J. Symbolic Computation (1985) **1**, 303–315

Theory of Summation in Finite Terms

MICHAEL KARR

Software Options Inc., Cambridge, Massachusetts 02138, *USA*

(*Received* 7 *November* 1984)

This paper discusses some of the mathematical aspects of an algorithm for finding formulas for finite sums. The results presented here concern a property of difference fields which show that the algorithm does not divide by zero, and an analogue to Liouville's theorem on elementary integrals.

1. Introduction

A decision procedure for the problem of determining the existence of a "formula" for a given summation has appeared in the computing literature (Karr, 1981). The purpose of this paper is to discuss some mathematical aspects of the problem which were suppressed in the presentation of the algorithmic aspects of the solution.

We consider summations in which the limit of the summation is not involved in the summand. Given such a sum $\sum_i f_i$, the problem of finding a formula g is that of inverting the formula $\Delta g = f$. This in turn suggests using difference fields (or rings) to study the problem. Indeed, the very definition of "finite terms" is made precise for this problem by requiring that g lie in a certain difference field.

This paper has two major results. The first is a remarkable property of the class of difference fields in which the decision procedure applies. This property is necessary only to show that at a certain point, the decision procedure does not divide by zero. Even the definitions are suppressed in Karr (1981). The second result is the difference field analogue to Liouville's theorem on elementary integrals (Rosenlicht, 1968). Its importance is more mathematical than algorithmic, although it does say "where to look" for a formula.

All fields in this paper have characteristic 0. We do not define difference fields in terms of Δ; rather, following the usual convention (Cohn, 1965):

DEFINITION. A *difference field* is a field F together with an automorphism σ of F. The *constant field* $K \subseteq F$ is the fixed field of σ.

One thinks of σ as a shift operator—$\sigma(f(x)) = f(x+1)$—so that Δ with the right algebraic properties may be defined as $\Delta f = \sigma f - f$. But σ is easier to work with, and Δ is seldom mentioned in what follows.

2. Extensions

Throughout this paper we shall consider extensions of the following kind.

0747–7171/85/030303 + 13 $03.00/0

DEFINITION. Let $F(t), \sigma$ be an extension difference field of F, σ. This extension is *first-order-linear* $\overset{\text{def}}{\Leftrightarrow}$

(a) $\sigma t = \alpha \cdot t + \beta$, where $\alpha, \beta \in F$.

(b) t is transcendental over F.

(c) $K(F(t)) = K(F)$ (i.e. the constant field is not extended).

By condition (a), we think of t as a solution to the first order linear difference equation $\sigma t - \alpha \cdot t = \beta$.

Using first-order-linear extensions, it is possible to model formal sums and products. If we let $\alpha = 1$, then t behaves like the indefinite sum $\sum_i \beta_i$. If we let $\beta = 0$, then t behaves like the indefinite product $\prod_i \alpha_i$. It is of special interest to know when an extension can be written with $\beta = 0$. The intrinsic property is this:

DEFINITION. Let E, σ be a difference field extension of F, σ. We say that $g \in E$ is *homogeneous over* $F \overset{\text{def}}{\Leftrightarrow} g \notin F$ but $\sigma g/g \in F$. We say the extension is *homogeneous over* $F \overset{\text{def}}{\Leftrightarrow}$ there exists a g which is homogeneous over F.

THEOREM 2.1. *Let $F(t), \sigma$ be a difference field extension of F, σ in which $\sigma t = \alpha \cdot t + \beta$. The following are equivalent.*

(a) The extension is homogeneous.

(b) There exists $g \in F[t]$, $g \notin F$, with $\sigma g/g \in F$.

(c) The equation $\sigma w - \alpha \cdot w = \beta$ can be solved for $w \in F$.

PROOF. Assume (a), and obtain $g_0 \in F(t)$, $g_0 \notin F$, with $\sigma g_0/g_0 \in F$. If t is algebraic, then $F(t) = F[t]$, so we can prove (b) by letting $g = g_0$. If t is transcendental, we write g_0 as the quotient of relatively prime polynomials, $g_0 = g_1/g_2$. Then

$$\sigma g_0/g_0 = (g_2 \cdot \sigma g_1)/(g_1 \cdot \sigma g_2) \Rightarrow g_1 | g_2 \cdot \sigma g_1 \text{ and } \sigma g_2 | g_2 \cdot \sigma g_1$$

$$\Rightarrow g_1 | \sigma g_1 \text{ and } \sigma g_2 | g_2 \quad (\text{because } \gcd(\sigma g_1, \sigma g_2) = 1).$$

Thus $\sigma g_1/g_1 \in F$ and similarly $\sigma g_2/g_2 \in F$. Now $g_i \notin F$ for either $i = 1$ or 2; otherwise $g_0 \in F$. Letting $g = g_i$ completes the proof that (a)$\Rightarrow$(b).

We next show that (b)$\Rightarrow$(c). Write g of part (b) as $g = \sum_i w_i t^i$, and let $u = \sigma g/g \in F$. The degree m of g is $\geqslant 1$, and we equate coefficients of t^m and t^{m-1} in $\sigma g = u \cdot g$:

$$\alpha^m \cdot \sigma w_m = u \cdot w_m \text{ and } \quad m \cdot \alpha^{m-1} \cdot \beta \cdot \sigma w_m + \alpha^{m-1} \cdot \sigma w_{m-1} = u \cdot w_{m-1}$$

$$\Rightarrow m \cdot \beta/\alpha + \sigma(w_{m-1}/w_m)/\alpha = w_{m-1}/w_m.$$

Letting $w = -w_{m-1}/(m \cdot w_m)$ shows that $-\beta + \sigma w = \alpha \cdot w$, proving (b)$\Rightarrow$(c).

Finally, assume (c), and subtract $\sigma w - \alpha \cdot w = \beta$ from $\sigma t - \alpha \cdot t = \beta$ to obtain $\sigma(t-w)/(t-w) = \alpha \in F$, and we let $g = t - w$, which is clearly not in F, so the extension is homogeneous. This completes the ring of implications.

