Finite Singularities and Hypergeometric Solutions of Linear Recurrence Equations

Mark van Hoeij

October 22, 1997

Abstract

In this paper the notion of finite singularities of difference operators is introduced. An application is given, namely a new algorithm for computing hypergeometric solutions of difference equations.

1 Introduction

The goal of this paper is to introduce the notion of finite singularities of difference equations (recurrence equations) and to give some of their properties. So far only the singularity at infinity has been studied because that is the only point in $P^1(\mathbb{C})$ which is invariant under the shift operator τ, where $\tau(x) = x+1$. Since $x \mapsto x+1$ does not leave the elements of $\mathbb{C}$ invariant, the finite singularities should be elements of $\mathbb{C}/\mathbb{Z}$ instead of $\mathbb{C}$.

In the theory of differential operators, a singularity p is studied by considering differential operators over $\mathbb{C}((x-p))$, or $\mathbb{C}((1/x))$ if $p = \infty$. The shift operator $\tau : \mathbb{C}(x) \to \mathbb{C}(x)$ can be extended to $\mathbb{C}((1/x))$ but not to $\mathbb{C}((x-p))$ for $p \in \mathbb{C}$, and so for finite singularities we can not use a construction similar to the one in the differential case. For a finite singularity $p = q + \mathbb{Z} \in \mathbb{C}/\mathbb{Z}$ where $q \in \mathbb{C}$ we will consider left solutions $u : \{q-M, q-(M+1), q-(M+2), \ldots\} \to \mathbb{C}$ and right solutions $u : \{q+M, q+M+1, q+M+2, \ldots\} \to \mathbb{C}$ of the difference equation, where M is a sufficiently large integer. We will show how one can obtain right solutions from left solutions by deforming the difference equation with $x \mapsto x+\epsilon$. After the deformation the left solutions are defined over the field of constants $\mathbb{C}(\epsilon)$, and a 1-1 map from these left solutions to the corresponding right solutions can be given. Then one can study the difference in ϵ-valuation between these left and right solutions. That yields integers about the singularity p which are useful for efficient computation of hypergeometric solutions.

Furthermore we can also use this construction to define a map from the left solutions to the right solutions of the original (not deformed) equation. This map will in general not be 1-1. If it is 1-1 then after a transformation the singularity can be discarded, similar to the differential case where semi-regular points can be discarded in Beke's algorithm (c.f. section 4 in [7]). The kernel and image of this map can sometimes be used for computing hypergeometric solutions as well. We also give two relations between infinite and finite singularities in the case of an equation of order 1, similar to Fuchs' relation in the differential case.

2 Preliminaries and definitions

Let $\mathcal{W}$ be the set of all functions to $\mathbb{C}$ that are defined on some subset of $\mathbb{C}$. Let $k = \mathbb{C}(x)$ and τ the $\mathbb{C}$-automorphism of k defined by $\tau(x) = x+1$. A *difference operator* is an operator

$$L = a_n\tau^n + \cdots a_0\tau^0 \tag{1}$$

that acts in the following way on $f \in \mathcal{W}$

$$(L(f))(x) = a_n f(x+n) + \cdots + a_0 f(x).$$

In this paper the coefficients a_i will be elements of k. The function $L(f) \in \mathcal{W}$ is defined for those $x \in \mathbb{C}$ for which $f(x), \ldots, f(x+n)$ and $a_0(x), \ldots, a_n(x)$ are defined. If $a_n \neq 0$ then n is called the *order* of L.

The set of all difference operators is

$$k[\tau] = \{a_n \tau^n + \cdots a_0 \tau^0 | n \in \mathbb{N}, a_0, \ldots, a_n \in k\}.$$

The following

$$\tau \cdot a = \tau(a)\tau \tag{2}$$

defines the multiplication on $k[\tau]$. This turns $k[\tau]$ into a non-commutative ring. Using this relation (2) any product of difference operators can be written in a unique way in the form (1), i.e. the coefficients in k appear on the left of the τ^i. Multiplication in $k[\tau]$ corresponds to composition of difference operators; if $L = L_1 \cdot L_2$ then $L(f) = L_1(L_2(f))$ (on the subset of $\mathbb{C}$ where both are defined).

A sequence $u(0), u(1), u(2), \ldots$ of complex numbers is a function

$$u : \mathbb{N} \to \mathbb{C}.$$

So a sequence is an element of $\mathcal{W}$. Now u is called a solution of L if $L(u) = 0$, i.e.

$$L(u)(x) = a_n u(x+n) + \cdots + a_0 u(x) = 0$$

for all x for which $L(u)(x)$ is defined. So a difference operator $L = a_n \tau^n + \cdots a_0 \tau^0$ of order n corresponds to a recurrence relation of order n. For example $u(m) = m!$ is a solution of $L = \tau - (x+1)$.

