Available online at www.sciencedirect.com
SCIENCE DIRECT
J. Differential Equations 202 (2004) 256–283
Journal of Differential Equations
http://www.elsevier.com/locate/jde

Classification of integrable $\mathcal{B}$-equations

Peter H. van der Kamp*

Applied Mathematics Group, Institute of Mathematics, Statistics and Actuarial Science, University of Kent, Canterbury, Kent CT2 7NF, UK

Received March 10, 2003; revised October 23, 2003

Abstract

We classify integrable equations which have the form $u_t = a_1 u_n + K(v_0, v_1, \ldots),\ v_t = a_2 v_n$, where $a_1, a_2 \in \mathbb{C}$, $n \in \mathbb{N}$ and K a quadratic polynomial in derivatives of v. This is done using the symbolic calculus, biunit coordinates and the Lech–Mahler theorem. Furthermore we present a method, based on resultants, to determine whether an equation is in a hierarchy of lower order.

Keywords: Evolution equations; Integrability; Symmetries; Classification; Number theory; Symbolic calculus; Biunit coordinates; Lech–Mahler theorem; Diophantine equations

1. Introduction

Bakirov devoted article [1] to the description of local symmetries of the following evolution equations with parameter a:

$$\begin{cases} u_t = u_n + v^2, \\ v_t = a v_n \end{cases} \tag{1}$$

for $n \geqslant 2$. This class of equations is interesting since it contains both integrable and almost integrable equations. These notions have the following strict meaning: an equation is called (symmetry-)*integrable* if it possesses infinitely many generalized symmetries and *almost integrable of depth* (*at least*, *at most*) n if there are exactly (at

*Fax: +44-1227-827932.
E-mail address: p.van-der-kamp@kent.ac.uk.

0022-0396/$ - see front matter
doi:10.1016/j.jde.2004.04.001

least, at most) n generalized symmetries. This terminology somehow reflects the idea of the conjecture of Fokas [6] that an equation is integrable if its depth equals the number of components. For a more thorough discussion of these matters and counterexamples to the conjecture of Fokas we refer to [14].

Bakirov presented the first example of an equation that is almost integrable of depth at least 1: Eq. (1) with $n=4$ and $a=\frac{1}{5}$ possesses a symmetry at order 6. By means of computer algebra it was shown, that the equation does not possess other symmetries of order $n\leqslant 53$. However, for a long time it was not known whether for this example the depth is higher than 1.

Paper [3], which was also devoted to equations of type (1), changed this situation. In this article, the symbolic calculus of Gel'fand and Dikiĭ [7] was used. In [3], to our knowledge, both the Lech–Mahler theorem and p-adic analysis first appeared in the literature in connection with symmetries of evolution equations. It was proven, by using p-adic analysis, that the equation of Bakirov does not have generalized symmetries at any order but at order 6, i.e., it was shown beyond doubt that 'one symmetry does not imply integrability'. An efficient way to find more almost integrable evolution equations together with some improvements of the p-adic method can be found in [13].

In this article, we will concentrate on the classification of *integrable* equations. It it important to realize that this simplifies the problem. For example, the classification of scalar equations (with respect to almost integrability) [10] relied on diophantine approximation theory [2], however, the classification of integrable equations can be performed without these elaborate techniques, as was shown in [12].

Using the Lech–Mahler theorem [8] it was conjectured [3, Conjecture 2.3] there are only finitely many integrable equations of form (1). This conjecture became a theorem in [4, Theorem 2.1], where the following list was proven to be exhaustive:

$$\begin{cases} u_t = au_2 + v^2, \\ v_t = v_2, \end{cases} \quad \begin{cases} u_t = au_3 + v^2, \\ v_t = v_3, \end{cases} \quad \begin{cases} u_t = -3u_4 + v^2, \\ v_t = v_4, \end{cases}$$
$$\begin{cases} u_t = -u_4 + v^2, \\ v_t = v_4, \end{cases} \quad \begin{cases} u_t = u_5 + v^2, \\ v_t = v_5, \end{cases} \quad \begin{cases} u_t = -\frac{1}{4}u_5 + v^2, \\ v_t = v_5, \end{cases}$$
$$\begin{cases} u_t = \frac{-13\pm 5\sqrt{5}}{2}u_5 + v^2, \\ v_t = v_5, \end{cases} \quad \begin{cases} u_t = -u_7 + v^2, \\ v_t = v_7, \end{cases} \tag{2}$$

where $a\in\mathbb{C},\ a\neq 0$. A corollary [4, Corollary 2.1] says that each of the equations in (2) with arbitrary quadratic part (in derivatives of v) is integrable as well. Also it was remarked that the list is not necessarily complete in this more general class of equations that is the object of classification in this article.

Definition 1. A $\mathcal{B}$-equation, after Bakirov, is an equation of the form

$$\mathcal{B}_n[a_1,a_2](K)\colon \begin{cases} u_t = a_1u_n + K(v_0, v_1, \ldots), \\ v_t = a_2v_n, \end{cases} \tag{3}$$

where $a_1, a_2 \in \mathbb{C}$, $n \in \mathbb{N}$ and K a quadratic polynomial in derivatives of v. A symmetry of such an equation of the form

$$\begin{pmatrix} b_1 u_m + S(v, v_1, \ldots) \\ b_2 v_m \end{pmatrix},$$

where $b_1, b_2 \in \mathbb{C}$, $m \in \mathbb{N}$ and S a quadratic polynomial in derivatives of v, is called a $\mathcal{B}$-*symmetry*.

This class of equations has the following nice property: any symmetry of a $\mathcal{B}$-equation with nonequal and nonzero eigenvalues, is a linear combination of $\mathcal{B}$-symmetries; if the eigenvalues are equal and the order of the $\mathcal{B}$-equation is higher than 1, any symmetry is a linear combination of $\mathcal{B}$-symmetries and the linear symmetry $(v_m, 0)$. This almost follows from the nonlinear injectiveness of the linear part of $\mathcal{B}$-equations [12].

In this article, we will solve the classification and recognition problems for $\mathcal{B}$-equations. We prove the existence of a certain finite number of integrable $\mathcal{B}$-equations at every order. Special attention has been given to proving that the hierarchies of symmetries are exhaustive. Furthermore, we are able to decide whether a $\mathcal{B}$-equation is in the hierarchy of an other equation and we give formulas for the number of new integrable equations at arbitrary order. Also we prove that all integrable $\mathcal{B}$-equations are real, up to complex scalings.

Although $\mathcal{B}$-equations seem quite special, the implication for the general equation is immediate. First of all whenever an equation has a part that is a nonintegrable $\mathcal{B}$-equation, the equation is not integrable. Furthermore an equation might be related by an invertible transformation to a $\mathcal{B}$-equation. Also the techniques that are employed and developed for this classification of $\mathcal{B}$-equations play a role in other classification programs [11,12].

Integrability has been related to several other notions among which solvability and solitonic behaviour [15]. $\mathcal{B}$-equations are triangular and therefore solvable in a certain sense. The equation for v is a homogeneous linear evolution equation. Once this has been solved, the equation for u reduces to an inhomogeneous version of the same equation. From my point of view it is an intriguing challenge to understand the analytic meaning of symmetry-integrability.

2. The symbolic calculus

The symmetry condition is obtained by requiring the vanishing of the Lie bracket of $\mathcal{B}_n[a_1, a_2](K)$ and $\mathcal{B}_m[b_1, b_2](S)$. This Lie bracket is computed using Fréchet derivatives, see [9]. We solve the symmetry condition using the symbolic calculus as developed by Gel'fand and Dikiĭ [7]. The symbolic calculus enables us to treat infinitely many orders at once. Moreover, the necessary and sufficient equations for the rate of eigenvalues are obtained directly without having to specify the nonlinear part explicitly.

