One Symmetry Does Not Imply Integrability

Frits Beukers
Department of Mathematics
University of Utrecht

Jan Sanders
Jing Ping Wang
Department of Mathematics & Computer Science
Vrije Universiteit, Amsterdam

April 28, 1998

Abstract

We show that that Bakirov's counterexample (which had been checked by computeralgebra methods to order 53) to the conjecture that one nontrivial symmetry of an evolution equation implies infinitely many is indeed a counterexample. To prove this we use the *symbolic method* of Gel'fand-Dikii and *p-adic analysis*. We also formulate a conjecture to the effect that almost all equations in the family considered by Bakirov have at most finitely many symmetries. This conjecture depends on the solution of a diophantine problem, which we explicitly state.

1 Introduction

It has, on the basis quite a lot of material, been conjectured that evolution equations in one space variable (like the Korteweg-de Vries equation) were integrable, i.e. in the possession of infinitely many symmetries once one nontrivial symmetry existed. Only one example put this conjecture in doubt. It was found by Bakirov[Bak91] (see also [Olv93], p. 381, exercise 5.15 and [Bil94]) that the system

$$\left.\begin{array}{rcl} u_t & = & u_4 + v^2 \\ v_t & = & \frac{1}{5} v_4 \end{array}\right\} \tag{1}$$

has one symmetry of order 6, but no others where found up till order 53. In this paper we intend to prove that indeed no other symmetries exist and therefore the conjecture is false. We have not found a counterexample to the conjecture in [Fok87] that the system of dimension n needs n symmetries to be integrable.
In this proposition some conditions play a role which have been inspired by the use of the symbolic method, introduced by Gel'fand-Dikii [GD75]. This method was used in [TQ81] to show (as an example) that the symmetries of the Sawada-Kotera equation have to be of order 1 or 5 (mod 6). In [SW97] this method has been extended to completely classify the symmetries of λ-homogeneous scalar equations with $\lambda > 0$ and of the form

$$u_t = u_k + f(u, \cdots, u_{k-1}).$$

The analysis depends on results from diophantine approximation theory [Beu97].

The basic idea (of the symbolic method) is very old, probably dating from the time when the position of index and power were not as fixed as they are today. In fact, the symbolic calculus of classical invariant theory relies on it. The idea is simply to replace u_i, where i is an index, in our case counting the number of derivatives, by $\xi^i u$, where ξ is now a symbol. We see that the basic operation of differentation, i.e. replacing u_i by u_{i+1}, is now replaced by multiplication with ξ, as is the case in Fourier transformation theory. If one has multiple u's, as in $u_i u_j$, one replaces this by $\frac{1}{2}\left(\xi_1^i \xi_2^j + \xi_1^j \xi_2^i\right) u^2$. We have averaged over the permutation group Σ_2 to retain complete equality among the symbols, reflecting the fact that $u_i u_j = u_j u_i$. Differentiation now becomes multiplication with $\xi_1 + \xi_2$.
With this method one can readily translate solvability questions into divisibility questions, which in the case of the class of equations considered in [Bak91], take the following form.
We shall work with the polynomials $f_{a,m}$ defined by $f_{a,m}(X) = a(X+1)^m - X^m - 1$, where a is non-zero complex number. The question we deal with is the following.

Question 1.1 *Given a, m, for which $b \in \mathbf{C}$ and $n \in \mathbf{N}$ does $f_{a,m}$ divide $f_{b,n}$?*

In the next section we explain how this question arises from the original question about the existence of symmetries of an evolution equation.