We would also like to consider sequences that are solutions of an operator like $L = \tau - 1/(x-3)$, however, the coefficients of this L are not defined for all $x \in \mathbb{N}$. To avoid such problems with domains of definition we will consider sets $V_{p,r}$ and $V_{p,l}$ consisting of germs of sequences. For $p \in \mathbb{C}/\mathbb{Z}$, $p = q + \mathbb{Z}$ for some $q \in \mathbb{C}$, define W_p as the set of functions from $q + \mathbb{Z}$ to $\mathbb{C}$. Define the equivalence relations $\sim_r$ and $\sim_l$ on W_p as

$$u \sim_r v \iff \exists_M \forall_{x>M} u(x) = v(x)$$

and

$$u \sim_l v \iff \exists_M \forall_{x<M} u(x) = v(x).$$

Now $V_{p,r} = W_p / \sim_r$ is the set of right germs of W_p and $V_{p,l} = W_p / \sim_l$ is the set of left germs of W_p. Every element of $V_{p,r}$ is a germ of a function to $\mathbb{C}$ that is defined on $\{q+M, q+M+1, \ldots\} \subset \mathbb{C}$ for some sufficiently large integer M. Now the action of $L = \tau - 1/(x-3)$ is not defined on W_0, because the images of L are not defined at $x = 3$ and hence these images are not elements of W_0. However, L is defined on $V_{p,r}$ and on $V_{p,l}$ for all p. The elements of the set $V_{0,r}$ can be represented by sequences $u : \mathbb{N} \to \mathbb{C}$ that are defined on all but a finite number of elements of $\mathbb{N}$, where two sequences are identified if they differ at only finitely many places. Similarly elements of $V_{p,r}$ can be represented by germs of functions $u : q + \mathbb{N} \to \mathbb{C}$. Multiplication and addition on $V_{p,r}$ corresponds to multiplication and addition of functions $u : q + \mathbb{N} \to \mathbb{C}$. The invertible elements of $V_{p,r}$ correspond to those u for which $u(x) = 0$ for only finitely many $x \in q + \mathbb{N}$. If u is zero for infinitely many $x \in q + \mathbb{N}$ then $1/u$ is not defined. In this case u is either 0 in $V_{p,r}$ (if the number of x for which $u(x) \neq 0$ is finite) or a zero-divisor in $V_{p,r}$ otherwise.

Each element $f \in k$ is a function from $\mathbb{C}$ to $\mathbb{C}$ that is defined on all but a finite number of elements of $\mathbb{C}$, so f is defined on the set $\{q+M, q+M+1, \ldots\} \subset \mathbb{C}$ whenever M is sufficiently large. This way k can be viewed as a subset of the sets $V_{p,r}$, and similarly also as a subset of $V_{p,l}$. Now $V_{p,r}$ and $V_{p,l}$ are k-algebras and $k[\tau]$-modules. The set $V_{0,r}$ is called $\mathcal{S}$ in [11], where it is shown that the Picard-Vessiot ring of L over k can be embedded in $\mathcal{S}$. This Picard-Vessiot ring can be embedded in each of the $V_{p,r}$ and $V_{p,l}$.

Definition 1 *Let* $L = a_n\tau^n + \cdots + a_0\tau^0 \in k[\tau]$ *and* $L \neq 0$. *Denote*

$$\mathrm{ord}(L) = \max(\{i|a_i \neq 0\}) - \min(\{i|a_i \neq 0\})$$

$$\mathrm{order}(L) = \max(\{i|a_i \neq 0\}).$$

L is called normal *if* $a_0 \neq 0$, *i.e. if* $\mathrm{ord}(L) = \mathrm{order}(L)$. *Let*

$$V_{p,r}(L) = \{u \in V_{p,r}|L(u) = 0\}$$

$$V_{p,l}(L) = \{u \in V_{p,l}|L(u) = 0\}$$

be the kernels of L on $V_{p,r}$ and on $V_{p,l}$. These will be called the solution spaces of L in $V_{p,r}$ and in $V_{p,l}$.

The *leading* coefficient of L is the highest non-zero coefficient of L (which is a_n if $a_n \neq 0$). The *trailing* coefficient is the lowest non-zero coefficient of L (which is a_0 if L is normal). L is called *monic* if the leading coefficient is 1.

Theorem 1 *The dimension (as a $\mathbb{C}$-vector space) of the solution spaces is*

$$\dim(V_{p,r}(L)) = \dim(V_{p,l}(L)) = \mathrm{ord}(L).$$

The problems with the domain of definition and problems with vanishing of the leading or trailing coefficients of L have been eliminated by taking germs of sequences (i.e. sequences modulo the given equivalence relation). This makes the theorem easy to prove, it corresponds to the well-known statement that recurrence relations of order n, for which the leading and trailing coefficients never vanish, have an n-dimensional solution space.

Definition 2 *A k-algebra V is called a* universal extension *of k if*

1. $\tau : V \to V$ *is an automorphism that extends* $\tau : k \to k$,
2. *for every $L \in k[\tau]$ the kernel of $L : V \to V$ is an* $\mathrm{ord}(L)$*-dimensional $\mathbb{C}$-vector space, and*
3. *for every $u \in V$ there exists a non-zero $L \in k[\tau]$ such that $L(u) = 0$.*

A universal extension exists because one can verify that $\{u \in V_{p,r}|\exists_L L(u) = 0\}$ is a $k[\tau]$-module and k-algebra (to show closure under addition and multiplication use LCLM and symmetric products of operators, see below for a definition). See section 6.2 in [11] for another existence proof, where a universal extension is constructed using a difference ring extension of $\mathbb{C}((1/x))$ (so a local construction at the point $p = \infty$, we used a finite point $p \in \mathbb{C}/\mathbb{Z}$).

