Rational Solutions of Linear Difference Equations

Mark van Hoeij
Department of Mathematics
Florida State University
Tallahassee, FL 32306-3027, USA
hoeij@math.fsu.edu

Abstract

This paper presents a new and sharper bound for denominators of rational solutions of linear difference and q-difference equations. This can be used to compute rational solutions more efficiently.

1 Introduction

Let τ be the $\mathbb{C}$-automorphism of $\mathbb{C}(x)$ defined by $\tau(x) = x+1$. In this paper we will consider the following homogeneous difference equations

$$\tau(Y) = AY \quad \text{with} \quad A \in GL_n(\mathbb{C}(x)) \tag{1}$$

and

$$a_n\tau^n(y) + \cdots + a_1\tau(y) + a_0 y = 0 \tag{2}$$

where $a_i \in \mathbb{C}(x)$ with $a_n \neq 0$, $a_0 \neq 0$. Inhomogeneous equations can be reduced to homogeneous equations (cf. section 2.2), so treating the homogeneous case is sufficient.

Computing a *bound for the denominator* is a key step in the algorithm (cf. [1, 3, 2]) for computing *rational solutions*, i.e. solutions $Y \in \mathbb{C}(x)^n$ or $y \in \mathbb{C}(x)$. The purpose of this paper is to give a sharper bound for the denominator of rational solutions of equation (1). A consequence of having a smaller denominator is that the numerator one needs to compute is also smaller, and this significantly speeds up the computation of the rational solutions. One of the applications of computing rational solutions is a generalization of Gosper's algorithm, given in [4].

Note that equation (2) can be reduced to equation (1) by taking $Y = (y, \tau(y), \ldots, \tau^{n-1}(y))^T$ (this results in a companion matrix). Hence our method can also be used to bound the denominator of solutions of equation (2). Examples show that our bound can be much smaller than the currently used bound. In particular, if all solutions are rational (i.e. if there are n linearly independent rational solutions) then our bound is exact. The idea in this paper is related to of *finite singularities*, which were introduced recently in [6]. Except for the points 0 and ∞, the method in this paper can also be used to bound the valuations of rational solutions of q-difference equations, if q is not a root of unity.

Acknowledgments: I would like to thank Michael Singer who pointed out me that this material can be explained more easily with matrix equations instead of scalar equations.

2 The bound

Definition 1 *Consider equation (2). A rational function $D \in C(x)$ is a* bound for the denominator *if each rational solution $y \in C(x)$ can be written as $y = N/D$ for some $N \in C[x]$. A* bound for the numerator *is an upper bound for the degree of N.*

Note that one could allow only polynomials D instead of rational functions (replace D by the numerator of D). We will not do so because that can increase the bound for the numerator.

Definition 2 *Consider equation (1). A vector $D = (D_1, \ldots, D_n)^T \in C(x)^n$ is a* bound for the denominator *if for each rational solution $Y = (Y_1, \ldots, Y_n)^T \in C(x)^n$ one has $Y_i = N_i/D_i$ for some $N_i \in C[x]$.*

So such bound is a separate bound D_i for each entry of the vector Y.

Definition 3 *Let $y \in C(x)$ and $p \in P^1(C) = C \bigcup \{\infty\}$. Let t_p be a local parameter at p; take $t_p = x - p$ if $p \in C$ and $t_p = 1/x$ if $p = \infty$. Then $y \in C(x) \subset C((t_p))$ can be written as $\sum_i y_i t_p^i$ where $y_i \in C$. Now the* valuation *of y at p is defined as $v_p(y) = \inf\{i | y_i \neq 0\}$.*

The valuation is the lowest power of t_p with a non-zero coefficient. The valuation of 0 is ∞.

If a is a polynomial and p is finite then $v_p(a)$ is the order of a at p, i.e. the highest power of $x-p$ that divides a. And $v_\infty(a) = -\text{degree}(a)$. If $y \in \mathbb{C}(x)$, $y = a/b$ where a and b are polynomials then $v_p(y) = v_p(a) - v_p(b)$. Furthermore the sum of $v_p(y)$ taken over all $p \in P^1(\mathbb{C})$ is zero. The following statements can easily be verified:

- If $y = N/D$ with $N \in \mathbb{C}[x]$ then
$$\text{degree}(N) = -v_\infty(D) - v_\infty(y). \tag{3}$$
Hence, given D, computing a bound for the numerator of y is equivalent with computing a lower bound for $v_\infty(y)$.