The Gel'fand–Dikiĭ transformation is a one-to-one mapping between differential expressions and polynomials. A quadratic differential monomial is transformed into a symmetric polynomial in two symbols as follows:

$$v_i v_j = \frac{\eta_1^i \eta_2^j + \eta_1^j \eta_2^i}{2}.$$

The expression is symmetrized and divided by the number of symbol-permutations in order to ensure that

$$v_i v_j = v_j v_i.$$

This procedure turns the operation of differentiation as well as the action of the Fréchet derivative on a linear term into ordinary multiplication. Thus the symmetry condition is equivalent to the following equation, cf. [13]:

$$G_n[a_1, a_2]S = G_m[b_1, b_2]K,$$

where $K, S \in \mathbb{C}[\eta_1, \eta_2]$ and the so-called G-functions are defined as follows:

$$G_n[a_1, a_2](\eta_1, \eta_2) = a_2(\eta_1 + \eta_2^n) - a_1(\eta_1 + \eta_2)^n.$$

If $G_m[b_1, b_2]K$ is divisible by $G_n[a_1, a_2]$ we have a symmetric polynomial expression for S which can be transformed back. An equation $\mathcal{B}_n[a_1, a_2](K)$ is trivially integrable if the function $G_n[a_1, a_2]$ divides K. This kind of equation has symmetries on every order and is in the hierarchy of some zeroth order equation. In the rest of this paper, we suppose that the *order of the* $\mathcal{B}$*-equation* n is positive and $G_n[a_1, a_2]$ does not divide K. Then $G_n[a_1, a_2]$ should have a common factor with $G_m[b_1, b_2]$ for there being a symmetry. Suppose we can find $a_1, a_2, b_1, b_2 \in \mathbb{C}$ such that

$$G_n[a_1, a_2] = FL, \quad G_m[b_1, b_2] = FT,$$

with $F, L, T \in \mathbb{C}[\eta_1, \eta_2]$. Then the Lie bracket of $\mathcal{B}_n[a_1, a_2](K)$ and $\mathcal{B}_m[b_1, b_2](S)$ vanishes if one takes $K = LM$ and $S = MT$. One is free to choose $M \in \mathbb{C}[\eta_1, \eta_2]$.

Thus the problem that needs to be solved for the classification of integrable $\mathcal{B}$-equations (3) can be stated as follows:

> Determine all divisors H of $G_n[a_1, a_2]$ such that there are infinitely many $m \in \mathbb{N}$ and $b_1, b_2 \in \mathbb{C}$ for which H divides $G_m[b_1, b_2]$.

We will perform the classification in full generality. All exceptional cases will explicitly be given and results will be illustrated with examples. We start at low order, so that the reader can become conversant with the symbolic calculus.

3. $\mathcal{B}$-equations of order 1, 2 or 3 and their symmetries

We prove that all $\mathcal{B}$-equations of order 1, 2 or 3 are integrable and we show how to efficiently calculate their symmetries.

Proposition 2. *All* 1*st order* $\mathcal{B}$*-equations are integrable.*

This proposition is easy to prove and an explicit formula for all the symmetries of $\mathcal{B}_1[a_1, a_2](a_3 v^2)$ can be given.

Proof of Proposition 2. To find all symmetries of $\mathcal{B}_1[a_1, a_2](K)$ we have to find for arbitrary m all (b_1, b_2) such that $\mathcal{G}_1[a_1, a_2]$ divides $\mathcal{G}_m[b_1, b_2]$. This can be done by substitution. Take $a_1 \neq a_2$. The $\mathcal{G}$-function

$$\mathcal{G}_1[a_1, a_2] = (a_2 - a_1)(\eta_1 + \eta_2)$$

has a common factor with $\mathcal{G}_m[b_1, b_2]$ if

$$b_2(\eta_1^m + (-\eta_1)^m) - b_1(\eta_1 - \eta_1)^m = 0.$$

The infinitely many solutions are $b_2 = 0$ or m is odd.

Exceptional case: Take $a_1 = a_2$. For any S the symmetry condition becomes

$$\mathcal{G}_m[b_1, b_2]K = 0.$$

Equality holds when $b_1 = b_2 = 0$. The symmetries (at any order) have arbitrary nonlinear part but no linear part. $\square$

Example 3. We explicitly write down the symmetries of

$$\begin{cases} u_t = a_1 u_1 + a_3 v^2, \\ v_t = a_2 v_1. \end{cases}$$

Its quadratic part is calculated as follows:

$$S = \frac{\mathcal{G}_m[b_1, b_2]}{\mathcal{G}_1[a_1, a_2]} K = \frac{a_3}{a_2 - a_1}\left(b_2 \frac{1}{\eta_1 + \eta_2}(\eta_1^m + \eta_2^m) - b_1(\eta_1 + \eta_2)^{m-1} \right).$$

By applying the inverse Gel'fand and Dikiĭ transformation, at even order m we obtain the symmetry

$$\begin{pmatrix} b_1 u_m + \dfrac{a_3 b_1}{a_1 - a_2} D_x^{m-1} v^2 \\ 0 \end{pmatrix}$$

and at odd order m we obtain the symmetry

$$\begin{pmatrix} b_1 u_m + \dfrac{a_3 b_1}{a_1 - a_2} D_x^{m-1} v^2 + \dfrac{a_3 b_2}{a_1 - a_2} D_x^{-1} v v_m \\ b_2 v_m \end{pmatrix}.$$

It is only here that we can describe the whole hierarchy in differential language. For higher-order $\mathcal{B}$-equations we have to do the computation of a particular symmetry symbolically and translate the result to obtain its differential expression.

Proposition 4. *All* 2*-nd order* $\mathcal{B}$*-equations are integrable.*

Proof. They have symmetries at all orders. The ratio of eigenvalues (and quadratic part) of the symmetries are fixed. Take $a_1 \neq a_2$ again and $a_2 \neq 0$, i.e., $r \neq 0, -1$. The $\mathcal{G}$-function

$$\mathcal{G}_2[a_1, a_2] = \frac{a_2 - a_1}{r}(\eta_1 - r\eta_2)(r\eta_1 - \eta_2) \quad \text{with} \quad r^2 + \frac{2a_1}{a_1 - a_2} r + 1 = 0$$

has a factor $(\eta_1 - r\eta_2)$ in common with $\mathcal{G}_m[b_1, b_2]$ when

$$\mathcal{G}_m[b_1, b_2]|_{\eta_1 = r\eta_2} = 0 \Rightarrow \frac{b_1}{b_2} = \frac{1 + r^m}{(1 + r)^m}.$$

For this ratio $(r\eta_1 - \eta_2)$ is a factor as well because the fraction

$$\frac{1 + r^m}{(1 + r)^m}$$

is invariant under $r \to 1/r$, i.e., the $\mathcal{G}$-function is symmetric in η_1, η_2.

Exceptional cases:

- When $a_1 = a_2$ the equation is integrable; we have $\mathcal{G}_2[a_1, a_1] = -2a_1\eta_1\eta_2$ divides $\mathcal{G}_m[b_1, b_2]$ for arbitrary $m > 2$ if $b_1 = b_2$.
- When $a_2 = 0$ the equation is integrable; we have $\mathcal{G}_2[a_1, 0] = -a_1(\eta_1 + \eta_2)^2$ divides $\mathcal{G}_m[b_1, b_2]$ for arbitrary $m > 2$ if $b_2 = 0$. □

We demonstrate the method by calculating a symmetry of some inhomogeneous 2nd-order equation.

Example 5. We calculate the 3rd order symmetry $\mathcal{B}_m[b_1, b_2](S)$ of

$$\begin{cases} u_t = a_1 u_2 + a_3 v^2 + a_4 v v_1 + a_5 v_1^2, \\ v_t = a_2 v_2. \end{cases}$$

The ratio of eigenvalues of the symmetry is

$$\frac{1+r^3}{(1+r)^3}=\frac{3a_1-a_2}{2a_2}.$$

We take $b_1=3a_1-a_2$ and $b_2=2a_2$. The $\mathcal{G}$-function of the symmetry is

$$\mathcal{G}_3[3a_1-a_2,2a_2]=3(\eta_1+\eta_2)\mathcal{G}_2[a_1,a_2].$$

The quadratic part S is obtained by multiplying

$$K=a_3+a_4\frac{\eta_1+\eta_2}{2}+a_5\eta_1\eta_2$$

with the ratio of $\mathcal{G}$-functions $3(\eta_1+\eta_2)$:

$$S=6a_3\frac{\eta_1+\eta_2}{2}+3a_4\left(\frac{\eta_1^2+\eta_2^2}{2}+\eta_1\eta_2\right)+6a_5\frac{\eta_1\eta_2^2+\eta_1^2\eta_2}{2}.$$

By applying the inverse Gel'fand and Dikiĭ transformation we obtain the 3rd order symmetry of the above equation

$$\begin{pmatrix}(3a_1-a_2)u_3+6a_3vv_1+3a_4(vv_2+v_1^2)+6a_5v_1v_2\\ 2a_2v_3\end{pmatrix}.$$

The procedure works for symmetries of any order.