Let V be a universal extension of k. V is unique (see [11]) up to difference isomorphisms (i.e. isomorphisms that commute with τ). V can be embedded in each of the $V_{p,r}$ and $V_{p,l}$ for any $p \in \mathbb{C}/\mathbb{Z}$ but not in a unique way because V has many difference automorphisms. We denote the solution space of L in V by $V(L)$. We use this notation $V(L)$ instead of $V_{p,r}(L)$ or $V_{p,l}$ when the $p \in \mathbb{C}/\mathbb{Z}$ and the choice l or r (left or right) are not relevant.

$k[\tau]$ is a Euclidean ring; one can compute $\mathrm{GCRD}(L_1, L_2)$, the *greatest common right divisor* of two operators L_1 and L_2, c.f. [8, 4]. One can also compute an operator $\mathrm{LCLM}(L_1, L_2)$, the *least common left multiple*. Requiring that the LCLM and GCRD are monic makes them uniquely defined.

Lemma 1 *For every non-zero $M \in k[\tau]$ there exists a unique monic normal $L \in k[\tau]$ for which*

$$V(L) = V(M).$$

If L_1 and L_2 are normal operators then

1. *L_1 is a right-hand factor of L_2 if and only if* $V(L_1) \subset V(L_2)$.
2. $L_3 = \mathrm{GCRD}(L_1, L_2)$ *is normal and* $V(L_3) = V(L_1) \bigcap V(L_2)$.

3. $L_4 = \mathrm{LCLM}(L_1, L_2)$ *is normal and* $V(L_4) = V(L_1) + V(L_2)$.

We will skip the proof. Later in the paper we will often only consider operators that are normal, or normal and monic. According to the lemma this is no real restriction.

Definition 3 *An element* u *of* $V_{p,r}$ *or* $V_{p,l}$ *or* V *is called* rational *if it is an element of* k*, and it is called* hypergeometric *if it is a solution of an operator of order 1, so* $\tau(u) = ru$ *for some* $r \in k$*. The set of all hypergeometric elements of* V *is denoted by* H*.*

For example the sequence $u(n) = n!$ is hypergeometric, it corresponds to a hypergeometric element of V. Rational sequences (u is a rational function in n) are also hypergeometric. $H^* = H \setminus \{0\}$ is a group under multiplication; hence for example $u(n) = (n!)^3/(n+3)$ is hypergeometric. If $u \in H^*$ and $L \in k[\tau]$ then $L(u)/u \in k$ and hence $L(u) \in H$. H is not closed under addition.

Lemma 2 *If* $a, b \in H^*$ *then* $a + b \in H \iff a/b \in k^*$.

Proof: Let $u = a/b \in H^*$. If $u \in k^* = k \setminus \{0\}$ then it is easy to see that $a + b \in H$. If $a + b = 0 \in H$ then clearly $u \in k^*$. Now assume $a, b, c \in H^*$ where $c = a + b$, and $u \notin k$. Then by definition of hypergeometric, $\tau(a) = ra$, $\tau(b) = sb$ and $\tau(c) = tc$ for some $r, s, t \in k^*$. Then $ta + tb = tc = \tau(c) = \tau(a + b) = \tau(a) + \tau(b) = ra + sb$ so $(r - t)a + (s - t)b = 0$. If $r \neq t$ then $u = a/b = -(s - t)/(r - t) \in k$, and if $r = t$ then $0 + (s - t)b = 0$ so $s = t = r$ and hence $\tau(a/b) = (ra)/(sb) = a/b$ which implies $a/b \in \mathbb{C} \subset k$.

□

In a similar way it can be shown more generally that for $u_1, \ldots, u_n \in H^*$, if $u_1 + \cdots + u_n = 0$ then $u_i/u_j \in k^*$ for some $i \neq j$. Similar to the differential case one can define

Definition 4 *Let* $L_1, L_2 \in k[\tau]$ *be normal and of order* ≥ 1*. Then the* symmetric product $L = L_1 \circledS L_2$ *is defined as the normal monic operator of minimal order such that* $y_1 y_2 \in V(L)$ *for all* $y_1 \in V(L_1)$ *and* $y_2 \in V(L_2)$*.*

Using the relation $L_1(y_1) = 0$ we can write any $\tau^i(y_1)$ as a k-linear combination of $\tau^0(y_1), \ldots, \tau^{n-1}(y_1)$ where $n = \mathrm{order}(L_1)$, and similarly for the $\tau^i(y_2)$. Then L can be obtained by computing a k-linear relation between $y_1 y_2$, $\tau(y_1)\tau(y_2)$, $\tau^2(y_1)\tau^2(y_2)$, ….

Lemma 3 *If* $L_1 = \tau - r$ *with* $r \in k^*$*,* $u \in H^*$ *with* $L_1(u) = 0$*, and* L_2 *is monic and normal then*

$$su \cdot L_2 \cdot \frac{1}{u} = L_1 \circledS L_2 \in k[\tau] \quad \text{where} \quad s = \tau^{\mathrm{order}(L_2)}(u)/u \in k^*.$$

To prove this note that $su \cdot L_2 \cdot \frac{1}{u}$ is monic and has the same solution space as $L_1 \circledS L_2$. Furthermore $L_2 \cdot v \in v \cdot k[\tau]$ for every $v \in H^*$ so $su \cdot L_2 \cdot \frac{1}{u} \in su \cdot 1/u \cdot k[\tau] = k[\tau]$.