2 The symbolic method

In the symbolic method one replaces derivatives u_k, v_k by powers $x^k u, y^k v$ (Usually one replaces u_k by x^k, but this leads to confusion in nonhomogeneous problemes and in the more variable case, since distinction between u and v disappears). When there are more u_k-s or v_ks involved we add more symbols, one for every u_k or v_k. These will be denoted by x_i, y_i. E.g. v_2^2 becomes $\frac{1}{2}\left(y_1^2 + y_2^2\right) v^2$. For the one-variable case, all definitions and proofs can be found in [SW97]. The generalization to the more variable case is straightforward. Since the specific equation we will be working on is very simple, we just write out the method for this case without giving the general theory. Consider the system (1) and rewrite it as $(u_4 + v^2)\frac{\partial}{\partial u} + \frac{1}{5} v_4 \frac{\partial}{\partial v}$. Its symbolic form is

$$\left(x_1^4 u + v^2\right) \frac{\partial}{\partial u} + \frac{1}{5} y_1^4 v \frac{\partial}{\partial v}$$

In order to compute the symmetries of our equation (1) we need the commutator of the linear part of the equation with an arbitrary homogeneous vectorfield (where $x[m]$ stands for $x_1, \cdots, x_m$):

$$\begin{aligned}
&[x_1^4 u \frac{\partial}{\partial u} + \frac{1}{5} y_1^4 v \frac{\partial}{\partial v}, A(x[m], y[l]) u^m v^l \frac{\partial}{\partial u} + B(x[n], y[k]) u^n v^k \frac{\partial}{\partial v}] = \\
= &\left((\sum_{i=1}^m x_i + \sum_{i=1}^l y_i)^4 - \sum_{i=1}^m x_i^4 - \frac{1}{5} \sum_{i=1}^l y_i^4 \right) A(x[m], y[l]) u^m v^l \frac{\partial}{\partial u} \\
+ &\left(\frac{1}{5} (\sum_{i=1}^n x_i + \sum_{i=1}^k y_i)^4 - \sum_{i=1}^n x_i^4 - \frac{1}{5} \sum_{i=1}^k y_i^4 \right) B(x[n], y[k]) u^n v^k \frac{\partial}{\partial v}
\end{aligned} \tag{2}$$

Putting this expression equal to zero, to find the lowest order term of our symmetry, we find that either $A = 0$ or $m = 1$ and $l = 0$; also $B = 0$ or $n = 0$ and $k = 1$. So the zeroth order term will be of the form

$$a x_1^p u \frac{\partial}{\partial u} + b y_1^q v \frac{\partial}{\partial v}$$

Or, if we go back to our old notation,

$$\left.\begin{aligned} u_t &= a u_p \\ v_t &= b v_q \end{aligned}\right\} \tag{3}$$

We look for symmetries of a given order, so we may as well take $q = p$ without loss of generality. Now computing the commutator of this zeroth order part of the (potential) symmetry with the first order (quadratic) part of our equations, we obtain

$$\begin{aligned} & [ax_1^p u\frac{\partial}{\partial u} + by_1^p v\frac{\partial}{\partial v}, \frac{1}{2}(y_1^0 + y_2^0)v^2\frac{\partial}{\partial u}] = \\ = \quad & (a(y_1+y_2)^p - b(y_1^p + y_2^p))\, v^2\frac{\partial}{\partial u} \end{aligned} \tag{4}$$

Defining $f_{\lambda,p}(\xi,\eta) = \lambda(\xi+\eta)^p - (\xi^p + \eta^p)$, we can now construct the quadratic terms of the symmetry as follows. We compute

$$[(x_1^4 u + v^2)\frac{\partial}{\partial u} + \frac{1}{5}y_1^4 v\frac{\partial}{\partial v}, (ax_1^p u + Av^2)\frac{\partial}{\partial u} + by_1^p v\frac{\partial}{\partial v}] = (\frac{1}{5}Af_{5,4} - bf_{\frac{a}{b},p})v^2\frac{\partial}{\partial u}.$$

Let

$$\hat{A} = 5bf_{\frac{a}{b},q}/f_{5,4}$$

If $\hat{A}$ is polynomial in y_1, y_2, then $(ax_1^p u + \hat{A}v^2)\frac{\partial}{\partial u} + by_1^p v\frac{\partial}{\partial v}$ is a symmetry of system (1). Whether $\hat{A}$ is indeed polynomial is answered by the following results.
We will prove in section 3 the following theorem.