Proposition 6. *All 3rd order $\mathcal{B}$-equations are integrable.*

Proof. All 3rd order equations have infinitely many symmetries but unlike the 2nd order equations not all of them have symmetries at even order. The reason is that $(\eta_1+\eta_2)$ is a divisor of $\mathcal{G}_m[b_1,b_2]$ only when m is odd or when $b_2=0$. Therefore, unless the 3rd order equation is in a lower hierarchy, its first symmetry appears at order 5. Take $a_2\neq 0,\ a_2-a_1$ again. The 3rd order $\mathcal{G}$-function factorizes like

$$\mathcal{G}_3[a_1,a_2]=\frac{a_1-a_2}{r}(\eta_1+\eta_2)(\eta_1-r\eta_2)(r\eta_1-\eta_2),$$

with

$$r^2+\frac{2a_1+a_2}{a_1-a_2}r+1=0.$$

This can be used to calculate all higher-order $\mathcal{G}$-functions in the same way we did for 2nd-order equations.

Exceptional cases:

- When $a_1=a_2$ the equation is integrable, $\mathcal{G}_2[a_1,a_1]=-3a_1\eta_1\eta_2(\eta_1+\eta_2)$ divides $\mathcal{G}_m[b_1,b_2]$ for arbitrary odd $m>3$ if $b_1=b_2$.

- When $a_2 = 0$ the equation is integrable, $\mathcal{G}_2[a_1, 0] = -a_1(\eta_1 + \eta_2)^3$ divides $\mathcal{G}_m[b_1, b_2]$ for arbitrary $m > 3$ if $b_2 = 0$. □

We have now proven that all $\mathcal{B}$-equations of order smaller than 4 are integrable.

4. $\mathcal{B}$-equations in a hierarchy of order 1, 2 or 3

In this section, we turn from the classification problem to the recognition problem. Using resultants we present an efficient way to determine whether a $\mathcal{B}$-equation is in a hierarchy of order 1, 2 or 3.

Theorem 7. *$\mathcal{B}_m[b_1, b_2](S)$ is in a hierarchy of order n, where n is 1, 2 or 3, if the degree of the greatest common divisor of $\mathcal{G}_m[b_1, b_2]$ and S equals $m - n$.*

Proof. Since every symmetric factor of degree n, where n is 1, 2 or 3, is a multiple of $\mathcal{G}_n[a_1, a_2]$ for some (calculable) a_1, a_2, the quadratic part can be written

$$S = \frac{\mathcal{G}_m[b_1, b_2]}{\mathcal{G}_n[a_1, a_2]} K$$

such that $\gcd(K, \mathcal{G}_n[a_1, a_2]) = 1$. □

The use of resultants is very effective here, as we will show in the following two examples. Recall that if the greatest common divisor of two polynomials has positive degree, then their resultant vanishes.

Example 8. The equation

$$\begin{cases} u_t = b_1 u_3 + b_3 v_2 v + b_4 v_1^2, \\ u_t = b_2 v_3 \end{cases}$$

can be in a hierarchy of order 1 or 2. The η_1-resultant of $\mathcal{G}_3[b_1, b_2]$ and S is:

$$\frac{\eta_2^6}{4}(b_3 - b_4)(2b_3 b_1 + b_3 b_2 - 2b_4 b_1 + 2b_4 b_2)^2.$$

There are two special cases.

- When $b_3 = b_4$ the quadratic part is

$$S = \frac{b_3}{2}(\eta_1 + \eta_2)^2.$$

The greatest common divisor of S and $\mathcal{G}_3[b_1, b_2]$ has degree 1, so the order of the hierarchy is 2. The ratio of eigenvalues can be calculated using the above factorising of the $\mathcal{G}_3$-function and the map

$$r \to \frac{1+r^2}{(1+r)^2}.$$

The equation commutes with

$$\begin{cases} u_t = (2b_1 + b_2)u_2 + 2b_3 v v_1, \\ v_t = 3b_2 v_2. \end{cases}$$

- When $b_3 = 2(b_1 - b_2)a_1,\ b_4 = (2b_1 + b_2)a_1$ the equation is in the hierarchy of

$$\begin{cases} u_t = b_1 u_1 + a_1(b_1 - b_2)v^2, \\ v_t = b_2 v_1. \end{cases}$$

All other cases are not in an other hierarchy.

The method works for any order in principle. However, it depends on the order and the number of parameters in the equation whether we can actually solve the resultant, cf. [12].

5. Integrable $\mathcal{B}$-equations of order higher than 3 and their symmetries

As we are now interested in equations that are not in a 1st, 2nd or 3rd order hierarchy, we need to consider common factors of $\mathcal{G}$-functions of degree at least 4, cf. the proof of Theorem 7. The case where $a_2 = 0$ is easy; the equation is integrable since $\mathcal{G}_n[a_1, 0] = a_1(\eta_1 + \eta_2)^n$ divides $\mathcal{G}_m[b_1, b_2]$ for arbitrary $m > n$ if $b_2 = 0$. In the following we assume $a_2 \neq 0$.

Lemma 9. *The function* $\mathcal{G}_n[1 + r^n, (1+r)^n](\eta_1, \eta_2)$ *has a factor of the form*

$$(\eta_1 - r\eta_2)(r\eta_1 - \eta_2)(\eta_1 - s\eta_2)(s\eta_1 - \eta_2), \quad s \neq r, r^{-1},$$

whenever

$$\begin{aligned} U_n(r,s) &= \mathcal{G}_n[1 + r^n, (1+r)^n](s, 1) \\ &= (1+r)^n + (s(1+r))^n - (1+s)^n - (r(1+s))^n = 0. \end{aligned}$$

Proof. The condition $U_n(r,s) = 0$ expresses the fact that the ratio of eigenvalues of the $\mathcal{G}$-function containing zero r equals the ratio of eigenvalues of the $\mathcal{G}$-function containing zero s

$$\frac{a_1}{a_2} = \frac{(1+r)^n}{1+r^n} = \frac{(1+s)^n}{1+s^n}. \qquad \square$$

Using the Lech–Mahler theorem, see Theorem 19, it was proven in [3] that the only factors of $\mathcal{G}$-functions (with nonzero eigenvalue) which appear on infinitely many orders have zeros forming a subset of a set of the form

$$\left\{0, -1, r, \frac{1}{r}, \bar{r}, \frac{1}{\bar{r}}\right\}. \tag{4}$$

Therefore, to find all hierarchies of $\mathcal{B}$-equations is to find all points r such that $U_m(r, \bar{r}) = 0$ for infinitely many integers m; the zeros $0, -1$ can be treated separately. At fixed order Lemma 10, which improves the method given in [4], can be used

Lemma 10. *The following method can be used to find all integrable $\mathcal{B}$-equations at fixed order n. Substitute*

$$r = \frac{x(1-y)}{y-x}, \quad \bar{r} = \frac{1-y}{y-x}$$

in $U_n(r, \bar{r}) = 0$ and apply an algorithm of Smyth, cf. [5], to solve the equation in roots of unity x, y.

Proof. By Corollary 21, of the Lech–Mahler theorem, one of the pairs

$$x = \frac{r}{\bar{r}}, \quad y = \frac{1+r}{1+\bar{r}}$$

or $r\bar{r}, \frac{1+r}{1+\bar{r}}$ are roots of unity. By the invariancy of $U_n(r, \bar{r})$ under $r \to 1/r$ we may choose the first pair. Thus the method gives all points r such that $U_m(r, \bar{r}) = 0$ for infinitely many m, including $m = n$. $\square$

In [4] the algorithm of Smyth was used to obtain the eigenvalues of all 4th- and 5th-order $\mathcal{B}$-equations in the list 2. Lemma 10 makes it possible to treat higher orders. By means of computer algebra, we raised the order up to 23. We did observe quite some structure in the minimal polynomials of all the points we calculated. However, a clear picture did not arose until we plotted the points in the complex plane. We have included the plot for order 23, cf. Fig. 1. Note that the upper half unit disc may be taken as a fundamental domain.