The proof of (c)$\Rightarrow$(a) in this result shows how to change the basis so that any homogeneous extension can be written with $\beta = 0$. We hereafter consider only the following type of homogeneous extension.

DEFINITION. We say that $F(t), \sigma$ is a $\prod$-*extension* of $F, \sigma \overset{\text{def}}{\Leftrightarrow}$

(a) The extension is first-order-linear.

(b) $\sigma t = \alpha \cdot t$.

We want to know when homogeneous extensions are also first-order-linear. This leads to:

DEFINITION. Given a difference field F, σ, the *homogeneous group*,

$$H(F, \sigma) \overset{\text{def}}{=} \{\sigma g/g \mid 0 \neq g \in F\}.$$

If σ is understood, we write $H(F)$; if F also is understood, we write H. The following is easily verified.

PROPOSITION. *The elements of H, with multiplication from F, form a group.*

We can now simply state the desired characterisation.

THEOREM 2.2. *Let $F(t), \sigma$ be a difference field extension of F, σ with $t \neq 0$; let $\sigma t = \alpha \cdot t$, $\alpha \in F$. This extension is first-order-linear $\Leftrightarrow \alpha^n \notin H(F)$, for all $n > 0$.*

PROOF. First, suppose $\alpha^n \in H(F)$; let $w \in F$ satisfy $\sigma w/w = \alpha^n$. Then:

$$\sigma(t^n/w) = \alpha^n \cdot t^n/\sigma w = t^n/w$$

$$\Rightarrow t^n/w \in K(F(t)) \quad \text{(since it is left fixed by } \sigma)$$

$$\Rightarrow t^n/w \in K \text{ or the constant field is extended.}$$

Thus, t is algebraic over F or the constant field is extended, proving that if the extension is first-order-linear, $\alpha^n \notin H(F)$ for $n > 0$.

For the converse, assume that the extension is not first-order-linear. Suppose first that t is algebraic over F, say of degree $m > 0$. Let $g(z) = \sum_i w_i t^i \in F[z]$ be the monic irreducible polynomial of t. Then $g(t) = 0$, and

$$0 = \sigma(g(t)) = \textstyle\sum_i \sigma w_i \cdot \alpha^i \cdot t^i.$$

If we let $h(z) = \sum_i (\sigma w_i \cdot \alpha^i) \cdot z^i$, we see that $h(t) = 0$, so h must be a multiple of g. Since g is monic, we conclude

$$\alpha^m \cdot w_i = \sigma w_i \cdot \alpha^i \text{ for } i.$$

By the irreducibility of g, either $g(z) = z$, contradicting $t \neq 0$, or, there is some i for which $w_i \neq 0$, and then $\alpha^{m-i} = \sigma w_i / w_i \in H$, so letting $n = m - i > 0$ completes the proof in the algebraic case.

The remaining possibility is that t is transcendental over F, but that the constant field is extended. Let $g_0 \in F(t)$, $g_0 \notin F$ with $\sigma g_0 = g_0$. Write g_0 as the quotient of relatively prime polynomials, g_1/g_2. Then:

$$\sigma g_1/\sigma g_2 = g_1/g_2 \Rightarrow \sigma g_i/g_i \in F,$$

because $\gcd(\sigma g_1, \sigma g_2) = 1$. One of the g_i must have positive degree. We may assume it to

be monic, and if it has more than one non-zero coefficient, we may argue as for the irreducible polynomial above to produce $\alpha^n \in H$. Otherwise, that g_i is of the form t^m for $m > 0$. The constant term w of the other g_i must be non-zero (else $\gcd(g_1, g_2) \neq 1$), and matching coefficients, we have $\sigma w = \alpha^m w$. Letting $n = m$ completes the proof.

The corresponding result for inhomogeneous extensions is much simpler.

THEOREM 2.3. *Let $F(t), \sigma$ be an inhomogeneous extension of F, σ in which $\sigma t = \alpha \cdot t + \beta$. Then the extension is first-order-linear.*

PROOF. If the constant field is extended, there exists $g \in F(t)$, $g \notin F$ with $\sigma g/g = 1 \in F$. Hence the extension is homogeneous, contrary to assumption. Suppose that t is algebraic over F, and let $g(z) = \sum w_i z^i$ its irreducible polynomial. We argue as in Theorem 2.2 to find that $h(z) = \sum \sigma w_i \cdot (\alpha z + \beta)^i$ is a multiple of $g(z)$, match coefficients of z^m and z^{m-1}, and then argue as in Theorem 2.1 to discover that the extension is homogeneous, a contradiction. Thus t is indeed transcendental.

This paper considers a slightly restricted class of inhomogeneous extensions.

DEFINITION. We say that $F(t), \sigma$ is a $\sum$-extension of $F, \sigma \overset{\text{def}}{\Leftrightarrow}$

(a) The extension is inhomogeneous.

(b) For $n \neq 0$, $\alpha^n \in H \Rightarrow \alpha \in H$ where $\sigma t = \alpha t + \beta$.

We can now characterise the fields studied in this paper.

DEFINITION. An extension $F(t), \sigma$ is a *$\prod\sum$-extension* of $F, \sigma \overset{\text{def}}{\Leftrightarrow}$ it is a $\prod$-extension or a $\sum$-extension. Given a constant difference field K, we say that F, σ is a *$\prod\sum$-field* over $K \overset{\text{def}}{\Leftrightarrow}$

(a) there is a tower of fields $K = F_0 \subset \cdots \subset F_n$ in which F_i, σ is a $\prod\sum$-extension of F_{i-1}, σ, for $i = 1, \ldots, n$, or

(b) F, σ is an infinite union of ascending $\prod\sum$-fields over K.

3. Regularity

We define functions arising from iterated applications of σ.

DEFINITION. Let $k \in \mathbb{Z}, f \in F$.

$$f_{(k,\sigma)} \overset{\text{def}}{=} \prod_{0 \leqslant i < k} \sigma^i f,$$

$$f_{\{k,\sigma\}} \overset{\text{def}}{=} \sum_{0 \leqslant i < k} f_{(i,\sigma)}.$$

If σ is clear from context, it is dropped.