Theorem 2.1 *Let $a \in \mathbf{C}$, $m \in \mathbf{Z}_{\geq 2}$ and consider*

$$f_{a,m}(X) = a(X+1)^m - X^m - 1.$$

Suppose that there are infinitely many pairs $b \in \mathbf{C}$, $n \in \mathbf{N}$ such that $f_{a,m}$ divides $f_{b,n}$. Then we are in one of the following cases,

$m = 2$. Then $n \in \mathbf{N}_{\geq 2}$ arbitrary and $b = (\alpha^n + 1)/(\alpha+1)^n$, where α is a zero of $f_{a,2}$.

$m = 3$. Then $n \in \mathbf{N}_{\geq 3}$ odd and $b = (\alpha^n + 1)/(\alpha+1)^n$, where α is a zero $\neq -1$ of $f_{a,3}$.

$m = 4$ and $a = -1$. Then $n \equiv 1 (\mathrm{mod}\ 3)$ and $b = (-1)^{n-1}$

$m = 4$ and $a = -3$. Then 4 divides n and $b = 1 + (1+i)^n$.

$m = 5$ and $a = -1/4$. Then $n \equiv 1 (\mathrm{mod}\ 4)$ and $b = (1+i)^{1-n}$.

$m = 5$ and $a = -4 + 10\cos(2\pi/5), -4 + 10\cos(4\pi/5)$. Then 5 divides n and $b = (a+1)^{n/5} + (-1)^{n/5}$.

For particular given a, m it is often possible to compute the complete set of b, n explicitly. This will be proved for the example $a = 5, m = 4$ in section 4. Note that this is precisely Bakirov's example.

Theorem 2.2 *Suppose $f_{5,4}$ divides $f_{b,n}$. then (b, n) equals $(5, 4)$ or $(11, 6)$.*

In this case $\hat{A} = \frac{25}{22}y_2^2 + \frac{20}{11}y_1 y_2 + \frac{25}{22}y_1^2$.
We now translate these results back to results on symmetries of evolution equations.

Corollary 2.3 *The system*

$$\left.\begin{array}{rcl} u_t &=& u_4 + v^2 \\ v_t &=& \frac{1}{5}v_4 \end{array}\right\} \tag{5}$$

has one and only one nontrivial symmetry:

$$\left(u_6 + \frac{5}{11}(5vv_2 + 4v_1^2)\right)\frac{\partial}{\partial u} + \frac{1}{11}v_6\frac{\partial}{\partial v} \tag{6}$$

Corollary 2.4 *The system*

$$\left.\begin{array}{rcl} u_t &=& u_m + v^2 \\ v_t &=& \frac{1}{a}v_m \end{array}\right\} \tag{7}$$

has a finite number of symmetries for all but a finite number of values (a, m).

3 The Lech-Mahler theorem

In this section we prove Theorem 2.1.
In our considerations it is important to realise that $f_{a,m}$ has double zeros for some values of a.

Lemma 3.1 *Suppose that $f_{a,m}$ has a multiple zero. Then this is given by an $m-1^{\rm st}$ root of unity ζ and $a = 1/(\zeta+1)^{m-1}$. Together with $1/\zeta$ these are the only multiple zeros and they have multiplicity two.*