3 A generalization of Gosper's algorithm

Gosper's algorithm (c.f. [6]) answers the following question: Let $M = \delta = \tau - 1$, $u \in H^*$, compute (if it exists) $v \in H^*$ such that $\delta(v) = u$. In [2] this was generalized to $u \in V$; given $L \in k[\tau]$ of minimal order such that $u \in V(L)$, then [2] gives a method to find $\tilde{L}$ of minimal order such that $\delta(V(\tilde{L})) = V(L)$, and if the orders of L and $\tilde{L}$ are the same then $r \in k[\tau]$ is given such that $v = r(u)$ is a solution of $\delta(v) = u$.

Now we will give a different generalization of Gosper's algorithm (which also generalizes [10]), let $u \in H^*$, $r \in k^*$ with $(\tau - r)(u) = 0$, and let M be any element of $k[\tau]$. Compute, if it exists, $v \in H^*$ such that $M(v) = u$.

Since $M(v) \in k \cdot v$ for all $v \in H$ we have $v = au$ for some $a \in k^*$. Now $u = M(v) = M(ua) = u(\frac{1}{u} \cdot M \cdot u)(a)$, so $1 = (\frac{1}{u} \cdot M \cdot u)(a) = s \cdot L(a)$ where $L = M \circledS (\tau - 1/r)$ and $s = \tau^{\mathrm{order}(M)}(u)/u \in k^*$. Hence we can compute all $v \in H^*$ for which $M(v) = u$ by computing all rational solutions of $L(a) = 1/s$, a problem for which algorithms exist, c.f. [1]. A similar result can be obtained for the differential case as well.

4 The singularity at infinity

It is well-known that one can study the singularity of L at the point $p = \infty$, and that this leads to several algorithms for difference operators. However, the finite singularities of L have not been studied until now, and these are useful as well. In section 6 we will show how the finite singularities can be used to give a more efficient algorithm for computing hypergeometric solutions of difference equations. In this section we will list the things we need to use from the singularity $p = \infty$. The finite singularities $p \in \mathbb{C}/\mathbb{Z}$ will be introduced in section 5.

Let $L = \tau - r$ or $L = a \cdot (\tau - r)$ for some $a \in k^*$, and let $u \in H^*$ be a non-zero solution of L. Define the commutative group

$$\mathcal{H}_\infty = \mathbb{C}^* \times \mathbb{Z} \times (\mathbb{C}/\mathbb{Z}).$$

We will use the additive notation for this group, $(c_1, n_1, d_1) + (c_2, n_2, d_2) = (c_1 c_2, n_1 + n_2, d_1 + d_2) \in \mathcal{H}_\infty$. Let $t = 1/x$. Then r can be written as $r = c \cdot t^n \cdot (1 + dt + e)$ for some $c, d \in \mathbb{C}$ and $e \in t^2\mathbb{C}[[t]]$. Now define the *growth* of L and *growth* of u at ∞ as

$$g_\infty(u) = g_\infty(L) = (c, n, d + \mathbb{Z}) \in \mathcal{H}_\infty.$$

$\mathbb{C}((t))$ where $t = 1/x$ is a difference field extension of k, $\tau(t) = \tau(1/x) = 1/(x+1) = t/(1+t) \in \mathbb{C}((t))$. The definition of $g_\infty(L)$ for an operator L of order 1 applies for $\mathbb{C}((t))[\tau]$ as well.

Definition 5 *Let $L \in \mathbb{C}((t))[\tau]$ be normal. Then $\overline{g}_\infty(L)$ is defined as the set of $g_\infty(M)$ for all right-hand factors $M \in \mathbb{C}((t))[\tau]$ of L of order 1.*

If $L \in k[\tau]$ then the set $\overline{g}_\infty(L)$ may contain more elements than the set of $g_\infty(M)$ for all first order right-hand factors $M \in k[\tau]$, because L can have more right-hand factors in $\mathbb{C}((t))[\tau]$ than in $k[\tau]$.

Lemma 4 *The number of elements of $\overline{g}_\infty(L)$ is at most* $\mathrm{order}(L)$.

This follows from factorization properties in $\mathbb{C}((t))[\tau]$, and also from the structure of the formal solutions at the point ∞. We give a brief sketch, for more details see [3, 5, 12]. The elements $(c, n, d) \in \mathbb{C} \times \mathbb{Z} \times (\mathbb{C}/\mathbb{Z})$ of $\overline{g}_\infty(L)$ can be computed as follows: For the ring $\mathbb{C}((t))[\tau]$ one can define a Newton polygon and Newton polynomial (called the τ-polygon and characteristic equation in [3]). The slopes of that polygon give the possible values for n, and c must be a root of the corresponding Newton polynomial. To find d we take the symmetric product of the operator with $\tau - 1/(ct^n)$, then we need to search for a factor $\tau - (1 + dt + e)$ for some $e \in t^2\mathbb{C}[[t]]$. Let $\delta = \tau - 1$. By writing the operator as a polynomial in δ instead of τ one can define a different Newton polygon (called the δ-polygon in [3]). Then d can be found as a root of a Newton polynomial for slope 1. This way the (c, n, d), and hence $\overline{g}_\infty(L)$, can be found with little computation.