In these definitions, and throughout this paper, we use the convention that

$$\sum_{m \leqslant i < n} f_i = -\sum_{n \leqslant i < m} f_i \quad \text{and} \quad \prod_{m \leqslant i < n} f_i = 1/\prod_{n \leqslant i < m} f_i.$$

Thus $m \leqslant i < n$ under a $\sum$ or $\prod$ does not imply that $m < n$. This abuse of notation coincides with the more usual convention of $\sum$ or $\prod$ over a null set only when $m = n$, but it is more appropriate for present purposes. For example, $1_{(k)} = k$, regardless of the sign of k.

DEFINITION. Observe that if $\sigma t = \alpha \cdot t + \beta$, $\sigma^k t$ will be a linear polynomial in t. Define α_k and β_k by the relation $\alpha_k \cdot t + \beta_k = \sigma^k t$.

The proofs of the following formulas are left to the reader.

IDENTITIES. For $k, l \in \mathbb{Z}$ (regardless of sign):

1. $$(f \cdot g)_{(k)} = f_{(k)} \cdot g_{(k)}; \quad (\sigma f)_{(k)} = \sigma(f_{(k)}),$$
2. $$f_{(k+l)} = \sigma^k f_{(l)} \cdot f_{(k)}.$$
3. $$f_{(k \cdot i, \sigma)} = (f_{(i,\sigma)})_{(k, \sigma^i)}.$$
4. $$f_{(-k)} = 1/\sigma^{-k} f_{(k)}.$$
5. $$(\sigma^k f/f)_{(l)} = (\sigma^l f/f)_{(k)}.$$
6. $$\sigma^k f - a_{(k)} \cdot f = a_{(k)} \cdot \sum_{0 \leqslant i < k} \sigma^i [\sigma f - a \cdot f]/\alpha_{(i+1)}, \quad a \neq 0.$$
7. $$\alpha_k = \alpha_{(k)}, \quad \beta_k = \alpha_{(k)} \cdot \sum_{0 \leqslant i < k} \sigma^i \beta / \alpha_{(+1)}.$$

The following properties are central to the study of $\prod\sum$-fields.

DEFINITION. A difference field is $\prod$-*regular* $\overset{\text{def}}{\Leftrightarrow} k \neq 0$ and $f_{(k)} = 1 \Rightarrow f^k = 1$.

DEFINITION. A difference field is $\sum$-*regular* $\overset{\text{def}}{\Leftrightarrow} k \neq 0$ and $f_{(k)} = 0 \Rightarrow (f = 0$ or $(f^k = 1$ and $f \neq 1))$.

DEFINITION. A difference field is $\prod\sum$-*regular* $\overset{\text{def}}{\Leftrightarrow}$ it has both these properties.

As we shall see, $\prod\sum$-fields are $\prod\sum$-regular. This property guarantees that given $f, g \in F$, the equations $f_{(k)} = g$ (resp. $f_{(k)} = g$) have at most one solution for k, provided that f is not a root of unity (resp. $f \neq 0$ and f is not a root of unity other than 1). In the decision procedure for summation, it is necessary to know whether the k exists, and if so, what it is. If there are certain algorithms for the constant field, there is a stronger version of mere $\prod\sum$-regularity, namely that the existence of k can be computed, and its value determined. Indeed, a major part of the proof of $\prod\sum$-regularity is essentially an algorithm for analysing the above equations, and is presented in Karr (1981). This paper will touch lightly on these matters and will concentrate on results which do not enter directly into the algorithms (and which do not appear in Karr (1981)), such as the following.

LEMMA 3.1. *Let F, σ be $\prod$-regular and let H be torsion-free. Then for $k \neq 0$, $f_{(k)} = l \Rightarrow f \in K$.*

PROOF. By Identity 1, $f_{(k)} = 1 \Rightarrow (\sigma f)_{(k)} = 1$. Dividing yields:

$$1 = (\sigma f/f)_{(k)} \Rightarrow (\sigma f/f)^k = 1 \Rightarrow \sigma f/f = 1 \Rightarrow f \in K.$$

The three implications are justified by $\prod$-regularity, torsion-freeness of H, and the definition of K.

LEMMA 3.2. *Let F, σ be $\prod\sum$-regular, let $H(F)$ be torsion-free, and let $F(t), \sigma$ be a $\prod\sum$-extension. If $f \in F(t)$ has the property that $f \notin F$ but $\sigma^k f/f \in F$ for some k, then the extension is a $\prod$-extension and f is a monomial in t.*

PROOF. Using the same kind of argument as in the proof of Theorem 2.1, we may assume that f is a polynomial of non-zero degree, which we write as $\sum_i v_i \cdot t^i$, with degree m. We let $\sigma^k f/f = u \in F$.

Assume we have a $\prod$-extension, but that f has a non-zero coefficient v_j from $j < m$. Matching coefficients in $\sigma^k f = u \cdot f$ yields

$$\sigma^k v_i \cdot \alpha_{(k)}^i = u \cdot v_i \Rightarrow \sigma^k(v_m/v_j) \cdot \alpha_{(k)}^{m-j} = v_m/v_j,$$

$$\Rightarrow (\alpha^{m-j} \cdot \sigma v/v)_{(k)} = 1 \quad \text{(Let } v = v_m/v_j \text{ and use Identities 1, 5)}$$

$$\Rightarrow \alpha^{(m-j)\cdot k} = (\sigma v/v)^{-k} \in H \quad (\textstyle\prod\text{-regularity, } H \text{ is a group}).$$

By Theorem 2.2, we do not have a $\prod$-extension, contradiction. This shows that in a $\prod$-extension, f is a monomial in t.