Proof. We solve the simultaneous equations $f_{a,m}(x) = f'_{a,m}(x) = 0$ in x. Explicitly, $a(x+1)^m = x^m + 1$ and $a(x+1)^{m-1} = x^{m-1}$. Multiply the second by $x+1$ and subtract the equations. We obtain $0 = 1 - x^{m-1}$. Hence x is an $m-1^{\rm st}$ root of unity and from the second equation we get $a = 1/(1+x)^{m-1}$. Since $f''_{a,m}(X) = m(m-1)(a(X+1)^{m-2} - X^{m-2})$ we see that $f''_{a,m}(x) = m(m+1)(1/(x+1) - 1/x) \neq 0$. Hence x is a double zero. Suppose we have a second $m-1^{\rm st}$ root of unity y such that $a(1+y)^{m-1} = 1$. In particular we find that $|1+y| = |1+x|$ and $|x| = |y|$. This implies that either $x = y$ or $x = \overline{y} = 1/y$. This proves our Lemma. $\diamond$

For the proof of Theorem 2.1 shall use the following theorem from number theory [Lec53].

Theorem 3.2 (Lech, Mahler) *Let $A_1, A_2, \ldots, A_n \in \mathbf{C}$ be non-zero complex numbers and similarly for $a_1, a_2, \ldots, a_n$. 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.

For us the following corollary is important

Corollary 3.3 *Let $A, B, C, D \in \mathbf{C}$ be non-zero complex numbers. Suppose that the equation*

$$A^k + B^k = C^k + D^k$$

has infinitely many integers k with $A^k + B^k \neq 0$ as solution. Then at least one of the pairs $A/C, B/D$ or $A/D, B/C$ consists of roots of unity.

Proof. According to Theorem 3.2 at least one of the ratios $A/B, A/C, A/D, B/C, B/D, C/D$ must be a root of unity. Without loss of generality we can assume A/B a root of unity or A/C a root of unity.
Suppose that A/C is an $n^{\rm th}$ root of unity. Then, if we replace k by $a + kn$ for $a = 0, 1, 2, \ldots, n-1$ our problem falls into a finite number of problems of the form

$$(A^a - C^a)(A^n)^k + B^a(B^n)^k = D^a(D^n)^k$$

At least one of them has infinitely many solutions. Hence, according to Theorem 3.2, at least one of $A/B, A/D, B/D$ is a root of unity. In the latter case we are done. Suppose, without loss of generality that A/B is an $m^{\rm th}$ root of unity. As before, our problem can now be split into a finite number of problems of the form $\alpha(A^{mn})^k = \beta(D^{mn})^k$ with $\beta \neq 0$. At least one of them has infinitely many solutions. Hence A/D is a root of unity. Together with A/B being a root of unity this implies that B/D is a root of unity, as asserted.
Suppose now that A/B is an $n^{\rm th}$ root of unity. Our problem can be split into a finite number of problems of the form

$$(A^a + B^a)(A^n)^k = C^a(C^n)^k + D^a(D^n)^k$$

with $A^a + B^a \neq 0$. At least one equation has infinitely many solutions, hence at least one of $A/C, A/D, C/D$ is a root of unity. The first case is treated above. The second case, after interchanging C and D comes down to A/C being a root of unity. Let us now assume C/D is an $m^{\rm th}$ root of unity. We get a finite number of equations of the form $\alpha(A^{mn})^k = \beta(C^{mn})^k$ with $\beta \neq 0$. Again by Theorem 3.2 A/C is a root of unity. Hence we are done. $\diamond$

Proof of Theorem 2.1. The case $m = 2$. The zeros of $f_{a,2}$ read $\alpha, 1/\alpha$ and it is clear that $f_{a,2}$ divides $f_{b,n}$ if and only if $f_{b,n}(\alpha) = 0$. The latter equality is equivalent to $b = (\alpha^n + 1)/(\alpha + 1)^n$.
The case $m = 3$. The zeros of $f_{a,3}$ read $-1, \alpha, 1/\alpha$ and it is clear that $f_{a,2}$ divides $f_{b,n}$ if and only if $f_{b,n}(-1) = 0$ and $f_{b,n}(\alpha) = 0$. The latter equalities are equivalent to n being odd and $b = (\alpha^n + 1)/(\alpha + 1)^n$.
The case $m \geq 4$. Let α, β be distinct zeros of $f_{a,m}$. Note that $f_{a,m}(\alpha) = f_{a,m}(\beta) = 0$ imply $a = (\alpha^m + 1)/(\alpha + 1)^m = (\beta^m + 1)/(\beta + 1)^m$. Hence

$$\left(\frac{1}{1+1/\alpha}\right)^m + \left(\frac{1}{1+\alpha}\right)^m = \left(\frac{1}{1+1/\beta}\right)^m + \left(\frac{1}{1+\beta}\right)^m.$$