The inspection of the patterns formed by the values r obtained in this way, can be described as a form of experimental mathematics. At every fixed order n the calculated points formed a similar pattern, which inspired to use biunit coordinates $\mathfrak{P}(\psi, \phi)$, cf. Definition 17 and Eq. (6). Since roots of unity play a special role in the

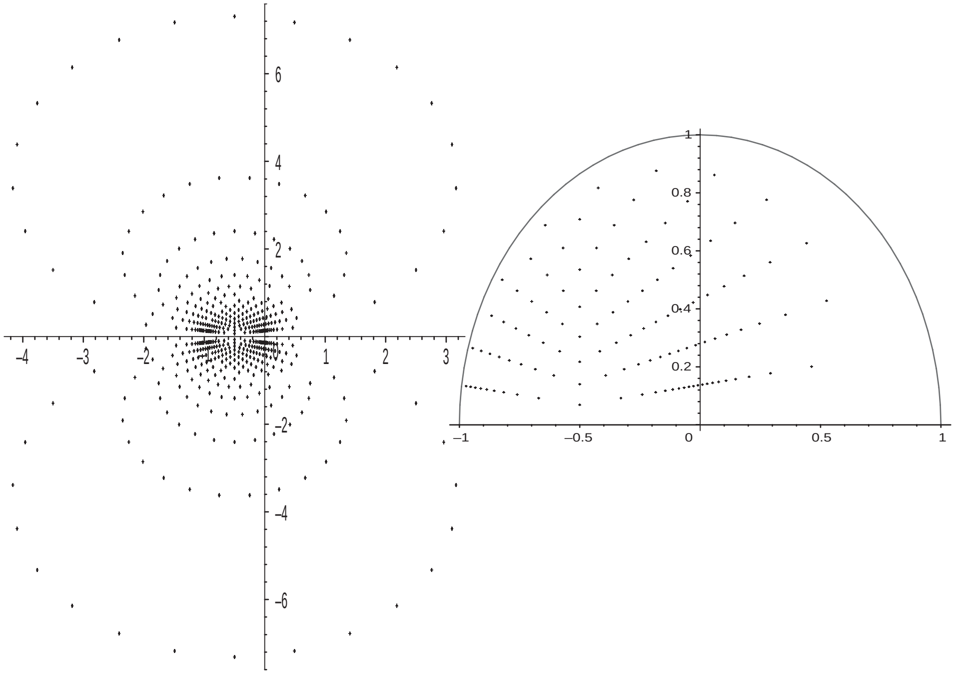

Fig. 1. The special zeros of $\mathcal{G}$-functions of integrable equations with order 23, in the complex plane and inside the upper half unit disc, form a nice pattern.

analysis of integrable equations and the points ± 1 often are exceptional cases, we will denote the set of all nth roots of unity ζ where $\zeta \neq \pm 1$ by Φ_n.

The following theorem asserts the existence of a certain finite set of integrable equations at any order $n > 3$. These correspond to the zeros r of $\mathcal{G}_n$ such that $U_m(r, \bar{r}) = 0$ for infinitely many m, including $m = n$. There are basically two kinds of zeros, those on the unit circle and those of the unit circle.

Theorem 11. *Let $n > 3$. To any point r in one of the sets*

(1) $r \in \mathfrak{P}(\Phi_{2n}, \Phi_{2n})$ *such that* $|r| \neq 1$,
(2) $r \in \Phi_{n-1}$,
(3) $r \in \Phi_{2n}$ *such that* $r^n = -1$

corresponds an integrable nth order $\mathcal{B}$-equation, which is not in a hierarchy of order smaller than 4.

Proof.

(1) For $r \in \mathfrak{P}(\Phi_{2n}, \Phi_{2n})$ the proof consists of showing that $U_m(r, \bar{r})$ has infinitely many solutions m including $m = n$. By substitution of

$$r = a\psi = b\phi - 1,$$

with $\psi, \phi \in \Phi_{2n}$, in $U_m(r, \bar{r})$ we get

$$U_m(\psi, \phi) = (b\bar{\phi})^m + (ab\psi\bar{\phi})^m - (b\phi)^m - (ab\bar{\psi}\phi)^m.$$

This vanishes when $m \equiv 0 \bmod n$. Note that when n is odd and $\eta_1 + \eta_2$ does not divide the quadratic part of the equation, no symmetries appear at even order. When r is real or on the unit circle the set $\{r, 1/r, \bar{r}, 1/\bar{r}\}$ does not contain 4 elements.

(2) The $(n-1)$th roots of unity are all double zeros of $\mathcal{G}_n$. They appear in conjugated pairs and are double zeros at order $m \equiv 1 \bmod n-1$ as well, cf. [3, Lemma 3.1]. A real zero and its conjugate do not form a pair.

(3) All odd powers of a primitive $(2n)$th root of unity are mapped to zero for all $m \equiv n \bmod 2n$. □

The following theorem asserts that there are no 'new' integrable $\mathcal{B}$-equations, i.e., equations that do not commute with an integrable $\mathcal{B}$-equation known by now.

Theorem 12. *Any integrable $\mathcal{B}$-symmetry is a symmetry of*

- *a $\mathcal{B}$-equation described in Theorem* 11, *or*
- *a* 1*st*, 2*nd or* 3*rd order $\mathcal{B}$-equation, or*
- *a* 5*th or* 7*th order $\mathcal{B}$-equation with equal eigenvalues.*

Proof. Suppose the eigenvalues are nonzero. Let H be a divisor of infinitely many $\mathcal{G}_m$. Any set of zeros Z of H is a subset of a set of form (4). If $0 \in Z$, the eigenvalues of the equation are equal. This problem was solved for the classification of scalar equations. It follows from [12, Theorem 5.8] or [10, Proposition 4.1] that the equation is a symmetry of a $\mathcal{B}$-equation of order 2,3,5 or 7. If

$$Z \subset \left\{-1, r, \frac{1}{r}\right\}$$

and the multiplicity of r is 1, the equation is a symmetry of a $\mathcal{B}$-equation of order 1, 2 or 3, cf. Theorem 7. If

$$Z \subset \left\{-1, r, \frac{1}{r}\right\}$$

and the multiplicity of r is 2, r is a root of unity. If

$$Z \subset \left\{-1, r, \frac{1}{r}, \bar{r}, \frac{1}{\bar{r}}\right\}$$

the biunit coordinates of r are roots of unity because otherwise none of the pairs

$$\frac{r}{\bar{r}}, \frac{1+r}{1+\bar{r}} \quad \text{or} \quad r\bar{r}, \frac{1+r}{1+\frac{1}{\bar{r}}}$$

are roots of unity. □

The following theorem asserts that any integrable $\mathcal{B}$-equation described in Theorem 11 has no other $\mathcal{B}$-symmetries than the symmetries proven to exist.

Theorem 13. *If the integrable $\mathcal{B}$-equation*

$$\begin{cases} u_t = (1+r^n)u_n + K, \\ v_t = (1+r)^n v_n \end{cases}$$

is not in a lower hierarchy it has no $\mathcal{B}$-symmetries other than the symmetries on order m, with:

(1) $m \equiv 0 \bmod n$ *if* $r \in \mathfrak{P}(\Phi_{2n}, \Phi_{2n})$, *and* $2|n$ *or* $2 \nmid n,\ \eta_1 + \eta_2 | K$,
(2) $m \equiv n \bmod 2n$ *if* $r \in \mathfrak{P}(\Phi_{2n}, \Phi_{2n})$, *and* $2 \nmid n,\ \eta_1 + \eta_2 \nmid K$,
(3) $m \equiv 1 \bmod n-1$ *if* $r \in \Phi_{n-1}$,
(4) $m \equiv n \bmod 2n$ *if* $r \in \Phi_{2n}$.