We show that $\sigma^k f/f \in F$ leads to a contradiction in a $\sum$-extension. We match coefficients of t^m and t^{m-1} in $\sigma^k f = f$, and perform the same manipulation as in the proof of Theorem 2.1 but with α and β replaced by $\alpha_{(k)}$ and β_k. This leads to:

$$\sigma^k v - \alpha_{(k)} \cdot v = \beta_k \quad \text{where } v = -v_{m-1}/(m \cdot v_m).$$

Using Identities 6 and 7 we conclude that

$$((\sigma z/z)/\alpha)_{(k)} = 0, \quad \text{where } z = \sigma v - \alpha \cdot v - \beta.$$

Note that z cannot be zero, or the extension would be homogeneous, by Theorem 2.1. By $\sum$-regularity, $(\sigma z/z)/\alpha$ is a root of unity other than 1. But if it is a root of unity, it can be shown to be equal to 1:

$$((\sigma z/z)/\alpha^j = 1 \Rightarrow \alpha^j \in H \Rightarrow \alpha \in H \Rightarrow (\sigma z/z)/\alpha = 1.$$

The second implication is part (b) of the definition of $\sum$-extension, and the last implication follows from the torsion-free-ness of H and the fact that $(\sigma z/z)/\alpha \in H$ and is a root of unity. The contradiction shows that $\sigma^k f/f \notin F$ in a $\sum$-extension.

The proof of $\prod\sum$-regularity proceeds by induction on $\prod\sum$-extensions. The following result provides the lift for $\prod$-regularity.

LEMMA 3.3. *Let $F(t)$ be a $\prod\sum$-extension of F, σ. If F is $\prod$-regular, then so is $F(t), \sigma$.*

PROOF. See that for Theorem 5 in Karr (1981).

The proof of Lemma 3.3 is not difficult. But the lifting of $\sum$-regularity becomes quite

involved, because it seems necessary to generalise it to a property which is stable in the lifting process.

DEFINITION. Given $\zeta_1, \ldots, \zeta_s \in K$, we use the convention:

$$\zeta_{ij} \overset{\text{def}}{=} \prod_{l=i}^{j} \zeta_l \text{ for } i \leqslant j+1.$$

Given a positive integer k, we say that $\zeta_1, \ldots, \zeta_s$ forms a *ζ-set (for k)* $\overset{\text{def}}{\Leftrightarrow}$

(a) $\zeta_i^k = 1$, $i = 1, \ldots, s$.

(b) $\zeta_{ij} \neq 1$, all $i \leqslant j$.

Associated with $\zeta_1, \ldots, \zeta_s$ are the recursively defined functions:

$$\gamma_{0i} \overset{\text{def}}{=} 1 \quad \text{for all } 0 \leqslant i < k$$

$$\gamma_{ri} \overset{\text{def}}{=} \sum_{i<j<k} \gamma_{r-1,j} \cdot \zeta_r^j \quad \text{for } 0 < r \leqslant s, \quad 0 \leqslant i < k.$$

Finally, a difference field is *ζ-regular* $\overset{\text{def}}{\Leftrightarrow}$ given non-zero f, $k > 0$ and any ζ-set for k:

$$\sum_{0 \leqslant i < k} \gamma_{si} \cdot f_{(i)} = 0 \Rightarrow \zeta_1, \ldots, \zeta_s, f \text{ is a } \zeta\text{-set.}$$

By setting $s = 0$ in the definition of ζ-regularity, we see

PROPOSITION. If a difference field is ζ-regular, it is $\sum$-regular.

Unlike $\sum$-regularity, there is no algorithmic variant of ζ-regularity, and in fact, even the definition of ζ-regularity is suppressed in Karr (1981). However, it plays a major role in the theory, and of the two major results of this paper, we may now state the first.

RESULT. Any $\prod\sum$-field is ζ-regular.

This is not obvious even in a constant field. To start the induction, we require the following:

FORMULAE. Let $\zeta_1, \ldots, \zeta_s$ be a ζ-set. Then for any $f \neq 0$:

$$\sum_{0 \leqslant i < k} \gamma_{si} \cdot f^i = \begin{cases} k \cdot \prod_{j=1}^{l-1} \dfrac{1}{\zeta_{j,l-1} - 1} \cdot \prod_{j=l}^{s} \dfrac{-\zeta_{lj}}{\zeta_{lj} - 1} & \text{if } \zeta_{ls} \cdot f = 1 \\ & \text{for an } l \text{ with } 1 \leqslant l \leqslant s+1 \\ \dfrac{f^k - 1}{f - 1} \cdot \prod_{i=1}^{s} \dfrac{1}{\zeta_{is} \cdot f - 1} & \text{otherwise.} \end{cases}$$

PROOF. For $s = 0$, the result is simply that for $\sum_{0 \leqslant i < k} f^i$. Inductively, assume $s > 0$, and that the result holds for $s-1$. Using the recursive definition of γ, completely expand the left-hand expression as a nested sum (with obvious omissions if $s = 1$ or 2):

$$\sum_{i_0=0}^{k-1} \sum_{i_1=i_0+1}^{k-1} \cdots \sum_{i_s=i_{s-1}+1}^{k-1} \zeta_1^{i_s} \cdots \zeta_s^{i_1} \cdot f^{i_0}$$

$$= \sum_{i_0=0}^{k-1} \sum_{i_1=i_0+1}^{k-1} \cdots \sum_{i_{s-1}=i_{s-2}+1}^{k-1} \frac{1-\zeta_1^{i_{s-1}+1}}{\zeta_1-1} \cdot \zeta_2^{i_{s-1}} \cdots \zeta_s^{i_1} \cdot f^{i_0}$$

$$= \frac{1}{\zeta_1-1} \cdot \sum_{i_0=0}^{k-1} \sum_{i_1=i_0+1}^{k-1} \cdots \sum_{i_{s-1}=i_{s-2}+1}^{k-1} \zeta_2^{i_{s-1}} \cdots \zeta_s^{i_1} \cdot f^{i_0}$$

$$+ \frac{-\zeta_1}{\zeta_1-1} \cdot \sum_{i_0=0}^{k-1} \sum_{i_1=i_0+1}^{k-1} \cdots \sum_{i_{s-1}=i_{s-2}+1}^{k-1} (\zeta_1 \cdot \zeta_2)^{i_{s-1}} \cdot \zeta_3 \cdots \zeta_s^{i_1} \cdot f^{i_0}.$$