- Let N_p be an integer for every $p \in P^1(\mathbb{C})$, and $N_p \neq 0$ for only finitely many p. Let N be the sum of the N_p taken over all $p \in P^1(\mathbb{C})$. Then

$$V = \{y \in \mathbb{C}(x) | v_p(y) + N_p \geq 0 \text{ for all } p\}$$

is a $\mathbb{C}$-vector space of dimension $\max\{0, N+1\}$. Note: this is a special case of the Riemann-Roch theorem, the case that the curve is $P^1(\mathbb{C})$. The N_p for finite points $p \in \mathbb{C}$ correspond to a bound for the denominator D for elements of V.

So computing a bound for the denominator of y is equivalent with computing a lower bound for the valuations $v_p(y)$ at every $p \in \mathbb{C}$ (assuming that this lower bound is nonzero for only finitely many $p \in \mathbb{C}$). To compute a bound for the numerator of y one needs to find a lower bound for the valuation at infinity and use equation (3). To find such lower bound for $v_\infty(y)$ for solutions y of equation (2) we can use the same approach as in [1, 2]. Bounds at infinity for equation (1) can be obtained from [2], similar to the differential case [5]. In the rest of this paper we will only consider the problem of bounding the denominator, in other words finding lower bounds for the valuations at finite points.

If $f_1, \ldots, f_m \in \mathbb{C}[x]$ then

$$v_p(\gcd(f_1, \ldots, f_m)) = \min\{v_p(f_1), \ldots, v_p(f_m)\} \qquad (4)$$

for all $p \in \mathbb{C}$. The same formula is also true for rational functions, if one defines the gcd $g \in \mathbb{C}(x)$ of $f_1, \ldots, f_m \in \mathbb{C}(x)$ in such a way that $f_i/g \in \mathbb{C}[x]$ and the degrees of f_i/g are minimal with this property. With formula (4) several properties of valuations can be translated to gcd's, and so one could consider using gcd's to give the bound in the next section. However, in this paper we will use valuations, because that makes the bound easier to define.

2.1 Bounding the valuation at a finite point

Consider the matrix $A \in GL_n(\mathbb{C}(x))$ in equation (1). Let $S \subset \mathbb{C}$ be the set of points $p \in \mathbb{C}$ for which A has a pole at p, or $\det(A(p)) = 0$. So for all $p \in \mathbb{C} \setminus S$ we can substitute p for x, and obtain a matrix $A(p) \in GL_n(\mathbb{C})$. Let

$$\overline{S} = \{p \in \mathbb{C} | \exists_{p_1, p_2 \in S} \ \ p - p_1 - 1 \in \mathbb{N}, p_2 - p \in \mathbb{N}\}$$

where $\mathbb{N}$ is the set of nonnegative integers. The sets S and $\overline{S}$ are finite. Note that if S is not empty then S is not a subset of $\overline{S}$.

If $p \notin S$ then A and A^{-1} do not have a pole at p. So if $p \notin S$ then Y has a pole at p if and only if Y has a pole at $p+1$ because of

$$Y(p+1) = A(p)Y(p) \ \text{ and } \ Y(p) = A^{-1}(p)Y(p+1).$$

So if a rational solution Y of equation (1) would have a pole at some $p \in \mathbb{C} \setminus \overline{S}$ then Y would have infinitely many poles, which is impossible for rational functions. Hence Y can not have any poles in $\mathbb{C} \setminus \overline{S}$, in other words 0 is a lower bound for the valuation at all $p \in \mathbb{C} \setminus \overline{S}$, for each entry of the vector $Y \in \mathbb{C}(x)^n$.

Let $p \in \overline{S}$. Take $N \in \mathbb{N}$ such that $p - N \notin \overline{S}$. Then $Y(p) = A(p-1)Y(p-1) = A(p-1)A(p-2)Y(p-2) = \cdots$, so

$$Y(p) = A_N(p)Y(p-N) \qquad (5)$$

and

$$Y = A_N \ \tau^{-N}(Y) \qquad (6)$$

where $A_N \in GL_n(\mathbb{C}(x))$ is defined as

$$A_N = \tau^{-1}(A)\tau^{-2}(A) \cdots \tau^{-N}(A). \qquad (7)$$

Define $B_i^l(p)$ as the minimum of the valuations at p of the entries in the i'th row of A_N. The entries of Y have no poles at $p - N$ because $p - N \notin \overline{S}$, so the entries of $\tau^{-N}(Y)$ have no pole at p. By equations (5,6) we have that Y_i (the i'th entry of Y) is the inner product of the i'th row of A_N with a vector $\tau^{-N}(Y)$ that has no poles (i.e. valuation ≥ 0) at p. Hence $v_p(Y_i) \geq B_i^l(p)$, i.e. $B_i^l(p)$ is a lower bound for $v_p(Y_i)$ for any rational solution Y. For each entry Y_i of Y one obtains a separate bound. The bound $B_i^l(p)$ for $p \in \overline{S}$ is called the *left-hand bound*.