5 Finite singularities of difference equations

The definitions in this section are the main results in this paper.

Definition 6 *Let $L = a_n\tau^n + \cdots a_0\tau^0 \in k[\tau]$. Then $p \in \mathbb{C}/\mathbb{Z}$ is called a* singularity *of L if there is an a_i with a pole in $p + \mathbb{Z}$, or if the leading or trailing coefficient (a_n and a_0 if $a_n \neq 0$ and $a_0 \neq 0$) has a root in $p + \mathbb{Z}$. The point ∞ is considered a singularity as well.*

The set of singularities of L is a finite subset of $\mathbb{C}/\mathbb{Z} \bigcup \{\infty\}$. One can multiply L on the left by an element of $\mathbb{C}[x]$ in order to obtain an element of $\mathbb{C}[x, \tau]$ with the same solution space. So without loss of generality we may assume that $L \in \mathbb{C}[x, \tau]$. Then the finite singularities are the roots modulo $\mathbb{Z}$ of the leading and trailing coefficients of L.

Let $p \in \mathbb{C}$ and $r \in k^*$. The valuation $v_p(r)$ is the largest integer n such that $r/(x-p)^n \in \mathbb{C}[[x-p]]$. The value of $v_p(0)$ is ∞.

Definition 7 *Let $r \in k^*$ and $p \in \mathbb{C}/\mathbb{Z}$. Then the* valuation *of r at p is*

$$v_p(r) = \sum_{q \in p+\mathbb{Z}} v_q(r).$$

Let $L = \tau - r$ or $L = a \cdot (\tau - r)$ for some $a \in k^*$, and let $u \in H^*$ be a non-zero solution of L. Then the valuation growth *or* growth *of L and u at p is defined as*

$$g_p(u) = g_p(L) = v_p(r) \in \mathbb{Z}.$$

Define $\mathcal{H}$ as the product of the additive group of all functions $\mathbb{C}/\mathbb{Z} \to \mathbb{Z}$ with finite support and the group $\mathcal{H}_\infty$. Then define

$$g(u) = g(L) = (p \mapsto g_p(u), g_\infty(u)) \in \mathcal{H}.$$

For example $u(n) = 2^n(n!)$. Then $g_p(u)$ is 1 if $p = \mathbb{Z}$, it is $(2, -1, 0)$ if $p = \infty$ and 0 otherwise.

A non-zero hypergeometric solution $u \in H^*$ of L corresponds to a first order right-hand factor $\tau - r \in k[\tau]$ of L where $r = \tau(u)/u$. The map $u \mapsto \tau(u)/u$ induces isomorphisms of multiplicative groups $H^*/\mathbb{C}^* \to k^*$ and $H^*/k^* \to k^*/\simeq$, where $r_1 \simeq r_2$ iff r_1/r_2 can be written as $\tau(y)/y$ for some $y \in k^*$.

Lemma 5 *The map $g : H^* \to \mathcal{H}$ is a group homomorphism. The kernel is k^*. The image is the set of $(f, (c, n, d + \mathbb{Z}))$ where $f : \mathbb{C}/\mathbb{Z} \to \mathbb{Z}$ and $c, d \in \mathbb{C}$ and $n \in \mathbb{Z}$ for which:*

$$n + \sum_{p \in \mathbb{C}/\mathbb{Z}} f(p) = 0 \quad \text{and} \quad d + \sum_{p \in \mathbb{C}/\mathbb{Z}} f(p)p \equiv 0 \mod \mathbb{Z}. \tag{3}$$

We omit the proof. The relations (3) will be called *Fuchs' relations*, because in the differential case a similar relation with the same name (lemma 9.2 in [7]) exists between the *exponential parts*, which are the differential equivalent of the $g_p(L)$. Note that the two sums are defined because f has a finite support; $f(p) \neq 0$ for only finitely many $p \in \mathbb{C}/\mathbb{Z}$. The equivalence class of $u \in H^*$ in H^*/k^* is called the *type* of u. The type of an operator $L = \tau - r$, $r \in k^*$ with non-zero solution u is the type of u, which corresponds to the image of r in $k^*/\simeq$. According to the lemma the type of u or L is given by $g(u)$ or $g(L)$.

Definition 8 *Let $L \in k[\tau]$ and suppose $p \in \mathbb{C}/\mathbb{Z}$ is not a singularity. Then for every $u \in V_{p,l}$ there is a unique sequence $\tilde{u} : p + \mathbb{Z} \to \mathbb{C}$ such that $L(\tilde{u}) = 0$ and such that the equivalence class of $\tilde{u}$ in $V_{p,l}$ is u. Taking the equivalence class (i.e. the germ) of $\tilde{u}$ in $V_{p,r}$ defines a 1-1 map:*