Since $\zeta_2, \ldots, \zeta_s$ and $\zeta_1 \cdot \zeta_2, \zeta_3, \ldots, \zeta_s$ are both ζ-sets of size $s-1$, we have produced two induction problems. Suppose first that $\zeta_{1s} \cdot f = 1$. Then for the first inductive problem, "$\zeta_{is} \cdot f$" $= \zeta_{j+1,s} \cdot f \neq 1$, so the second formula applies, yielding zero when $1/\zeta_{1s}$ is substituted for f. In the second inductive problem, the first formula applies, with "l" $= 1$, which gives (remembering "ζ_{1j}" $= \zeta_{1,j+1}$ and "s" $= s-1$):

$$\frac{-\zeta_1}{\zeta_1-1} \cdot k \cdot \prod_{j=1}^{s-1} \frac{-\zeta_{1,j+1}}{\zeta_{1,j+1}-1}.$$

Re-indexing and incorporating $-\zeta_1/(\zeta_1-1)$ into the product yields the result for $l=1$.

Next, suppose that $\zeta_{2s} \cdot f = 1$. Then for the second inductive problem, "$\zeta_{is} \cdot f$" $\neq 1$, so the second formula applies yielding 0 as above. In the first inductive problem, the first formula applies with "f" $= 1$, giving (because "ζ_{1i}" $= \zeta_{2,i+1}$ and "s" $= s-1$):

$$\frac{1}{\zeta_1-1} \cdot k \cdot \prod_{j=1}^{s-1} \frac{-\zeta_{2,j+1}}{\zeta_{2,j+1}-1}.$$

Re-indexing the product shows that this is correct for $l=2$.

To conclude the proof of the first formula, we examine the remaining cases in which $\zeta_{is} \cdot f = 1$, namely for $3 \leqslant l \leqslant s+1$. In both inductive problems, the first formula applies, yielding (with "l" $= l-1$ and appropriate substitution for "ζ_{ij}"):

$$\frac{1}{\zeta_1-1} \cdot k \cdot \prod_{j=1}^{l-2} \frac{1}{\zeta_{j+1,l-1}-1} \cdot \prod_{j=l-1}^{s-1} \frac{-\zeta_{l,j+1}}{\zeta_{l,j+1}-1}$$

$$+ \frac{-\zeta_1}{\zeta_1-1} \cdot k \cdot \frac{1}{\zeta_{1,l-1}-1} \cdot \prod_{j=2}^{l-2} \frac{1}{\zeta_{j+1,l-1}-1} \cdot \prod_{j=l-1}^{s-1} \frac{-\zeta_{l,j+1}}{\zeta_{l,j+1}-1}.$$

This equals the first formula, completing its proof.

If the first formula does not apply, then we know that $\zeta_{ls} \cdot f \neq 1$ for all l $1 \leqslant l \leqslant s+1$. Hence, in each of the inductive problems, the second formula applies, and a calculation like the previous one yields the second formula.

COROLLARY $\gamma_{s0} = (-l)^s$.

PROOF. Left to reader.

We are now in a position to start the inductive process of proving regularity in $\prod\sum$-fields.

LEMMA 3.4. *A constant difference field is $\prod$-regular, ζ-regular and its homogeneous group is torsion-free.*

PROOF. Since in this case $f_{(k)} = f^k$, $\prod$-regularity is immediate; since $H(K) = \{1\}$, the torsion-free property is also. To prove ζ-regularity, let $\zeta_1, \ldots, \zeta_s$ be a ζ-set. If $\sum_i \gamma_{si} \cdot f^i = 0$, the first of the Formulae cannot have applied because for $k > 0$ it is non-zero. We thus conclude $\zeta_{ls} \cdot f \neq 1$. Hence the second of the Formulae applies, from which we deduce $f^k - 1 = 0$. The rest of the ζ-set conditions for $\zeta_1, \ldots, \zeta_s, f$ follow from those for $\zeta_1, \ldots, \zeta_s$.

The following result is used in the lifting of ζ-regularity, and will eventually provide us with the result that if F, σ is a $\prod\sum$-field over K, so is F, σ^k for $k \neq 0$.

LEMMA 3.5. Let E, σ be $\prod$- and $\sum$-regular; suppose $H(F)$ is torsion-free. If $F(t), \sigma$ is a $\prod$-extension (resp. $\sum$-extension), then for $k \neq 0$, $F(t), \sigma^k$ is a $\prod$-extension (resp. $\sum$-extension) of F, σ^k.

PROOF. Parts (a) and (b) of the definition of first-order-linear are clear. Suppose part (c) is false, i.e. $f \in F(t)$, $f \notin F$ with $\sigma^k f = f$. By Lemma 3.1, the extension is a $\prod$-extension and $f = u \cdot t^n$ for $n \neq 0$, $u \in F$. Then:

$$1 = \sigma^k f / f = (\sigma f / f)_{(k)} = (\alpha^n \cdot \sigma u / u)_{(k)}. \qquad \text{(Identity 5)}$$

We saw in the proof of Lemma 3.1 that this equation shows that we do not have a $\prod$-extension, a contradiction which proves part (c).

To complete the proof in the case of a $\prod$-extension, all that is needed is that $\beta_k = 0$, which is obvious. In a $\sum$-extension, we must show that $F(t), \sigma^k$ is an inhomogeneous extension of F, σ^k. By Theorem 2.1, we must show that $\sigma^k w - \alpha_{(k)} \cdot w = \beta_k$ cannot be solved for $w \in F$, an argument made in the proof of Lemma 3.1. This shows we have an inhomogeneous extension. The last step is to prove part (b) in the definition of a $\sum$-extension. Let $n \neq 0$.

$$\begin{aligned} & \alpha_{(k)}^n \in H(F, \sigma^k) \\ \Rightarrow\ & \exists\ w \text{ with } \alpha_{(k)}^n = \sigma^k w / w = (\sigma w / w)^{(k)} \\ \Rightarrow\ & (\alpha^n / (\sigma w / w))_{(k)} = 1 \Rightarrow \alpha^{n \cdot k} \in H \Rightarrow \alpha \in H \\ \Rightarrow\ & \exists\ v \text{ with } \alpha = \sigma v / v \Rightarrow \alpha_{(k)} = (\sigma v / v)_{(k)} = \sigma^k v / v \in H(F, \sigma^k). \end{aligned}$$

This is the required implication.