Proof. From the proof of Theorem 11, we know that symmetries exist at these orders. We now prove that the equations do not have any other symmetries.

(1) We write $U_m(r, \bar{r})$ in terms of ψ and ϕ using Eqs. (A.1) and (A.2). Furthermore, we perform the transformations

$$\psi^2 \to \mu v, \quad \phi^2 \to v.$$

Thus, we obtain the Diophantine equation

$$\left(\frac{1-\mu}{1-v}\right)^m = \frac{1-\mu^m}{1-v^m} \tag{5}$$

for roots of unity μ, v. By Theorem 22, under the conditions

$$\mu, v \neq \pm 1, \quad \mu \neq v, \bar{v}, \quad \mu^m, v^m \neq 1.$$

Eq. (5) has no solution unless $m = 1$. We check the conditions. When $\mu = -1$ we find that $\phi = \pm i\psi$, we have

$$|r + \tfrac{1}{2}| = \tfrac{1}{2}.$$

In this case Eq. (5) reduces to

$$v^m = 1 \quad \text{when } m \text{ even},$$

$$(1-v)^m = 2^{m-1}(1-v^m) \quad \text{when } m \text{ odd},$$

with $v \neq \pm 1$ a root of unity. The same equation, in μ instead of v is obtained when $v = -1$, i.e., when $\phi = \pm i$ or

$$r + \bar{r} = -2.$$

By Proposition 24 the equation for odd order has no solutions $m > 1$. For the even solutions, note that we are in the case where n is even. The equation is not in a lower hierarchy if ψ is a primitive $(2n)$th root of unity. This implies that v is a primitive nth root of unity and the even solutions are given by $m \equiv 0 \bmod n$.

(2) When n is odd and $\eta_1 + \eta_2$ does not divide K there is no symmetry at any odd order since $\eta_1 + \eta_2$ does not divide $\mathcal{G}_{2m+1}$.
(3) When $m \not\equiv 1 \bmod n-1$ the point $r \in \Phi_{n-1}$ is not a double zero of $\mathcal{G}_m$.
(4) Two $(2n)$th roots of unity $r = \psi,\ s = \phi$ are both zeros of $\mathcal{G}_m$ if $U_m(\psi, \phi) = 0$. By applying the transformation

$$\psi \to -\mu, \quad \phi \to -v$$

we obtain

$$\left(\frac{1-\mu}{1-v}\right)^m = \frac{1+(-\mu)^m}{1+(-v)^m}$$

for $(2n)$th roots of unity μ, v. Suppose that

$$\mu, v \neq -1, \quad \mu \neq v, \bar{v}.$$

Then, by Theorem 22, the equation has no odd solutions $m > 1$ such that $\mu^m, v^m \neq 1$. For even m we use Theorem 25, which states that

$$\left(\frac{1-\mu}{1-v}\right)^m = \frac{1+\mu^m}{1+v^m}$$

has no solutions $m > 1$ such that $\mu^m, v^m \neq -1$. □

5.1. *Quadratic part of the integrable $\mathcal{B}$-equations*

We describe the quadratic part of the integrable $\mathcal{B}$-equations and we show that the equations are real (up to a complex scaling).

If $a_1 = 0$ then K can be anything because the $\mathcal{G}$-function of the equation divides the $\mathcal{G}$-functions of all the symmetries. Take $a_1 \neq 0$. Let Q be the greatest common divisor of

$$\mathcal{G}_n[1+r^n,(1+r)^n]$$

and

$$\eta_1\eta_2(\eta_1+\eta_2)(\eta_1-r\eta_2)(r\eta_1-\eta_2)(\eta_1-\bar{r}\eta_2)(\bar{r}\eta_1-\eta_2).$$

Q is the common factor of all $\mathcal{G}$-functions of the symmetries. The quadratic part of the equation can be written as

$$K=\frac{\mathcal{G}_n}{Q}P,$$

with P an arbitrary symmetric polynomial that does not have Q as a divisor.

Although in the analysis complex roots of unity play an important role, in the end the equations turn out to be real.

Proposition 14. *All integrable $\mathcal{B}$-equations with nonzero eigenvalues are real, up to a complex scaling.*

Proof. Since

$$\frac{a_1}{a_2}=\frac{1+r^n}{(1+r)^n}=\frac{1+\bar{r}^n}{(1+\bar{r})^n}=\frac{\bar{a}_1}{\bar{a}_2}$$

all ratios of eigenvalues of integrable $\mathcal{B}$-equations are real valued. What about the quadratic part? We have

$$\begin{aligned}(\eta_1-r\eta_2)&(r\eta_1-\eta_2)(\eta_1-\bar{r}\eta_2)(\bar{r}\eta_1-\eta_2)\\&=r\bar{r}(\eta_1^4+\eta_2^4)+(r\bar{r}+1)(r+\bar{r})\eta_1\eta_2(\eta_1^2+\eta_2^2).\end{aligned}$$

Hence Q is real. Therefore, the quadratic part is real if the eigenvalues and P are chosen to be real. □

We demonstrate our method by calculating an integrable equation together with its first higher-order symmetry.

Example 15. Take $n=6$. The line

$$\mathbb{R}e^{\frac{1}{3}\pi i}-1$$

intersects the imaginary axis in the point

$$r=\sqrt{3}i.$$

This is a zero of the $\mathcal{G}$-function $\mathcal{G}_6[-13, 32]$, since

$$\frac{1+r^6}{(1+r)^6} = -\frac{13}{32}.$$

The polynomial dividing all $\mathcal{G}$-functions of the symmetries is

$$Q = (3\eta_1^2 + \eta_2^2)(\eta_1^2 + 3\eta_1^2).$$

The quadratic part of the equation is, with $P = \frac{1}{2}$,

$$K = \frac{\mathcal{G}_6[-13, 32]}{2Q} = \frac{15}{2}(\eta_1^2 + \eta_2^2) + 13\eta_1\eta_2.$$

Therefore the equation

$$\begin{cases} u_t = -13u_6 + 15vv_2 + 13v_1^2, \\ v_t = 32v_6 \end{cases}$$

is integrable. Let us calculate the symmetry $\mathcal{B}_{12}[b_1, b_2](S)$. To obtain the eigenvalues we compute

$$\frac{b_1}{b_2} = \frac{1+r^{12}}{(1+r)^{12}} = \frac{365}{2048}.$$

The symbolic quadratic part is given by

$$S = \frac{\mathcal{G}_{12}[365, 2048]}{\mathcal{G}_6[-13, 32]} K.$$

By applying the inverse Gel'fand and Dikiĭ transformation we obtain the symmetry at order 12:

$$\begin{pmatrix} 365u_{12} + 561vv_8 - 1460v_1v_7 - 9900v_2v_6 - 21\,900v_3v_5 - 13\,893v_4^2 \\ 2048v_{12} \end{pmatrix}.$$

6. $\mathcal{B}$-equations in a lower hierarchy

We describe all $\mathcal{B}$-equations that belong to a lower hierarchy. This solves the recognition problem. Let K be the quadratic part of an integrable $\mathcal{B}$-equation. Let k be the degree of

$$Q = \frac{\mathcal{G}_n}{\gcd(\mathcal{G}_n, K)}.$$

If the equation is nondegenerate we have $0<k<8$. If k<4 or k=7 the equation is in a kth order hierarchy. It never happens that $k=6$ because whenever $\mathcal{G}_6$ has zeros 0 and r it does not have $\bar{r}$ as zero. The remaining cases are enumerated as in Theorem 11.

(1) Let $r \neq -1$ be a zero of the polynomial Q. It has biunit coordinates (ζ^a, ζ^b) where ζ is a primitive $(2n)$th root of unity. The equation is in a hierarchy of order d, with d (>3) a divisor of n, if a/n and b/n are integer multiples of $1/d$.
(2) The equation is in a hierarchy of order $d+1$, with $d(>2)$ a divisor of $n-1$, if the double zero r is a dth root of unity.
(3) When $n = lm$ with l odd and $m>3$ the equation can be in a mth order hierarchy. This is the case if $\mathcal{G}_n/\mathcal{G}_m$ divides K.