$$E_{p,r} : V_{p,l}(L) \to V_{p,r}(L)$$

called the extension map*, or* extension to the right*. Similarly define*

$$E_{p,l} : V_{p,r}(L) \to V_{p,l}(L)$$

which is extension to the left*.*

Let $L = a_n\tau^0 + \cdots + a_0\tau^0 \in k[\tau]$ with $a_n \neq 0$ and $a_0 \neq 0$, and let $p \in \mathbb{C}/\mathbb{Z}$ be a singularity. We choose a basis for $V_{p,l}(L)$ as follows. Let q_l (resp. q_r) in $p + \mathbb{Z}$ be the minimum (resp. maximum) of the *problem points at* p, i.e. the elements of the set $p + \mathbb{Z}$ that occur as a root of a_na_0 or as a pole in $\{a_0, \ldots, a_n\}$. Define $u_i : \{q_l - 1, q_l - 2, \ldots\} \to \mathbb{C}$ by: for $1 \leq j \leq n$ let $u_i(q_l - j)$ be 1 if $i = j$ and 0 otherwise. The other values of u_i are determined by the recurrence equation $L(u_i) = 0$. Now $u_1, \ldots, u_n$ is a basis of $V_{p,l}(L)$. Similarly we can define a basis $v_1, \ldots, v_n$ of $V_{p,r}(L)$ where $v_i : \{q_r + 1, q_r + 2, \ldots\} \to \mathbb{C}$. Let $L_\epsilon \in \mathbb{C}(x, \epsilon)[\tau]$ be the *deformation* of L, which is L with x replaced by $x + \epsilon$, where ϵ is a new constant (a is called a *constant* if $\tau(a) = a$). So we increased the field of constants from $\mathbb{C}$ to $\mathbb{C}(\epsilon)$. For $a \in \mathbb{C}(\epsilon)$ the valuation $v_\epsilon(a)$ is the largest integer m for which $a/\epsilon^m \in \mathbb{C}[[\epsilon]]$. Now $p \in \mathbb{C}/\mathbb{Z} \subset \mathbb{C}(\epsilon)/\mathbb{Z}$

is not a singularity of L_ϵ. So the $\mathbb{C}(\epsilon)$-vector spaces $V_{p,l}(L_\epsilon)$ and $V_{p,r}(L_\epsilon)$ can be identified by $E_{p,r}$ and elements u of these sets can be identified with a function $u : p+\mathbb{Z} \to \mathbb{C}(\epsilon)$ for which $L_\epsilon(u) = 0$. For such u define the *left valuation* $v_{\epsilon,l}(u)$ as $\min(\{v_\epsilon(u(m))|m \in p+\mathbb{Z}, m < q_l\})$ and *the right valuation* $v_{\epsilon,r}(u) = \min(\{v_\epsilon(u(m))|m \in p+\mathbb{Z}, m > q_r\})$. If $v_{\epsilon,l}(u) \geq 0$ then we can define the *left projection* $\rho_l(u) \in V_{p,l}(L)$ by substituting $\epsilon = 0$ in u (in other words: taking u mod ϵ). Similarly if $v_{\epsilon,r}(u) \geq 0$ then the *right projection* $\rho_r(u) \in V_{p,r}(L)$ is defined. For each basis element u_i of $V_{p,l}(L)$ we can choose $\tilde{u}_i \in V_{p,l}(L_\epsilon)$ with left valuation ≥ 0 and $\rho_l(\tilde{u}_i) = u_i$. These $\tilde{u}_i$ are not unique. Similarly we can choose $\tilde{v}_i \in V_{p,r}(L_\epsilon)$ with right valuation ≥ 0 and $\rho_r(\tilde{v}_i) = v_i$. The following definition is the main result of this paper.

Definition 9 *With notations as above, define the* minimum valuation growth *of L at p as*

$$g_{p,r}(L) = \min(\{v_{\epsilon,r}(\tilde{u}_i)|1 \leq i \leq n).$$

Define the maximum valuation growth *as*

$$g_{p,l}(L) = -\min(\{v_{\epsilon,l}(\tilde{v}_i)|1 \leq i \leq n).$$

Define the $\mathbb{C}$-linear maps

$$E_{p,r} : V_{p,l}(L) \to V_{p,r}(L) \quad \text{and} \quad E_{p,l} : V_{p,r}(L) \to V_{p,l}(L)$$

by

$$E_{p,r}(u_i) = \rho_r(\tilde{u_i}/\epsilon^{g_{p,r}(L)}) \quad \text{and} \quad E_{p,l}(v_i) = \rho_l(\tilde{v}_i\epsilon^{g_{p,l}(L)}).$$

Define

$$\overline{g}_p(L) = \{i \in \mathbb{Z}|g_{p,r}(L) \leq i \leq g_{p,l}(L)\}.$$

If $p \in \mathbb{C}/\mathbb{Z}$ is not singular then $\overline{g}_p(L) = \{0\}$. If $p \in \mathbb{C}/\mathbb{Z}$ is singular and $\overline{g}_p(L) = \{0\}$ then p is called an *apparent* singularity. If $\overline{g}_p(L)$ has only 1 element then p is called a *semi-apparent* singularity. If $\overline{g}_p(L)$ has more than 1 element then p is called an *essential* singularity. Note that the definition of $E_{p,r}$ and $E_{p,l}$ depends on L because $g_{p,r}(L)$ and $g_{p,l}(L)$ depend on L. So, if confusion could occur, these should be denoted as $E_{p,r,L}$ and $E_{p,l,L}$.