Suppose that $f_{a,m}$ divides $f_{b,n}$ for some b, n. Then we also have

$$\left(\frac{1}{1+1/\alpha}\right)^n + \left(\frac{1}{1+\alpha}\right)^n = \left(\frac{1}{1+1/\beta}\right)^n + \left(\frac{1}{1+\beta}\right)^n.$$

In the theorem it is assumed that there are infinitely many such n. Hence, according to Corollary 3.3, the ratios $(1+1/\alpha)/(1+1/\beta), (1+\alpha)/(1+\beta)$ or the ratios $(1+1/\alpha)/(1+\beta), (1+\alpha)/(1+1/\beta)$ are roots of unity. According to Lemma 3.4 we can choose α, β in such a way that this does not happen, unless (a, m) is in one of the exceptional cases listed above.
So it remains to consider these cases. $\diamond$

Lemma 3.4 *Let $a \in \mathbf{C}$, $m \in \mathbf{N}$ and $f_{a,m} = a(X+1)^m - X^m - 1$. Suppose $m \geq 4$ and*

$$(a, m) \neq (-1, 4), (-3, 4), (-1/4, 5), (-4 + 10\cos(2\pi/5), 5), (-4 + 10\cos(4\pi/5), 5)$$

Then $f_{a,m}$ has two zeros $\alpha, \beta \neq 0, -1$ such that none of the pairs $\alpha/\beta, (1+\alpha)/(1+\beta)$ or $\alpha\beta, (1+\alpha)/(1+1/\beta)$ consists of roots of unity.

Proof. Let α, β be two zeros of $f_{a,m}$ not equal to $0, -1$. Suppose that $\alpha/\beta, (1+\alpha)/(1+\beta)$ are roots of unity. Then we have $|\alpha| = |\beta|$ and $|1+\alpha| = |1+\beta|$. Hence β lies on the intersection of the circles $|z| = |\alpha|$ and $|z+1| = |1+\alpha|$ which implies $\beta = \alpha$ or $\beta = \overline{\alpha}$. Similarly if $\alpha\beta$ and $(1+\alpha)/(1+1/\beta)$ are roots of unity then $\beta = 1/\alpha$ or $\beta = 1/\overline{\alpha}$. As a consequence the statement of the Lemma is proved for any $f_{a,m}$ whose zeros are not a subset of a set of the form $V_\alpha = \{-1, \alpha, 1/\alpha, \overline{\alpha}, 1/\overline{\alpha}\}$.
Suppose now that there exists an α such that the zeros of $f_{a,m}$ form a subset of V_α. If $f_{a,m}$ has multiple zeros then, according to Lemma 3.1, the multiple zero is an $(m-1)^{\text{st}}$ root of unity which we may assume to be equal to α. Together with $1/\alpha$ these are the only multiple zeros and they have multiplicity two. Whether $f_{a,m}$ has multiple zeros or not it is clear that if $m \geq 6$ then $f_{a,m}$ has a zero not in V_α and the Lemma is true.
Suppose $m = 4$. In the case of double zeros we have $\alpha = 1, \omega$ or ω^2, where $\omega = e^{2\pi i/3}$. Note that $\alpha = 1$ implies $a = 1/8$ and $f_{1/8,4} = -(X-1)^2(7X^2 + 10X + 7)/8$. We verify by hand that our Lemma is true for this polynomial. Note that $\alpha = \omega, \omega^2$ implies $a = -1$, which case is excluded by our assumptions. Now suppose $f_{a,4}$ has only simple zeros. Then $f_{a,4}$ has, up to a constant factor, the shape

$$(X - \alpha)(X - 1/\alpha)(X - \overline{\alpha})(X - 1/\overline{\alpha}).$$

We also have

$$\frac{f_{a,4}}{a-1} = X^4 + \frac{4a}{a-1}X^3 + \frac{6a}{a-1}X^2 + \frac{4a}{a-1}X + 1$$