7. The number of integrable $\mathcal{B}$-equations

We present formulas for the number of nth order integrable equations and for the number of nth order integrable equations that are not in a lower-order hierarchy of order higher than 3.

(1) The number of points $r \in \mathfrak{P}(\Phi_{2n}, \Phi_{2n})$ leading to different eigenvalues of integrable equations is

$$f(n) = \begin{cases} \dfrac{(n-2)^2}{4} & \text{if } n \text{ is even}, \\ \dfrac{(n-1)(n-3)}{4} & \text{if } n \text{ is odd}. \end{cases}$$

We count the number of points in the upper half plane (because conjugation leaves the set invariant) excluding the points on the unit circle where $\bar{r} = r^{-1}$. Put $\zeta = e^{\frac{1}{n}\pi i}$. The imaginary part of $\mathfrak{P}(\zeta^a, \zeta^b)$ is positive only when $0<b<a$. There are exactly

$$\sum_{a=1}^{n-2} a$$

such points. A point is on the unit circle when the angle of the line through 0 is twice the angle of the line through -1. The set Φ_{n-1} contains

$$\left\lfloor \frac{n-1}{2} \right\rfloor$$

points on the upper half unit circle. Subtracting these two numbers and dividing by 2 (because inversion leaves the set invariant) gives the desired number. If $g(n)$

is the number of these integrable equations not in the hierarchy of an other equation we have

$$f(n) = \sum_{d|n} g(d)$$

and by Möbius' inversion

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right),$$

with the Möbius function defined as follows: (p_i are prime)

$$\mu\left(\prod_{i=1}^{j} p_i^{\alpha_i}\right) = \begin{cases} 1 & \text{if } \alpha_i = 0 \text{ for all } i, \\ 0 & \text{if } \alpha_i > 1 \text{ for some } i, \\ (-1)^j & \text{if } \alpha_i = 1 \text{ for all } i. \end{cases}$$

(2) The number of complex $(n-1)$th roots of unity giving different eigenvalues at fixed n is

$$f(n) = \begin{cases} \dfrac{n-2}{2} & \text{if } n \text{ is even}, \\ \dfrac{n-3}{2} & \text{if } n \text{ is odd}. \end{cases}$$

We counted the zeros that are above the real line. If $g(n)$ is the number of these integrable equations not in the hierarchy of an other we have

$$f(n) = \sum_{d|n-1} g(d+1)$$

and by Möbius' inversion

$$g(n) = \sum_{d|n-1} \mu(d) f\left(\frac{n-1}{d} + 1\right).$$

(3) This case is concerned with vanishing first eigenvalue. When n is prime, twice a prime or a power of 2 , the equation is not in a lower hierarchy.

At order 5 there is the extra equation with eigenvalue 1. Its $\mathcal{G}$-function has the set of zeros $\{0, -1, \zeta_3, \zeta_3^2\}$. Adding this all together we have the following.

Proposition 16. *Let* $3 < n \in \mathbb{N}$. *There are exactly*

$$\frac{n(n-2)}{4} \quad \textit{when } n \textit{ even},$$

Table 1
Numbers of integrable equations

n	4	5	6	7	8	9	10	11	12	13
#	3	5	7	8	12	15	18	23	26	33
n	14	15	16	17	18	19	20	21	22	23
#	37	44	45	61	57	76	74	89	87	116

$$\frac{(n+1)(n-3)}{4} \quad \textit{when } n \textit{ odd}, \ n \neq 5$$
$$\frac{(n-1)^2}{4} \quad \textit{when } n = 5$$

nondegenerate nth order integrable $\mathcal{B}$-equations.

Finally, the number of nth order integrable equations that are not in a lower hierarchy with $3 < n < 24$ is given in Table 1.

Acknowledgments

I thank Frits Beukers for proving the theorems in Appendix C and Jan Sanders and Jing Ping Wang for useful discussions.

Appendix A. Biunit coordinates

We introduce an uncommon way to describe complex numbers which will be especially convenient when describing the solutions to $\mathcal{G}$-functions that correspond to the integrable equations.

The most familiar way to describe a point r in the complex plane is probably

$$r = \Re(r) + \Im(r)i,$$

where $\Re(r) \in \mathbb{R}$ is the real part of r, $\Im(r) \in \mathbb{R}$ is the imaginary part of r and $i^2 = -1$. A second way to describe $r \in \mathbb{C}$ is

$$r = |r|e^{\arg(r)i},$$

where $|r| > 0$ is the absolute value of r and $0 \leqslant \arg(r) < 2\pi$ the argument of r. Yet, we would like to give a third description.

Definition 17. We call (ψ, ϕ), where $|\psi| = |\phi| = 1$, $\psi, \phi \neq \pm 1$, *biunit coordinates* of the point $r \in \mathbb{C} \backslash \mathbb{R}$, which is the intersection of the lines $\psi\mathbb{R}$ and $\phi\mathbb{R} - 1$, cf. Fig. 2.

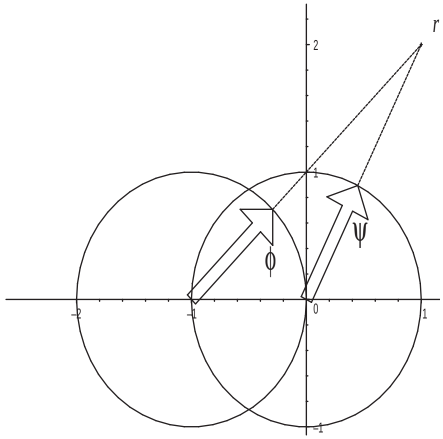

Fig. 2. The point r in biunit coordinates (ψ, ϕ).

Lemma 18. *If* (ψ, ϕ) *are biunit coordinates of* r, *then we have*

$$r = \mathfrak{P}(\psi, \phi) = \psi^2 \frac{(\phi + 1)(\phi - 1)}{(\psi + \phi)(\psi - \phi)}. \tag{A.1}$$

Proof. We solve the system of linear equations in $|r|$ and $|r + 1|$

$$|r| \sin(\arg(r)) = |r + 1| \sin(\arg(r + 1)),$$

$$|r + 1| \cos(\arg(r + 1)) = |r| \cos(\arg(r)) + 1.$$

This gives

$$|r| = \frac{\sin(\arg(r + 1))}{\cos(\arg(r + 1)) \sin(\arg(r)) - \sin(\arg(r + 1)) \cos(\arg(r))}.$$

Using the identities

$$\sin(\arg(r)) = \frac{\psi - \psi^{-1}}{2i}, \quad \cos(\arg(r)) = \frac{\psi + \psi^{-1}}{2},$$

$$\sin(\arg(r + 1)) = \frac{\phi - \phi^{-1}}{2i}, \quad \cos(\arg(r + 1)) = \frac{\phi + \phi^{-1}}{2},$$

we express $|r|$ in terms of ψ, ϕ. Multiplying $|r|(\psi, \phi)$ by ψ gives expression (A.1). $\square$

From Definition 17 and from expression (A.1) it is clear that if (ψ, ϕ) are biunit coordinates of r, then $(-\psi, \phi)$ and $(\psi, -\phi)$ are biunit coordinates of r as well. Note that we have $\psi \neq \pm\phi$, i.e., there is no point $r \in \mathbb{C}$ with biunit coordinates $(\psi, \pm\psi)$.

The set of points

$$\{\mathfrak{P}(a,b) | a \in A, b \in B\}$$

is denoted with $\mathfrak{P}(A,B)$.

Conjugation is a simple operation in biunit coordinates. If the biunit coordinates of r are given by (ψ, ϕ) we have (ψ^{-1}, ϕ^{-1}) as biunit coordinates of $\bar{r}$, i.e.,

$$\bar{r} = \mathfrak{P}(\psi^{-1}, \phi^{-1}) = \frac{(\psi+1)(\phi-1)}{(\psi-\phi)(\psi+\phi)}, \tag{A.2}$$

since $\bar{\psi} = \psi^{-1}$ whenever $|\psi| = 1$.

Appendix B. Corollaries of the Lech–Mahler theorem

The following theorem is formulated and proven in [8].