Lemma 6 *For all non-zero solutions u of L_ϵ we have $v_{\epsilon,r}(u) - v_{\epsilon,l}(u) \in \overline{g}_p(L)$. In particular for all $p \in \mathbb{C}/\mathbb{Z}$ we have $\overline{g}_p(L) \neq \emptyset$, i.e. $g_{p,r}(L) \leq g_{p,l}(L)$.*

Proof: Without loss of generality we may assume that $v_{\epsilon,l}(u) = 0$. Write u on the basis $\tilde{u}_i$ (notations the same as above), $u = c_1\tilde{u}_1 + \cdots + c_n\tilde{u}_n$ with $c_i \in \mathbb{C}(\epsilon)$. Since $v_\epsilon(u) \geq 0$ it follows that $v_\epsilon(c_i) \geq 0$. Hence the right valuation of u must be at least the minimum of the right valuations of the $\tilde{u}_i$, so $v_{\epsilon,r}(u) \geq g_{p,r}(L)$, hence $v_{\epsilon,r}(u) - v_{\epsilon,l}(u) \geq g_{p,r}(L)$. In a similar way one has $v_{\epsilon,r}(u) - v_{\epsilon,l}(u) \leq g_{p,l}(L)$, and the statement follows.

□

Lemma 7 *If L is normal and* $\mathrm{order}(L) = 1$ *then $g_{p,r}(L) = g_{p,l}(L) = g_p(L)$, in other words $\overline{g}_p(L) = \{g_p(L)\}$.*

We skip the proof. The following lemma follows from lemma 6.

Lemma 8 *Let $L, L_1, L_2 \in k[\tau]$ be normal and $L = L_1L_2$. Then $\overline{g}_p(L_2) \subset \overline{g}_p(L)$.*

Lemma 9 *Let $L_1, L_2 \in k[\tau]$ be normal, and let* $\mathrm{order}(L_2) = 1$. *Then $\overline{g}_p(L_1 \circledS L_2) = \overline{g}_p(L_1) + g_p(L_2)$ for all $p \in \mathbb{C}/\mathbb{Z} \bigcup \{\infty\}$.*

Lemma 10 *If $g_{p,r}(L) = g_{p,l}(L)$ (i.e. p is a semi-apparent singularity) then $E_{p,r}$ and $E_{p,l}$ are each other's inverses. If $g_{p,r}(L) \neq g_{p,l}(L)$ (i.e. p is an essential singularity) then the image of $E_{p,r}$ (resp. $E_{p,l}$) is a subset of the kernel of $E_{p,l}$ (resp. $E_{p,r}$).*

$$\mathrm{Im}(E_{p,r}) \subset \mathrm{Ker}(E_{p,l}) \quad \text{and} \quad \mathrm{Im}(E_{p,l}) \subset \mathrm{Ker}(E_{p,r}).$$

If $p \in \mathbb{C}/\mathbb{Z}$ is not a singularity then $E_{p,l}$ and $E_{p,r}$ are isomorphisms of G-modules where G is the *difference Galois group* (for a definition see [11]) of L. However, at singularities the linear maps $E_{p,r}$ and $E_{p,l}$ are in general not G-homomorphisms, because at essential singularities the kernels and images are non-trivial even when L is irreducible.

6 Computing hypergeometric solutions

Computing hypergeometric solutions is equivalent to computing first order right-hand factors; if $u \in H^*$ is a non-zero hypergeometric solution then $\tau - \tau(u)/u \in k[\tau]$ is a right-hand factor of L. The type of u is determined by $g(u)$, so when $g(u)$ is known, an operator $\tau - r$ with the same type can be constructed. By taking the symmetric product with $\tau - 1/r$ we get a right-hand factor $\tau - (\tau(u)/u)/r$ which has the trivial type and hence a rational solution. So all u can be found by trying all possible $g(u)$ and computing rational solutions for each case. This leads to the following algorithm.

Algorithm hypergeometric solutions
Input: $L = a_n\tau^n + \cdots + a_0\tau^0$ with $a_n \neq 0$, $a_0 \neq 0$ and $n \geq 2$.
Output: All hypergeometric solutions, parametrized by constants c_i.

1. Let $S = \{p_1, \ldots, p_m\} \subset \mathbb{C}/\mathbb{Z} \bigcup \{\infty\}$ be the set of singularities.
2. result := {}
3. For all $h = (h_1, \ldots, h_m)$ with $h_i \in \overline{g}_{p_i}(L)$ that satisfy Fuch's relations (3) do
   (a) Construct $r \in k^*$ such that the singularities of $\tau - r$ are in S, and $g_{p_i}(\tau - r) = h_i$.
   (b) Let $b_1, \ldots, b_q \in k$ be a basis of rational solutions of $L \circledS (\tau - 1/r)$.
   (c) If $q > 0$ then result := result$\bigcup\{u \cdot (c_1 b_1 + \cdots + c_q b_q)\}$ where c_i are parameters and $u \in H^*$ is a solution of $\tau - r$.
4. RETURN result.

Note that we could skip all apparent finite singularities in the algorithm, that would not change the computation. Furthermore we can compute $r \in k^*$ such that $\{g_p(\tau - r)\} = \overline{g}_p(L)$ for all semi-apparent singularities $p \in \mathbb{C}/\mathbb{Z}$ and such that $\tau - r$ does not have other finite singularities. Then $L \circledS (\tau - 1/r)$ has an apparent singularity at all these p, and this way these p can be discarded as well.