Hence comparison of the coefficients yields $3(b + \overline{b}) + 2(2 + b\overline{b}) = 0$ where $b = \alpha + 1/\alpha$. Note that this implies $|b + 3/2| = 1/2$, hence $|\alpha + 1/\alpha + 3/2| = 1/2$. Let us take $\beta = \overline{\alpha}$. If $\alpha\beta = |\alpha|^2$ were a root of unity, this would be 1. Hence $|\alpha| = 1$ and together with $\alpha + 1/\alpha + 1/2| = 3/2$ this yields $\alpha = 1$. We have dealt with this case above. So $\alpha\beta$ is not a root of unity. According to Lemma 3.5 the condition $|\alpha + 1/\alpha + 3/2| = 1/2$ entails that $x = \alpha/\overline{\alpha}$ and $y = (1+\alpha)/(1+\overline{\alpha})$ cannot be both

roots of unity unless $\alpha = 1, \omega, \omega^2, -1 \pm i$ or $(-1 \pm i)/2$. We already excluded $1, \omega, \omega^2$. The cases $\alpha = -1 \pm i$ and $(-1 \pm i)/2$ yield $a = -3$ which we excluded from our assumptions
Suppose $m = 5$. In the case of double zeros we have $\alpha = 1, \pm i$. Note that $\alpha = 1$ implies $a = 1/16$ and $f_{1/16,5} = -5(X+1)(X-1)^2(3X^2+2X+3)/16$. The Lemma is true for this polynomial. Note that $\alpha \pm i$ implies $a = -1/4$, which case is excluded by our assumptions. Now suppose $f_{a,5}$ has only simple zeros. Then $f_{a,5}$ has, up to a constant factor, the shape

$$(X+1)(X-\alpha)(X-1/\alpha)(X-\overline{\alpha})(X-1/\overline{\alpha})$$

. We also have

$$\frac{f_{a,5}}{(a-1)(X+1)} = X^4 + \frac{4a+1}{a-1}X^3 + \frac{6a-1}{a-1}X^2 + \frac{4a+1}{a-1}X + 1$$

Hence comparison of the coefficients yields $(b+\overline{b}) + (2+b\overline{b}) = 2$ where $b = \alpha + 1/\alpha$. Note that this implies $|b+1| = 1$ hence $|\alpha + 1/\alpha + 1| = 1$. Let us take $\beta = \overline{\alpha}$. If $\alpha\beta = |\alpha|^2$ were a root of unity, then it is 1 and hence $|\alpha| = 1$. Together with $|\alpha + 1/\alpha + 1| = 1$ this implies $\alpha = -1, \pm i$. But we have dealt with these cases above. According to Lemma 3.6 the condition $|\alpha + 1/\alpha + 1| = 1$ entails that $x = \alpha/\overline{\alpha}$ and $y = (1+\alpha)/(1+\overline{\alpha})$ cannot be both roots of unity unless $\alpha = -1, \pm i, -1-\zeta, -1-\zeta-\zeta^3$, where ζ is any primitive fifth root of unity. The values $\pm i$ are already dealt with. The value $\alpha = -1$ cannot happen. Finally the values of α in the cyclotomic field $\mathbf{Q}(\zeta)$ give rise to $a = -4 + 10\cos(2\pi/5), -4 + 10\cos(4\pi/5)$, which were also excluded. $\diamond$