Theorem 19 (Lech–Mahler). *Let $a_1, a_2, \dots, a_n, A_1, A_2, \dots, A_n$ be nonzero complex numbers. Suppose that none of the ratios A_i/A_j with $i \neq j$ is a root of unity. Then the equation*

$$a_1 A_1^k + a_2 A_2^k + \cdots + a_n A_n^k = 0$$

in the unknown integer k has finitely many solutions.

Using this theorem the following corollaries can be proven, cf. [3,12].

Corollary 20. *Let a, b, c, d, A, B, C, D be nonzero complex numbers. Suppose that the equation*

$$aA^k + bB^k + cC^k + dD^k = 0$$

has infinitely many integers k as solution. Then at least one of the pairs $A/B, C/D$ or $A/C, B/D$ or $A/D, B/C$ consists of roots of unity.

Corollary 21. *Let a, b, c, d, A, B, C, D be nonzero complex numbers. Suppose that $aA^k + bB^k \neq 0$ for all k and that the equation*

$$aA^k + bB^k + cC^k + dD^k = 0$$

has infinitely many integers k as solution. Then at least one of the pairs $A/C, B/D$ or $A/D, B/C$ consists of roots of unity.

Appendix C. Diophantine equations

The material presented here is adapted from work done by Beukers.

Theorem 22 (Beukers). *Let μ, v be roots of unity. Suppose that $\mu, v \neq \pm 1$, $\mu^n, v^n \neq 1$ and $\mu \neq v, v^{-1}$. Then the Diophantine equation*

$$\left(\frac{1-\mu}{1-v}\right)^n = \frac{1-\mu^n}{1-v^n} \tag{C.1}$$

in the unknown positive integer n has no solution unless $n = 1$.

Proof. The case $n = 2$ is excluded with the following argument. Suppose

$$\left(\frac{1-\mu}{1-v}\right)^2 = \frac{1-\mu^2}{1-v^2}.$$

Then

$$\frac{1-\mu}{1-v} = \frac{1+\mu}{1+v}.$$

Hence

$$1 + v - \mu - \mu v = 1 - v + \mu - \mu v.$$

So, $\mu = v$, a contradiction.

When $n > 2$ we use Lemma 23. Choose m, a, b positive integers such that

$$\mu = \zeta_m^a, \quad v = \zeta_m^b,$$

where $\zeta_m = e^{2\pi i/m}$ and $\gcd(a, b, m) = 1$. We distinguish two cases.

(1) $\gcd(a, m) = 1$ or $\gcd(b, m) = 1$. Suppose the first case happens. Let a^* be the inverse of a modulo m. Then we see that

$$v = \mu^{a^* b}.$$

We apply Lemma 23 with $l \equiv a^* b \pmod{m}$ and conclude that $l = \pm 1$. In other words, $a \equiv \pm b \pmod{m}$ and we see that $\mu = v$ or $\mu = v^{-1}$.

(2) $\gcd(a, m) > 1$ and $\gcd(b, m) > 1$. In this case the idea is to choose an integer l with $\gcd(l, m) = 1$ such that

$$v^l = v, \quad \mu^l \neq 1, \quad \mu, \mu^{-1}.$$

Now replace μ, v in the original equation by $\mu^l, v^l = v$. Divide the newly obtained equation by the old one and we obtain an equation of form (C.2). Now apply Lemma 23 to conclude that $\mu^l = 1$, μ or μ^{-1}. Thus we get a contradiction, i.e., the original equation has no solution once we have found a suitable l.

Now let us choose l. Since $\gcd(a,b,m)=1$, we can assume that not both $\gcd(a,m)$ and $\gcd(b,m)$ are even. Hence there is an odd prime p which divides one of them, say $\gcd(b,m)$. Because p is odd we can choose an integer

$$l = 1 + \frac{km}{p},$$

with $k = \pm 2$ and $\gcd(l,m)=1$. Clearly, we have $\nu^l = \nu$. Moreover,

$$\mu^l = \zeta_m^{a+akm/p} = \mu\zeta_m^{akm/p} = \mu e^{\pm 4\pi i a/p}.$$

Since a is not divisible by p we see that μ^l/μ is a nontrivial pth root of unity. Therefore $\mu^l \neq \mu$. Suppose that $\mu^l = \mu^{-1}$. This implies that

$$\mu e^{\pm 4\pi i a/p} = \mu^{-1},$$

i.e., μ is a pth root of unity. So if μ is not a pth root of unity, l is found.

Now assume that μ is a pth root of unity. So p divides m exactly once. Suppose that ν is an Nth root of unity. Since p divides b we get that N is not divisible by p. In particular, $\gcd(p,N)=1$. Suppose that $p>3$. Then we choose, using the Chinese remainder theorem, the number l such that

$$l \equiv 1 \bmod N, \quad l \equiv 2 \bmod p.$$

Note that $\nu^l = l$ and $\mu^l = \mu^2$ which is different from μ, μ^{-1} since $p>3$. We are left with the case $p=3$. Now suppose that $N \neq 3,4,6$. Then there is an integer c, relatively prime with N such that $c \not\equiv \pm 1 \bmod N$. Choose l such that $l \equiv 1 \bmod 3$ and $l \equiv c \bmod N$. Then

$$\mu^l = \mu, \quad \nu^l = \nu^c \neq \nu, \nu^{-1}.$$

We apply our argument with ν and μ interchanged to conclude that we get a contradiction once more. Since $N = 3,6$ are not possible because 3 does not divide N, we are left with the case $p=3,\ N=4$. Hence, we can assume that $\mu = \omega$, with ω a primitive 3rd root of unity, and $\nu = i$. Taking absolute values squared on both sides of

$$\left(\frac{1-\omega}{1-i}\right)^n = \frac{1-\omega^n}{1-i^n}$$

yields

$$\left(\frac{3}{2}\right)^n = \frac{3}{2^\varepsilon},$$

where $\varepsilon = 1$ or 2 depending on whether n is odd or even. This is clearly impossible when $n>1$. $\square$

Lemma 23 (Beukers). *Let μ be a root of unity and l an integer. Suppose that $\mu \neq \pm 1$ and that for some $n > 2$ we have*

$$\left(\frac{1-\mu^l}{1-\mu}\right)^n = \frac{1-\mu^{ln}}{1-\mu^n}. \tag{C.2}$$

Then μ^l is either $1, \mu$ or μ^{-1}.

Proof. Suppose that μ is a primitive mth root of unity for some $m \geqslant 3$. By Galois theory Eq. (C.2) still holds if we replace μ by μ^h for any integer h with $\gcd(h, m) = 1$. So we can assume that

$$\mu = e^{2\pi i/m}.$$

We can also assume that $|l| \leqslant m/2$ by shifting l over multiples of m if necessary. For any $x \in [-\pi, \pi]$ we have the straightforward inequalities

$$\frac{2}{\pi}|x| \leqslant |1 - e^{ix}| \leqslant |x|.$$

From this it follows that:

$$\left|\frac{1-\mu^l}{1-\mu}\right| \geqslant \frac{(2/\pi)(2\pi|l|/m)}{2\pi/m} = \frac{2|l|}{\pi}.$$

On the other hand,

$$\left|\frac{1-\mu^{ln}}{1-\mu^n}\right| = |1 + \mu^n + \mu^{2n} + \cdots + \mu^{(|l|-1)n}| \leqslant |l|.$$

Hence, we find that

$$\left(\frac{2|l|}{\pi}\right)^n \leqslant |l|.$$

From this it follows that

$$(2|l|/\pi)^{n-1} \leqslant \pi/2.$$

Using $n > 2$ we get

$$|l| \leqslant (\pi/2)^{1.5} < 2.$$

Hence $|l| \leqslant 1$ and we have $\mu^l = 1, \mu$ or μ^{-1}, as asserted. $\square$

Proposition 24. *Let μ be a root of unity. Suppose that $\mu \neq \pm 1$. Then the diophantine equation*

$$(1-\mu)^n = 2^{n-1}(1-\mu^n)$$

in the unknown positive integer n has no solution unless $n = 1$.