The following result is what really motivates the definition of ζ-sets and ζ-regularity. With $s = 0$, it is the key to lifting $\sum$-regularity, but to prove it for "s", F, σ must be ζ-regular for "$s+1$". Thus, lifting $\sum$-regularity arbitrarily high seems to require ζ-regularity with an arbitrarily large "s" in the starting field. But since ζ-regularity is an "impossibility" property, it does not infiltrate the decision procedure.

LEMMA 3.6. *Let F, σ be ζ-regular, and let $F(t), \sigma$ be a $\prod\sum$-extension. Let $h \in F[t]$, $h \in F$ and let t not divide h in a $\prod$-extension. Let $0 \neq u \in F$. Then for any $k > 0$:*

$$\sum_{0 \leqslant i < k} \gamma_{si} \cdot u_{(i)} \cdot \sigma^i h \neq 0.$$

PROOF. We assume that the sum in 0, and derive a contradiction. Assume first we have a $\prod$-extension. Since h has no factors of period 0, its constant term is non-zero. Let $h = vt^n + \ldots + w$. If the sum is zero, then its coefficient of t^n and its constant term must be

zero. Specifically, by ζ-regularity:

$$\sum_{0 \leqslant i<k} \gamma_{si} \cdot u_{(i)} \cdot \sigma^i v \cdot \alpha_{(k)}^n = 0 = \sum_{0 \leqslant i<k} \gamma_{si} \cdot u_{(i)} \cdot \sigma^i w$$

$$\Rightarrow (u \cdot (\sigma v/v) \cdot \alpha^n)^k = 1 = (u \cdot (\sigma w/w))^k.$$

By dividing these equations, one sees that $\alpha^{n \cdot k} \neq h$, contradicting Theorem 2.2. This proves the result in $\prod$-extensions.

In $\sum$-extensions, we let $h = v \cdot t^n + w \cdot t^{n-1} + \ldots$, $v \neq 0$, and argue that the coefficients of t^n and t^{n-1} in the expanded sum are zero.

$$\sum_{0 \leqslant i<k} \gamma_{si} \cdot (u \cdot \alpha^n)_{(i)} \cdot \sigma^i v = 0 = \sum_{0 \leqslant i<k} \gamma_{si} \cdot (u \cdot \alpha^{n-1})_{(i)} \cdot [\sigma^i v \cdot n \cdot \beta_i + \sigma^i w].$$

From the first equality and ζ-regularity, we obtain

$$\zeta_1, \ldots, \zeta_{s+1} \text{ is a } \zeta\text{-set where } \zeta_{s+1} \overset{\text{def}}{=} u \cdot \alpha^n \cdot \sigma v/v.$$

Substituting the implied value for u into the second equation gives

$$0 = n \cdot v \cdot \sum_{0 \leqslant i<k} \gamma_{si} \cdot \zeta_{s+1}^i \cdot [\beta_i + \sigma^i(w/(n \cdot v))]/\alpha_{(i)}.$$

Letting $z = -w/(n \cdot v)$, we rewrite this equality

$$\sum_{0 \leqslant i<k} \gamma_{si} \cdot \zeta_{s+1}^i \sigma^i z/\alpha_{(i)} = \sum_{0 \leqslant i<k} \gamma_{si} \cdot \zeta_{s+1}^i \cdot \beta_i/\alpha_{(i)}$$

$$= \sum_{0 \leqslant i<k} \gamma_{si} \cdot \zeta_{i+1}^i \cdot \Big(\alpha_{(i)} \cdot \sum_{0 \leqslant j<i} \sigma^j \beta/\alpha_{(j+1)}\Big) \cdot \alpha_{(i)} \qquad \text{(Identity 7)}$$

$$= \sum_{0 \leqslant i<k-1} \Big(\sum_{i<j<k} \gamma_{sj} \cdot \zeta_{s+1}^j\Big) \cdot \sigma^i \beta/\alpha_{(i+1)} \qquad \text{(reverse } \textstyle\sum\text{'s)}$$

$$= \sum_{0 \leqslant i<k-1} \gamma_{s+1,j} \cdot \sigma^i \beta/\alpha_{(i+1)} \qquad \text{(definition of } \gamma_{s+1}\text{) (‡).}$$

We return to the first expression in this line of equalities, and make the substitution

$$\gamma_{si} \cdot \zeta_{s+1}^i = \gamma_{s+1,i-1} - \gamma_{s+1,i}$$

for $i > 0$, and $\gamma_{s0} = -\gamma_{s+1,0}$ (from the Corollary):

$$-\gamma_{s+1,0} \cdot z + \sum_{0 \leqslant i<k} \gamma_{s+1,i-1} \cdot \sigma^i z/\alpha_{(i)} - \sum_{0 \leqslant i<k} \gamma_{s+1,i} \cdot \sigma^i z/\alpha_{(i)}.$$

From the definition, $\gamma_{s+1,k-1} = 0$, so we re-index and combine with (‡)

$$\sum_{0 \leqslant i<k} \gamma_{s+1,i} \cdot \sigma^i[(\sigma z - \alpha \cdot z - \beta)/\alpha]/\alpha_{(i)} = 0.$$

Letting $y = (\sigma z - \alpha \cdot z - \beta)/\alpha$, we know that $y \neq 0$ (or the extension is inhomogeneous), so we divide the equation by y:

$$\sum_{0 \leqslant i<k} \gamma_{s+1,i}((\sigma y/y)/\alpha)_{(i)} = 0$$

$$\Rightarrow (\sigma y/y) \cdot \alpha \text{ is a root of unity other than 1} \qquad (\zeta\text{-regularity}).$$

An argument in the proof of Lemma 3.1 shows that this is impossible, the final contradiction which establishes the result.