Instead of taking $N \in \mathbb{N}$ such that $p - N \notin \overline{S}$ one can also take $N \in \mathbb{N}$ such that $p + N \notin \overline{S}$. Then instead of equation (5) we can use

$$Y(p) = A_{-N}(p)Y(p+N) \ \text{ where } \ A_{-N} = \tau^N(A_N^{-1}). \qquad (8)$$

Now we can compute the smallest valuation at p in the i'th row of A_{-N}. This way another bound $B_i^r(p)$ for $p \in \overline{S}$ is obtained, which will be called the *right-hand bound*. Note that in case of a companion matrix system (if one started with equation (2) and reduced it to equation (1)) the computation of A^{-1} is easy so in this case computing right-hand bounds is not significantly harder than computing left-hand bounds. One can take the maximum $B_i(p) = \max\{B_i^l(p), B_i^r(p)\}$ of these two bounds as a (possibly better) lower bound for the valuations $v_p(Y_i)$ of the rational solutions Y at points $p \in \overline{S}$.

Computing the product in equation (7) is the most time consuming part in the computation of the bounds. To speed this up, one can first multiply each of these factors $\tau^{-i}(A)$ by some power of $x - p$ (in order to remove all poles at $x = p$) and then compute this product modulo a suitable power of $x - p$. This way one can obtain lower bounds for the valuation without having to completely evaluate the product in equation (7).

Theorem 1 *Let $p \in \overline{S}$. If all solutions of equation (1) are rational then the left-hand bound $B_i^l(p)$ and right-hand bound $B_i^r(p)$ are sharp. So these two bounds coincide in this case.*

Proof: Let $p \in \overline{S}$ and $q = p + N \notin \overline{S}$ where $N \in \mathbb{N}$. There exists a unique n by n matrix $Z = (Z_{ij})$ such that each Z_{ij} is a function from $q + \mathbb{N}$ to $\mathbb{C}$, that each column of Z is a solution of equation (1) and that $Z(q)$ is the identity matrix. Equation (1) lets one find the values of Z_{ij} successively at the points $q+1, q+2, \ldots$. The columns of Z form a basis of the solution space. Such a matrix is called a *fundamental solution matrix.*

If all solutions are rational then $Z_{ij} : q + \mathbb{N} \to \mathbb{C}$ are rational functions, $Z_{ij} \in \mathbb{C}(x)$. Now $Z = A_{-N}\tau^N(Z)$ because of equation (8), so

$$Z - A_{-N} = A_{-N}(\tau^N(Z) - I) \qquad (9)$$

The matrix $\tau^N(Z)$ is the identity at the point p, or equivalently: the valuations of the entries of $\tau^N(Z) - I$ are > 0 at the point p. Hence the minimum valuation at p in the i'th row of equation (9) is greater than the minimum valuation in the i'th row of A_{-N} (which equals the right-hand bound

$B_i^r(p)$). This is only possible if the minimum valuation at p in the i'th row of Z equals $B_i^r(p)$ as well. So the i'th entry of at least one of the columns of Z (each column is a rational solution of equation (1)) has valuation $B_i^r(p)$ at p. Hence the right-hand bound is sharp, and in the same way it can be shown that the left-hand bound is sharp as well, which completes the proof.

A second way to speed up the computation of bounds is illustrated by the following example. Suppose $S = \{-7/3, -1, 1, 47, 50, 101/2\}$, so $\overline{S} = \{0, 1, \ldots, 50\}$. Suppose we have computed the bounds $B_i^l(p)$ for $p \in \{0, 1, 2\}$. Let $m = \min\{B_i^l(2) | i = 1, \ldots, n\}$. Then $Y(3) = A(2)Y(2)$ where $A(2) \in GL_n(\mathbb{C})$ so $\min\{v_3(Y_i) | i = 1, \ldots, n\} = \min\{v_2(Y_i) | i = 1, \ldots, n\}$. The right-hand side of this equation is $\geq m$. Similarly, for $p \in \{2, 3, \ldots, 46\}$ the vector $Y(p+1)$ is the product of a matrix $A(p)$ (A has no poles at p) with the vector $Y(p)$, and so m is a lower bound for $v_p(Y_i)$ for $p \in \{3, 4, \ldots, 47\}$. In fact $m = \min\{B_i^l(p) | i = 1, \ldots, n\}$ for all $p \in \{3, 4, \ldots, 47\}$. So $B_i^l(p)$ need not be computed for $p \in \{3, 4, \ldots, 47\}$. This way we do not need to compute products of large numbers of matrices (although some of these $B_i^l(p)$ might possibly be better, i.e. higher, than m). To bound the valuations at $p \in \{48, 49, 50\}$ we can use the right-hand bound $B_i^r(p)$.