For $L \in k[\tau]$ the *field of definition* is the smallest subfield of $\mathbb{C}$ over which all coefficients are defined. This is always a finite extension of $\mathbb{Q}$ and hence not an algebraically closed field. One of the main benefits of our algorithm over the algorithm in [9] is that instead of having to compute in the splitting field of all singularities, our algorithm "only" needs to compute in the splitting field of the essential singularities, which is likely to be much smaller. Furthermore the number of cases (the number of loops in step 3) in our algorithm is usually much smaller than (but at most equal to) the number of cases in [9].

7 Improvements

A small improvement is the following: when during the algorithm a hypergeometric solution u is found (equivalently: when a first order right hand factor $\tau - r$ is found where $r = \tau(u)/u \in k^*$), we can write $L = L_2 \cdot (\tau - r)$. Let $M = L \circledS (\tau - 1/r) = L_3 \cdot (\tau - 1)$ for some L_3 with $\mathrm{order}(L_3) = \mathrm{order}(L) - 1$. The non-constant hypergeometric solutions of M can be obtained by computing the hypergeometric solutions of L_3 and applying Gosper's algorithm on those. Multiplying the hypergeometric solutions of M by u gives the hypergeometric solutions of L. This process is called *reduction of order*. It may speed up the algorithm in the previous section if a hypergeometric solution is found early in the computation.

If all singularities are semi-apparent then the algorithm in the previous section is fast because there are few cases to check in step 3. If $p \in \mathbb{C}/\mathbb{Z}$ is not semi-apparent then in some cases we can also use the images and kernels of $E_{p,r}$ and $E_{p,l}$ to find factors or hypergeometric solutions of L. For example if L is normal and has order 2 then by lemma 10 we have $\mathrm{Im}(E_{p,r}) = \mathrm{Ker}(E_{p,l})$ and $\mathrm{Im}(E_{p,l}) = \mathrm{Ker}(E_{p,r})$. If $u \in H^*$ is a hypergeometric solution of L, then either $g_p(u) = g_{p,r}(L)$ or $u \in \mathrm{Ker}(E_{p,r})$. And either $g_p(u) = g_{p,l}(L)$ or $u \in \mathrm{Ker}(E_{p,l})$. So $u \in \mathrm{Ker}(E_{p,r})$ or $u \in \mathrm{Ker}(E_{p,l})$ (or both). Let $r = \tau(u)/u \in k^*$. If we had bounds on the degrees of the numerator and denominator of r then r can be computed by checking both cases $u \in \mathrm{Ker}(E_{p,r})$ or $u \in \mathrm{Ker}(E_{p,l})$. So there are at most two possible r. Such bounds can be obtained by a careful study of the algorithm in the previous section. Let K_p be the smallest field over which p and L are defined. Then all right-hand factors $\tau - r$ that we find are defined over K_p, because $\mathrm{Ker}(E_{p,r})$ and $\mathrm{Ker}(E_{p,l})$ are 1-dimensional and are defined over K_p. So then r must be an element of K_p for every essential singularity p, and we can conclude

Theorem 2 *Let $L \in K(x)[\tau]$ be an operator of order 2, where $K \subset \mathbb{C}$ and let $K_p = K(q)$ if $p = q + \mathbb{Z}$ for some $q \in \mathbb{C}$. Let $S \subset \mathbb{C}/\mathbb{Z}$ be the set of essential singularities. If $S \neq \emptyset$ then the number of first order monic right-hand factors $\tau - r$ is at most two, and they are elements of $\tilde{K}(x)[\tau]$ where $\tilde{K} = \bigcap_{p \in S} K_p$.*

If $S = \emptyset$ then computing the first order right-hand factors is easy. In this case the only algebraic extension that can occur is the $c \in \mathbb{C}^*$ in (c, n, d), which can be at most an extension of degree $\mathrm{order}(L) = 2$. If $S \neq \emptyset$ then we can skip all cases in the algorithm that would lead to an extension larger than $\tilde{K}$. This way computations with exponentially large algebraic extensions are avoided in the algorithm in the case of order 2.

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 and M. van Hoeij. A method for the Integration of Solutions of Ore Equations, *ISSAC'97 Proceedings*, p. 172 – 175, 1997.

[3] A. Barkatou and A. Duval. Sur les séries formelles solutions d'équations aux différences polynomiales. *Ann. Inst. Fourier (Grenoble)*, 44(2):495–524, 1994.

[4] M. Bronstein and M. Petkovšek. An introduction to pseudo-linear algebra. *Theoret. Comput. Sci.*, 157(1):3–33, 1996.

[5] A. Duval. Lemmes de Hensel et factorisation formelle pour les opérateurs aux différences. *Funkcial. Ekvac.*, 26(3):349–368, 1983.

[6] Jr. Gosper, R. William. Decision procedure for indefinite hypergeometric summation. *Proc. Nat. Acad. Sci. U.S.A.*, 75(1):40–42, 1978.

[7] M. van Hoeij. Factorization of Differential Operators with Rational Functions Coefficients, *to appear in J. Symb. Comp.* 1997.

[8] O. Ore. *The theory of non-commutative polynomials*, Ann. Maths. **34**, 480 – 508, 1933.

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

[10] M. Petkovšek. A generalization of Gosper's algorithm. *Discrete Math.*, 134(1-3):125–131, 1994. Algebraic and topological methods in graph theory (Lake Bled, 1991).

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

[12] E. Tournier. Solutions formelles d'équations différentielles, *Thèse d'Etat, Faculté des Sciences de Grenoble*, 1987.