LEMMA 3.7. Let $F(t), \sigma$ be a $\prod\sum$-extension of F, σ. Suppose for all $i \neq 0$, F, σ^i is ζ-regular and $H(F, \sigma^i)$ is torsion-free. Then $F(t), \sigma$ is ζ-regular.

PROOF. Let $\zeta_1, \ldots, \zeta_s$ be a ζ-set for $k > 0$, and let $f \in F(t)$. If $f \in F$, we can use ζ-regularity of F, σ, so we show that $f \notin F$ leads to a contradiction. Extend the notion of degree from $F[t]$ to $F(t)$ by

$$\deg(g) \stackrel{\text{def}}{=} \deg(\text{num}(f)) - \deg(\text{den}(f));$$

let $m = \deg(f)$. Since $\gamma_{s0} \neq 0$ (Corollary), and since $\deg(f_{(i)}) = m \cdot i$, if $m < 0$, the degree of the $i = 0$ term would be 0 and would be larger than all other terms, so $\deg(\sum_i \gamma_{si} \cdot f_{(i)}) = 0$, contradicting $\deg 0 = -\infty$. Thus $m \geqslant 0$.

If $m > 0$, $\deg(\sum_i \gamma_{si} \cdot f_i)$ will be $r \cdot m$ where r is the largest index $< k$ such that $\gamma_{st} \neq 0$. Since $\gamma_{s0} \neq 0$, some such r will exist, making this degree positive, so that the sum cannot possibly be zero, contradiction. Thus $m = 0$.

In Karr (1981), there is a reduction method important to the decision procedure which shows that if $\sum_i \gamma_{si} \cdot f_{(i)} = 0$, there exists a polynomial $h \in F[t]$, where $h \notin F$ and H is not divisible by t in a $\prod$-extension, a non-zero $u \in F$, and $p \geqslant 0$, always 0 in a $\sum$-extension, with

$$\sum_{0 \leqslant i < k} \gamma_{si} \cdot \sigma^i h(u/t^p)_{(i)} = 0.$$

Suppose we have a $\sum$-extension with $p > 0$. Looking at the partial fraction expansion of the left-hand side of this equation (and using t not dividing h in a $\prod$-extension), we see that t occurs to the power $r \cdot p$ in the denominator, where r is as above. But since the right-hand side is zero, we see $r \cdot p = 0$, whence $r = 0$. In this case, the above simplifies to $\gamma_{s0} \cdot h = (-1)^s \cdot h = 0$, a contradiction proving $p = 0$ in all extensions. Lemma 3.6 provides the final contradiction.

Since we have occasionally used torsion-free-ness of H in lifting, we must also lift torsion-free-ness. The relevant result is:

LEMMA 3.8. *Let $F(t), \sigma$ be a $\prod\sum$-extension of F, σ and suppose F, σ is $\prod$-regular and $H(F)$ is torsion-free. Then $H(F(t))$ is torsion-free.*

PROOF. Let $f \in F(t)$, $(\sigma f/f)^k = 1$ with $k \neq 0$. Assume that f has an irreducible factor f, i.e. f divides num(f) or den(f). We first consider the case in which $\sigma\text{f}/\text{f} \notin F$. Without loss of generality, we may assume that $\sigma^k \text{f} | \text{f} \Rightarrow k \geqslant 0$. Since σf will contain factors σ^lf only when $l > 0$ we conclude f is a factor of σf/f, and thus of $(\sigma\text{f}/\text{f})^k$, so that this quantity cannot be equal to 1. Thus, $\sigma\text{f}/\text{f} \in F$.

By Lemma 3.1, we know that we can write $f = u \cdot t^n$, with $n \neq 0$ only in a $\prod$-extension. But in a $\prod$-extension,

$$1 = (\sigma f/f)^k = \alpha^{n-k} \cdot \sigma u^k / u^k \Rightarrow \alpha^{n \cdot k} \in H \Rightarrow n = 0.$$

The last implication is by Theorem 2.2. In all extensions, then, $f \in F$, and we conclude $f = 1$ by torsion-free-ness of $H(F)$.

The proof of the following result is by now a technical exercise.

THEOREM. *Let F, σ be a $\prod\sum$-field over K. Then:*

(*a*) *F, σ is $\prod$-regular and ζ-regular.*

(*b*) *H is torsion-free.*

(*c*) *F, σ^k is $\prod\sum$-field over K for $k \neq 0$.*

4. Solutions

In this section, we shall study the solution to $\sigma g - a \cdot g = f$ where $a, f \in F$. In particular, we want to understand in which $\prod\sum$-fields the equation can be solved, if it cannot be solved for $g \in F$.

DEFINITION. A *basis* for the $\prod\sum$-tower $F = F_0 \subseteq \ldots \subseteq F_n = E$ is a tuple $t_1, \ldots, t_n$ where $F_i = F_{i-1}(t_i)$. We define $\alpha_i, \beta_i \in F_{i-1}$ by $\sigma t_i = \alpha_i \cdot t_i + \beta_i$ (*not* by iterated applications of σ).

Given an equation $\sigma g - a \cdot g = f$ with $a, f \in F$, it is helpful to adjust a basis relative to a and F.

DEFINITION. Given a tower and its basis as above, and $a \in F$, we say that the basis is *normalized* wrt (with respect to) $a \overset{\text{def}}{\Leftrightarrow}$

$$\beta_i \neq 0 \quad \text{and} \quad a/\alpha_i \in H(F_{i-1}) \Rightarrow \alpha_i = a, \quad \text{for } i = 1, \ldots, n.$$

The basis is *reduced* wrt $F \overset{\text{def}}{\Leftrightarrow}$ for $i = 1, \ldots, n$:

$$\beta_i \neq 0 \quad \text{and} \quad \exists\, h \in F_{i-1} \text{ with } \sigma h - \alpha_i \cdot h + \beta \in F \Rightarrow \beta_i \in F.$$

PROPOSITION. *For any finite $\prod\sum$-tower, and $a \in F$, there exists a basis which is normalised wrt α and reduced wrt F.*

PROOF. A procedure for normalising and reducing a basis is given in Karr (1981).