2.2 The inhomogeneous case

Consider the equation

$$\tau(Y) = AY + Z \tag{10}$$

where $A \in GL_n(\mathbb{C}(x))$, $Z \in \mathbb{C}(x)^n$ and where we search for solutions $Y \in \mathbb{C}(x)^n$. Let $\tilde{Y}$ be a new difference variable that is interpreted as a constant. The difference equation for this is

$$\tau(\tilde{Y}) = \tilde{Y}. \tag{11}$$

Combining equations (10,11) and replacing Z by $\tilde{Y}Z$ results in the homogeneous equation

$$\tau \begin{pmatrix} Y \\ \tilde{Y} \end{pmatrix} = \begin{pmatrix} A & Z \\ 0 & 1 \end{pmatrix} \begin{pmatrix} Y \\ \tilde{Y} \end{pmatrix}.$$

The solutions of the inhomogeneous n by n equation (10) can be obtained from the solutions of this homogeneous $n+1$ by $n+1$ equation.

3 Example

Consider the following difference equation

$$\tau^2(y) - 2\frac{(x+101)\,(x-99)}{(x+102)\,(x-98)}\tau(y) + \frac{(x-100)\,(x+100)}{(x+102)\,(x-98)}y = 0.$$

A basis for the rational solutions $y \in \mathbb{C}(x)$ is $1/(x-100)$, $1/(x+100)$. In the current algorithm (cf. [1]) in Maple the bound D will be a polynomial of degree 201, $D = (x-100)(x-99)(x-98)\cdots(x+100)$. Our bound in this example is $D = (x-100)(x+100)$, which is sharp. With this smaller denominator, the numerator N that needs to be computed ($N = c_0 + c_1 x$ where c_0, c_1 are arbitrary constants) is also much smaller and hence the computation will be faster.

To find the bound $(x-100)(x+100)$ for the denominator of y, we first consider

$$Y = \begin{pmatrix} y \\ \tau(y) \end{pmatrix}, \quad \tau(Y) = AY \text{ where } A = \begin{pmatrix} 0 & 1 \\ -a_0 & -a_1 \end{pmatrix}.$$

Here a_0 is the coefficient of y in the equation and a_1 is the coefficient of $\tau(y)$. The set S is $\{-102, -100, 98, 100\}$ and $\overline{S} = \{-101, -100, \ldots, 99, 100\}$. To find the left-hand bounds at $p = -101$, $p = -100$ and $p = -99$ we need the valuations of A_1 at $p = -101$, the valuations of A_2 at $p = -100$ and the valuations of A_3 at $p = -99$.

$$A_1 = \begin{pmatrix} 0 & 1 \\ -\frac{(x-101)\,(x+99)}{(x+101)\,(x-99)} & 2\,\frac{(x-100)\,(x+100)}{(x+101)\,(x-99)} \end{pmatrix},$$

$$A_2 = \begin{pmatrix} -\frac{(x-102)\,(x+98)}{(x+100)\,(x-100)} & 2\,\frac{(x-101)\,(x+99)}{(x+100)\,(x-100)} \\ -2\,\frac{(x-102)\,(x+98)}{(x+101)\,(x-99)} & 3\,\frac{(x-101)\,(x+99)}{(x+101)\,(x-99)} \end{pmatrix},$$

$$A_3 = \begin{pmatrix} -2\,\frac{(x-103)\,(x+97)}{(x+100)\,(x-100)} & 3\,\frac{(x-102)\,(x+98)}{(x+100)\,(x-100)} \\ -3\,\frac{(x-103)\,(x+97)}{(x+101)\,(x-99)} & 4\,\frac{(x-102)\,(x+98)}{(x+101)\,(x-99)} \end{pmatrix}.$$