Lemma 3.5 *Let $z \in \mathbf{C}$ be such that $|z + 1/z + 3/2| = 1/2$ and such that $z/\overline{z}, (1+z)/(1+\overline{z})$ are both roots of unity. Then $z = -1 \pm i$, $-1/2 \pm 1/2$ or $z^3 = 1$.*

Proof. Put $x = z/\overline{z}$ and $y = (1+z)/(1+\overline{z})$. A short calculation shows that $z = x(y-1)/(y-x)$. Substituting this in the condition $|z + 1/z + 3/2| = 1/2$ gives us, after some calculation using Maple,

$$2x^2y^2 - x^2y + x^2 - xy^3 - 2xy^2 - xy + 2y^2 - y^3 + y^4 = 0$$

. Using an algorithm by C.J.Smyth [S] we can solve this equation for roots of unity and find that

$$(x,y) = (1,1), (1, \pm i), (\pm i, -1), (\pm i, \mp i), (\omega, \omega^2), (\omega^2, \omega)$$

where $\omega = e^{2\pi i/3}$. These pairs give rise to the values of z in our Lemma. $\diamond$

Lemma 3.6 *Let $z \in \mathbf{C}$ be such that $|z + 1/z + 1/2| = 1/2$ and such that $z/\overline{z}, (1+z)/(1+\overline{z})$ are both roots of unity. Then $z = -1, \pm i$ or $z = -1-\zeta, -1-\zeta-\zeta^3$.*

Proof. Put $x = z/\overline{z}$ and $y = (1+z)/(1+\overline{z})$. A short calculation shows that $z = x(y-1)/(y-x)$. Substituting this in the condition $|z + 1/z + 1/2| = 1/2$ gives us, after some calculation using Maple,

$$x^2y^2 - x^2y + x^2 - xy - xy^3 + y^2 - y^3 + y^4 = 0$$

Using the algorithm by C.J.Smyth [S] we can solve this equation for roots of unity and find that

$$(x,y) = (1,1), (\pm 1, \pm i), (\zeta, \zeta^2), (\zeta, \zeta^4)$$

where ζ is any primitive fifth root of unity. These pairs give rise to the values of z in our Lemma. $\diamond$

4 Skolem's method

In this section we prove Theorem 2.2.
We will assume that the reader is familiar with the concept of p-adic numbers. The set of p-adic numbers is denoted by $\mathbf{Q}_p$ and the set of p-adic integers by $\mathbf{Z}_p$.

Lemma 4.1 *Suppose p is an odd prime. Let $A, B, C, D \in \mathbf{Z}_p$ and suppose they are not zero modulo p. Write*

$$A^{p-1} = 1 + p\alpha,\ B^{p-1} = 1 + p\beta,\ C^{p-1} = 1 + p\gamma,\ D^{p-1} = 1 + p\delta$$

where $\alpha, \beta, \gamma, \delta \in \mathbf{Z}_p$. Denote for every $m \in \mathbf{Z}$, $u_m = A^m + B^m - C^m - D^m$.
Let $k \in \mathbf{Z}$ and suppose that $u_k \not\equiv 0 \pmod p$. Then $u_{k+r(p-1)} \neq 0$ for all $r \in \mathbf{Z}$.
Suppose $u_k = 0$ and $\alpha A^k + \beta B^k - \gamma C^k - \delta D^k \not\equiv 0 \pmod p$. Then $u_{k+r(p-1)} = 0,\ r \in \mathbf{Z}$ implies $r = 0$.

