1 - a_2 + 3)}, \frac{a_0 + a_1 + a_2 + 1}{3a_0 - a_1 - a_2 + 3}.$$

(3) Let the characteristic polynomial of M be

$$a(x) = -4 - 2x + ex^2 + x^3 + x^4 \in \mathbb{Z}[x].$$

The algorithm `Is_expansive`$([-4, -2, e, 1, 1])$ gives that M is expansive if and only if the numbers

$$\frac{14}{2-e}, \quad \frac{(100+27e)}{7(2-e)}, \quad \frac{16(69+25e)}{7(100+27e)}, \quad \frac{7(4-e)}{100+27e} \tag{7}$$

are all positive. Simplifying (7) we have that $-3 < \lfloor -69/25 \rfloor < e < 2$.

4. Bilinear transformation

In this section we give a method for applying the (1) bilinear transformation to the (5) polynomial, which uses only $n(n+1)$ additions and n binary shifts.

Clearly,

$$b(\mu) = b\left(\frac{\lambda+1}{\lambda-1}\right) = \frac{1}{(\lambda-1)^n}(a_0\lambda^n + \ldots + a_n) = \frac{1}{(\lambda-1)^n}a(\lambda) \tag{8}$$

for an appropriate $a(\lambda)$ polynomial. The polynomial $a(\lambda)$ has the same distribution of roots relative to the imaginary axis as does $b(\mu)$ relative to the unit circle. Our task is to obtain the coefficients a_i of $a(\lambda)$ in terms of the coefficients b_i of $b(\mu)$. Since

$$\left(\frac{2}{\lambda-1} + 1\right) = \frac{\lambda+1}{\lambda-1},$$

therefore if we let $\mu = 1 + \sigma$ then

$$b(1+\sigma) = b_0(1+\sigma)^n + \cdots + b_n = c_0\sigma^n + \cdots + c_n = c(\sigma) \tag{9}$$

for appropriate c_i-s. The coefficients c_i in (9) can be obtained using a sequence of Horner's scheme. Then let $\sigma = 2/(\lambda - 1)$, so we have that

$$(10)\quad b\left(\frac{\lambda+1}{\lambda-1}\right) = c(\sigma) = \frac{1}{(\lambda-1)^n}(2^n c_0 + 2^{n-1}c_1(\lambda-1) + \ldots + c_n(\lambda-1)^n).$$

Comparing (8) with (10) the required a_i-s can be obtained by a second application of Horner's rule to the coefficients $c_n, 2c_{n-1}, 2^2c_{n-2}, \ldots, 2^n c_0$. All together we performed $n(n+1)$ additions plus n binary shifts.

5. Summary

Deciding the expansivity of an operator $M \in \mathbb{Z}^{n\times n}$ by our algorithm requires $\Theta(n^2)$ arithmetic operations in $\mathbb{Q}$. To see what this theoretical speed means in practice we performed computer tests. In our experiment 100000 polynomials of degree n were generated with random integer coefficients between -100 and 100. This was repeated 8 times, changing the fixed degree of the polynomials from 3 up to 10.

For each random polynomial we checked if it defines an expansive operator, both by the Lehmer-Schur method and by our method (they gave the same results). We counted the number of arithmetic operations (additions and multiplications) needed to decide the expansivity. The figures show the cumulated number of all operations performed when *expansive* operators were found. We present the number of additions, multiplications and all operations as functions of the degree, showed on a logarithmic scale.