The valuations of the entries of these matrices at resp. $p = -101$, $p = -100$ and $p = -99$ are

$$\begin{pmatrix} \infty & 0 \\ -1 & -1 \end{pmatrix}, \quad \begin{pmatrix} -1 & -1 \\ 0 & 0 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Taking the minimum in each row results in the following left-hand bounds

$$\begin{pmatrix} 0 \\ -1 \end{pmatrix}, \quad \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

The exponents of $(x+101)$, $(x+100)$, and $(x+99)$ in the vector D below are -1 times these left-hand bounds. Using the same argument as at the end of section 2.1 we find 0 as a lower bound for the valuation at $p \in \{-98, \ldots, 97, 98\}$. For $p \in \{99, 100\}$ we can compute the right-hand bounds. Combining all these lower bounds for the valuations gives the bound for the denominator

$$\begin{aligned} D &= \begin{pmatrix} (x+101)^0(x+100)^1(x-99)^0(x-100)^1 \\ (x+101)^1(x+100)^0(x-99)^1(x-100)^0 \end{pmatrix} \\ &= \begin{pmatrix} (x+100)(x-100) \\ (x+101)(x-99) \end{pmatrix} \end{aligned}$$

The bound for y is the first entry, and the bound for $\tau(y)$ is the second entry of this vector.

3.1 Equations of order 1

For an equation $\tau(y) + ay = 0$ of order 1 with $a \in \mathbb{C}(x)$, $a \neq 0$, the dimension of the solution space is 1. So if there is a non-zero rational solution $y \in \mathbb{C}(x)$, then all solutions are rational and our bound is sharp. Hence in this case $v_p(y)$ is equal to both the left-hand and the right-hand bound at every $p \in \mathbb{C}$, so $v_p(y) = B^l(p) = B^r(p)$. Note that a non-zero rational function $y \in \mathbb{C}(x)$ is determined up to a constant factor by its valuations $v_p(y)$, $p \in \mathbb{C}$.

So in order to compute the rational solutions of $\tau(y) + ay = 0$ all we need to do is compute the $B^l(p)$ and/or the $B^r(p)$ (if $B^l(p) \neq B^r(p)$ then there is no non-zero rational solution). Then construct $y \in \mathbb{C}(x)$ such that $v_p(y) = B^l(p)$ for every $p \in \mathbb{C}$. Then verify whether y is a solution (either by substituting it in the equation, or by computing the $g_p(L)$, see below). If it is not, then there are no rational solutions.

Note that finding the bounds $B^l(p)$ and $B^r(p)$ is a computation very similar to computing the sets $\overline{g}_p(L)$ from [6]. If L is an operator of order 1, corresponding to a difference equation $\tau(y) + ay = 0$ of order 1, then L has a non-zero rational solution if and only if all $g_p(L)$ are trivial, where p runs through the set of finite singularities and the point at infinity.

So for equations of order 1, we do not need to solve a system of linear equations (like in Gosper's algorithm) for finding the numerator of the solutions. This is possible because the bounds $B^l(p)$ and $B^r(p)$ equal the valuation of every non-zero rational solution in this case.

References

[1] S. A. Abramov. Rational solutions of linear difference and q-difference equations with polynomial coefficients, *Programming and Comput. Software* **21**, No 6, p. 273 – 278. Transl. from *Programmirovanie*, No 6, p. 3 – 11, (1995).

[2] S. A. Abramov, M.A. Barkatou. Rational Solutions of First Order Linear Difference Systems, *these ISSAC proceedings.* (1998).

[3] S. A. Abramov, M. Bronstein, M. Petkovsek. On Polynomial Solutions of Linear Operator Equations, *ISSAC'95 proceedings, Montreal, ACM Press*, (1995).

[4] S. A. Abramov, M. van Hoeij, A method for the Integration of Solutions of Ore Equations *ISSAC'97 Proceedings*, p. 172-175 (1997).

[5] M.A. Barkatou, E. Pflügel. A rational algorithm to compute a super-irreducible form of a linear differential system, *RR IMAG-LMC, Grenoble.* To appear. (1997).

[6] M. van Hoeij. Finite Singularities and Hypergeometric Solutions of Linear Recurrence Equations. preprint. Available from `http://klein.math.fsu.edu/~hoeij/papers.html`

[7] M. Petkovšek. Hypergeometric solutions of linear recurrences with polynomial coefficients. *J. Symbolic Comput.*, 14(2-3):243–264, 1992.

[8] M. van der Put, M.F. Singer. Galois Theory of Difference Equations, ISBN 3-540-63243-3, 1997.