We can state the second major result of this paper.

RESULT. Given a $\prod\sum$-field F, σ with non-zero $a, f \in F$, let $t_1, \ldots, t_n$ be a basis for a $\prod\sum$-tower $F \subseteq \ldots \subseteq E$, where the basis is normalized wrt a and reduced wrt F. The equation $\sigma g - a \cdot g = f$ has a solution for $g \in E \Leftrightarrow$

$$\exists\, v \in F, c_i \in K \quad \text{with} \quad f = \sigma v - \alpha \cdot v + \sum_{i \in S} c_i \cdot \beta_i,$$

where

$$S = \{i \mid 0 \neq \beta_i \in F \text{ and } \alpha_i = a\}.$$

One direction of the equivalence is trivial. If f has the required form, a solution is

$$g = v + \sum_{i \in S} c_i \cdot t_i.$$

The interesting part is that solutions always have this form.

LEMMA 4.1. *Let $F(t), \sigma$ be a $\prod$-extension of F, σ. Suppose that $a, f \in F$ and that $\sigma g - a \cdot g = f$ has a non-zero solution in $F(t)$ but not in F. Then $f = 0$ and $a/\alpha^m \in H(F)$ for some $m \neq 0$.*

PROOF. By results in Karr (1981) we may conclude that if g exists, it is in $F[t, 1/t]$, i.e. $g = \sum_i v_i t^i$ where i ranges over $\mathbb{Z}$. Examine the constant term in $\sigma g - a \cdot g = f$, namely $\sigma v_0 - a \cdot v_0 = f$. If $f \neq 0$, then $v_0 \neq 0$, but then v_0 is a non-zero solution in F. Thus, $f = 0$. And if $v_0 \neq 0$, $v_m \neq 0$ for some $m \neq 0$, and by looking at the coefficient of t^m in $\sigma g - a \cdot g$, we see $a/\alpha^m \in H(F)$.

LEMMA 4.2. *Let $F(t)$, σ be a $\sum$-extension of F, σ with basis normalised wrt $a \in F$; let $f \in F$. If $\sigma g - a \cdot g = f$ has a solution in $F(t)$ but not in F, then $f \neq 0$, $a = \alpha$ and there exists $v \in F$, and non-zero $c \in K$ with $f = \sigma v - a \cdot v + c \cdot \beta$.*

PROOF. If $\sigma g - a \cdot g = 0$ with $g \in F(t)$ but $g \notin F$, then the extension is by definition homogeneous, contradicting the definition of a $\sum$-extension. Thus $f \neq 0$. By methods of Karr (1981), we can prove that if g exists, it is in $F[t]$, and further, that $\deg(g) \leqslant 1$. Thus we may write $g = v_1 \cdot t + v_0$ with $v_1 \neq 0$. Looking at the coefficient of t in the equation, we learn that $a/\alpha = \sigma v_1 / v_1 \in H$, whence $a = \alpha$ by the normalised property, and $v_1 \in K$ since $\sigma v_1 / v_1 = 1$. The c and v in the statement of the Lemma may be obtained by $c = v_1$ and $v = v_0$, and substituting these in the equation for the constant term of $\sigma g - a \cdot g = f$.

PROOF OF RESULT. There is nothing to prove if $n = 0$. Inductively assume t for $n-1$, and apply it to the tower $F_1 \subset \ldots = F_n$. This yields:

$$f = \sigma h - a \cdot h + \sum_{2 \leqslant i \leqslant n} c_i \cdot \beta_i \quad \text{with}$$

$$h \in F_1 \quad \text{and} \quad [c_i = 0 \text{ or } (0 \neq \beta_i \in F_1 \text{ and } \alpha_i = a)].$$

Suppose there is a j such that $c_j \neq 0$, $\alpha_i = a$, $0 \neq \beta, \in F_1$ but $\beta_j \in F$. Let j be maximal. Then

$$c_j \cdot \beta_j + \sigma h - a \cdot h + \sum_{2 \leqslant i < j} c_i \cdot \beta_i = f - \sum_{j < i \leqslant n} c_i \cdot \beta_i \in F$$

$$\Rightarrow \beta_j + \sigma h_0 - \alpha_j \cdot h_0 = 1/c_j \cdot \Big(f - \sum_{j < i \leqslant n} c\beta_i\Big) \in F,$$

$$\text{where } h_0 = 1/c_j \Big(h + \sum_{2 \leqslant i < j} c_i t_i\Big) \in F_{j-1}$$

$$\Rightarrow \beta_j \in F \qquad \text{(by the reduced property).}$$

This contradicts the assumption that $\beta_j \notin F$, so in fact, for all $c_i \neq 0$, we have $\beta_i \in F$. Thus, indexing may be restricted to $S - \{1\}$, and we have a solution (namely h) in F_1 for:

$$\sigma g - a \cdot g = f - \sum_{i \in S - \{1\}} c_i \cdot \beta_i \in F.$$

If this happens to have a solution $v \in F$, then letting $c_1 = 0$ if $1 \in S$ proves the result in this case. Otherwise, we have an inhomogeneous equation, solvable in F_1 but not in F. Lemma 1 says that F_1 is a $\sum$-extension of F, and Lemma 2 says that $\alpha_i = a$ and yields $v \in F$ and $c_1 \in K$ with

$$f - \sum_{i \in S - \{1\}} c_i \cdot \beta_i = \sigma v - a \cdot v + c_1 \beta_1.$$

Since $\beta_1 \in F$, $1 \in S$, completing the proof.

References

Cohn, R. M. (1965). *Difference Algebra.* New York: Interscience.
Karr, M. (1981). Summation in finite terms. *J. Assoc. Comp. Mach.* **28**, 305–350.
Rosenlicht, M. (1968). Liouville's theorem on functions with elementary integrals. *Pacific J. Math.* **24**, 153–161.