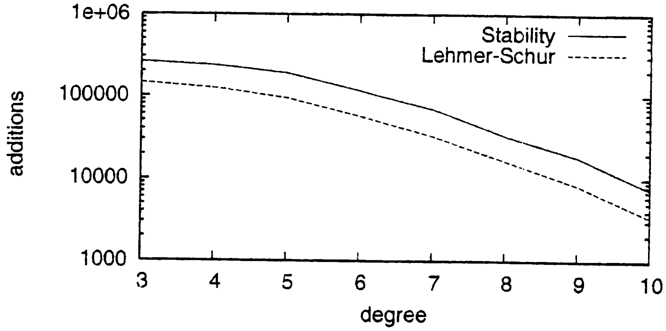

Fig. 1. The number of additions performed by the two algorithms

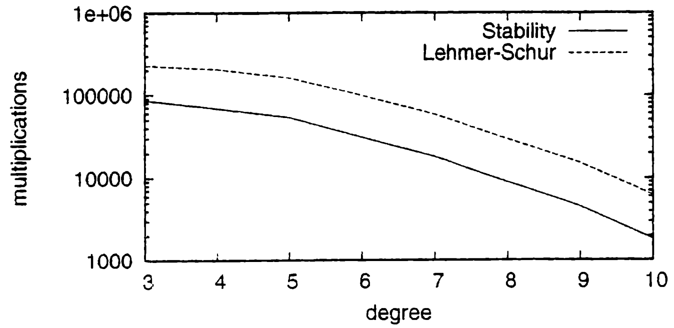

Fig. 2. The number of multiplications performed by the two algorithms

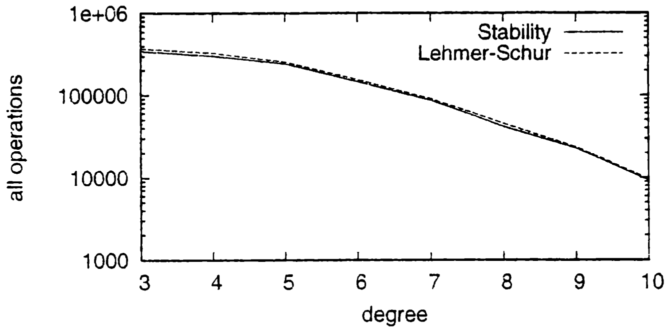

Fig. 3. The number of all arithmetic operations performed by the two algorithms

The number of expansive cases decreases as the degree increases. The decreasing number of operations is due to this fact. From the concave shape of the curves we can read that this decrease is even faster than exponential. What is more interesting is the approximately constant vertical difference between curves in all three figures. The tests show that our method needs about twice as much additions as the Lehmer-Schur method. On the other hand it only needs one third of the number of multiplications of the latter. The number of all operations is almost the same, slightly in favour of our algorithm. If addition is faster than multiplication it is worth choosing our test based on stability checking rather than the Lehmer-Schur method.

We conclude that in the case of expansive operators our method is a good alternative of the Lehmer-Schur method. We should choose it if we know in advance that the operator is likely to be expansive. This can happen if we know that another operator "close" to it is expansive. We use this method for an extensive search of *all* expansive operators in a parameter space where, in a certain sense, expansive operators are close to each other.

References

[1] **Cormen T.H., Leiserson Ch.E., Rivest R.L. and Stein C.,** *Introduction to algorithms,*, MIT Press, 2003.

[2] **Henrici P.,** *Applied and computational complex analysis I.,* Wiley, 1974.

[3] **Henrici P.,** *Applied and computational complex analysis II.,* Wiley, 1977.

[4] **Kovács A.,** On computation of attractors for invertible expanding linear operators in $\mathbb{Z}^k$, *Publ. Math. Debrecen,* **56** (1-2) (2000), 97-120.

[5] **Kovács A.,** Generalized binary number systems, *Annales Univ. Sci. Budapest. Sect. Comp.,* **20** (2001), 195-206.

[6] **Kovács A.,** Number expansion in lattices, *Math. and Comp. Modelling,* **38** (2003), 909-915.

[7] **Lehmer D.H.,** A machine method for solving polynomial equations, *J. ACM,* **2** (1961), 151-162.

[8] **Tóth J., Szili L. and Zachár A.,** Stability of polynomials, *Mathematica in Education and Research,* **7** (2) (1998), 5-12.

(Received December 12, 2004)

P. Burcsi and A. Kovács
Department of Computer Algebra
Eötvös Loránd University
H-1518 Budapest, P.O.B. 32
attila@complg.inf.elte.hu
bupe@compalg.inf.elte.hu