Proof. Division by $1-\mu$ gives

$$(1-\mu)^{n-1} = 2^{n-1}(1+\mu+\cdots+\mu^{n-1}).$$

Therefore

$$\frac{1-\mu}{2}$$

should be an algebraic integer, i.e., in $\mathbb{Z}[\mu]$, which is clearly not the case. □

Theorem 25 (Beukers). *Let μ, v be roots of unity. Suppose that*

$$\mu, v \neq \pm 1, \quad \mu^n, v^n \neq -1, \quad \mu \neq v, v^{-1}, \; n > 1.$$

Then the Diophantine equation

$$\left(\frac{1-\mu}{1-v}\right)^n = \frac{1 \pm \mu^n}{1+v^n}$$

in the unknown positive integer n has no solutions.

Proof. The proof is similar to the proof of Theorem 22. The only differences are

- The case $n=2$ is excluded with the following argument. Suppose

$$\left(\frac{1-\mu}{1-v}\right)^2 = \frac{1+\mu^2}{1+v^2}.$$

  Then

$$(1-\mu)^2(1+v^2)-(1-v)^2(1+\mu^2) = 2(\mu-v)(\mu v-1) = 0.$$

  So, $\mu = v$ or $\mu = 1/v$, a contradiction. Suppose

$$\left(\frac{1-\mu}{1-v}\right)^2 = \frac{1-\mu^2}{1+v^2}.$$

  Then

$$(1-\mu)^2(1+v^2)-(1-v)^2(1-\mu^2) = 2(\mu-1)(\mu(v^2-v+1)-v) = 0.$$

  Since $\mu \neq 1$ we have

$$\mu = v/(v^2-v+1).$$

Substituting this into $\mu\bar{\mu} = 1$ and using that $\bar{v} = 1/v$ we obtain that $v^2 = -1$ or $v = 1$, contradicting the assumptions.

- In the case $\gcd(a, m) = 1$ or $\gcd(b, m) = 1$ we use Lemma 26 instead of Lemma 23 to conclude that $\mu^l \in \{\mu, 1, \mu^{-1}\}$.
- The absolute value squared of $(1 + \omega^n)/(1 + i^n)$ yields

$$\begin{aligned} &\tfrac{1}{4} \text{ when } n \equiv 4, 8 \bmod 12,\\ &\tfrac{1}{2} \text{ when } n \equiv 1, 5, 7, 11 \bmod 12,\\ &1 \text{ when } n \equiv 0 \bmod 12,\\ &2 \text{ when } n \equiv 3 \bmod 6. \end{aligned}$$

The absolute value squared of $(1 - \omega^n)/(1 + i^n)$ yields

$$\begin{aligned} &\tfrac{3}{4} \text{ when } n \equiv 4, 8 \bmod 12,\\ &\tfrac{3}{2} \text{ when } n \equiv 1, 5, 7, 11 \bmod 12,\\ &0 \text{ when } n \equiv 0, 3, 9 \bmod 12. \qquad \square \end{aligned}$$

Lemma 26. *Let $\mu \neq \pm 1$ be a root of unity and l an integer. Suppose that for some $n \geqslant 2$ we have*

$$\left(\frac{1 - \mu^l}{1 - \mu}\right)^n = \frac{1 + \alpha\mu^{ln}}{1 + \mu^n}, \quad \alpha = \pm 1, \mu^n \neq -1. \tag{C.3}$$

Then, if $\alpha = 1$ we have $\mu^l = \mu$ or $\mu^l = \mu^{-1}$ and if $\alpha = -1$ we have $\mu^l = 1$.

Proof. Suppose that μ is a primitive mth root of unity for some $m \geqslant 3$. By Galois theory Eq. (C.3) still holds if we replace μ by μ^h for any integer h with $\gcd(h, m) = 1$. So we can assume that $\mu = e^{2\pi i/m}$. We can also assume that $|l| \leqslant m/2$ by shifting l over multiples of m if necessary.

We have the estimate

$$\left(\frac{2|l|}{\pi}\right)^n \leqslant \left|\frac{1 - \mu^l}{1 - \mu}\right|^n.$$

On the other hand, we can give an upper bound for right-hand side by using the bound $|1 \pm \mu^{ln}| \leqslant 2$ to obtain

$$\left(\frac{2|l|}{\pi}\right)^n \leqslant \frac{2}{|1 + \mu^n|}$$

and hence

$$\left|\cos\left(\pi\frac{n}{m}\right)\right| \leqslant \left(\frac{\pi}{2|l|}\right)^n.$$

Then, using the estimate

$$|\cos \pi x| \geqslant |2x - k|,$$

where k is the nearest odd integer to $2x$, and $|l| \geqslant 2$ we get

$$\left|\frac{n}{m} - \frac{k}{2}\right| \leqslant \frac{1}{2}\left(\frac{\pi}{4}\right)^n.$$

From these estimates it follows that $n/m \geqslant 0.19$. Using this and the lower bound $|n/m - k/2| \geqslant 1/(2m)$ we get

$$\frac{1}{m} \leqslant \left(\frac{\pi}{4}\right)^{0.19m}.$$

Hence $m \leqslant 100$. But then,

$$\frac{1}{100} \leqslant \frac{1}{m} \leqslant \left(\frac{\pi}{2|l|}\right)^n,$$

which in its turn implies that

$$\left(\frac{2|l|}{\pi}\right)^n \leqslant 100.$$

So we are left with a finite number of triples l, m, n. A small computer search yields no solutions with $\alpha = \pm 1,\ 2 \leqslant |l| \leqslant m/2$. When $\alpha = 1$ there are the solutions $l = \pm 1$ and hence $\mu^l = \mu$ or μ^{-1}. When $\alpha = 0$ we have $\mu^l = 1$. $\square$

References

[1] I.M. Bakirov, On the symmetries of some system of evolution equations, Technical Report, Akad. Nauk SSSR Ural. Otdel. Bashkir. Nauchn. Tsentr, Ufa, 1991.

[2] F. Beukers, On a sequence of polynomials, J. Pure Appl. Algebra 117/118 (1997) 97–103; Algorithms for algebra (Eindhoven, 1996).

[3] F. Beukers, J.A. Sanders, J.P. Wang, One symmetry does not imply integrability, J. Differential Equations 146 (1) (1998) 251–260.

[4] F. Beukers, J.A. Sanders, J.P. Wang, On integrability of systems of evolution equations, J. Differential Equations 172 (2) (2001) 396–408.

[5] F. Beukers, C.J. Smyth, Cyclotomic points on curves, in: A.K.Peters (Ed.), Millennial Conference on Number Theory, Urbana-Champaign, May 21–26, 2000, 2001.

[6] A.S. Fokas, Symmetries and integrability, Stud. Appl. Math. 77 (1987) 253–299.
[7] I.M. Gel'fand, L.A. Dikiĭ, Asymptotic properties of the resolvent of Sturm–Liouville equations, and the algebra of Korteweg–de Vries equations, Uspehi Mat. Nauk 30(5(185)) (1975) 67–100 (English translation: Russ. Math. Surv. 30 (5) (1975) 77–113).
[8] C. Lech, A note on recurring sequences, Arkiv. Mat. 2 (1953) 417–421.
[9] P.J. Olver, Applications of Lie Groups to Differential Equations, Graduate Texts in Mathematics, 2nd Edition, Vol. 107, Springer, New York, 1993.
[10] J.A. Sanders, J.P. Wang, On the integrability of homogeneous scalar evolution equations, J. Differential Equations 147 (2) (1998) 410–434.
[11] J.A. Sanders, J.P. Wang, On the integrability of systems of second order evolution equations with two components, Technical Report WS-557, Vrije Universiteit Amsterdam, Amsterdam, 2001, accepted for publication, Journal of Differential Equations.
[12] P.H. van der Kamp, Symmetries of evolution equations: A diophantine approach, Ph.D. Thesis, Vrije Universiteit, Amsterdam, 2002.
[13] P.H. van der Kamp, J.A. Sanders, On testing integrability, J. Nonlinear Math. Phys. 8 (4) (2001) 561–574.
[14] P.H. van der Kamp, J.A. Sanders, Almost integrable evolution equations, Selecta Math. (N.S.) 8 (4) (2002) 705–719.
[15] V.E. Zakharov (Ed.), What is Integrability? Springer, Berlin, 1991.