Proof. Note that by Fermat's little theorem,

$$\begin{aligned} u_{k+r(p-1)} &= A^{k+r(p-1)} + B^{k+r(p-1)} - C^{k+r(p-1)} - D^{k+r(p-1)} \\ &\equiv A^k + B^k - C^k - D^k \equiv u_k \pmod p \end{aligned}$$

Since $u_k \not\equiv 0 \pmod p$ we conclude that $u_{k+r(p-1)} \not\equiv 0 \pmod p$ for all $r \in \mathbf{Z}$ and our first statement follows.
Suppose $u_{k+r(p-1)} = 0$ and assume $r \geq 0$. Then

$$\begin{aligned} 0 &= A^{k+r(p-1)} + B^{k+r(p-1)} - C^{k+r(p-1)} - D^{k+r(p-1)} \\ &= A^k(1+p\alpha)^r + B^k(1+p\beta)^r - C^k(1+p\gamma)^r - D^k(1+p\delta)^r \\ &= \sum_{t=1}^{r} \binom{r}{t} p^t (A^k\alpha^t + B^k\beta^t - C^k\gamma^t - D^k\delta^t) \end{aligned}$$

Suppose that $r \neq 0$. We divide by pr and use the fact that $\frac{1}{r}\binom{r}{t} = \frac{1}{t}\binom{r-1}{t-1}$ to obtain,

$$0 = A^k\alpha + \cdots - D^k\delta + \sum_{t=2}^{r} \binom{r-1}{t-1} \frac{p^{t-1}}{t} (A^k\alpha^t + \cdots - D^k\delta^t)$$

The summation is of course empty when $r = 1$. Since $p \geq 3$ the number $\frac{p^{t-1}}{t}$ has p-adic valuation less than $1/p$. So after reduction modulo p we obtain

$$0 \equiv A^k\alpha + B^k\beta - C^k\gamma - D^k\delta \pmod p$$

which contradicts our assumption. Hence we conclude $r = 0$. When $r < 0$ we can repeat the above proof with $A^{-1}, \ldots, D^{-1}$ instead of A, B, C, D. $\diamond$

Proof of Theorem 2.2. When $f = f_{5,4}$ divides $f_{b,n}$ this means in particular that the zeros of f are a subset of the zeros of $f_{b,n}$. This holds true in any field, also p-adic fields. Let r, s be two zeros of f. Then clearly, $\frac{(r+1)^4}{r^4+1} = \frac{(s+1)^4}{s^4+1}$. Suppose f divides $f_{b,n}$ for some b, n. Then we also have $\frac{(r+1)^n}{r^n+1} = \frac{(s+1)^n}{s^n+1}$ and hence $((r+1)s)^n + (r+1)^n - ((s+1)r)^n - (s+1)^n = 0$. Note that modulo 181 we have the factorisation

$$f \equiv 4(x-66)(x-139)(x-96)(x-56) \pmod{181}$$

Since 181 does not divide the discriminant of f this implies that f has four roots in $\mathbf{Q}_{181}$. Modulo 181^2 they read,

$$66 + 13 \cdot 181,\ 139 + 29 \cdot 181,\ 96 + 93 \cdot 181,\ 56 + 44 \cdot 181 \pmod{181^2}$$

We now apply Lemma 4.1 with $p = 181$ and $A = (r+1)s, B = r+1, C = r(s+1), D = s+1$. We take r, s to be the first two roots. Then, modulo 181^2 we get

$$A \equiv 67 + 13 \cdot 181,\ B \equiv 82,\ C \equiv 140 + 29 \cdot 181,\ D \equiv 9 + 165 \cdot 181 \pmod{181^2}$$

We also compute modulo 181,

$$\alpha \equiv 33,\ \beta \equiv 46,\ \gamma \equiv 40,\ \delta \equiv 140 \pmod{181}$$

A straightforward computation shows that $u_k \equiv 0 \pmod{181}$ and $0 \leq k < 180$ yields $k = 0, 1, 4, 6$. Lemma 4.1 now implies that $u_{k+180r} \neq 0$ for all r when $k \neq 0, 1, 4, 6$. When $k = 0, 1, 4$ or 6 we easily check that $u_k = 0$ and $\alpha A^k + \cdots - \delta D^k \not\equiv 0 \pmod{181}$. Again, application of Lemma 4.1 shows that $u_k = 0 \Rightarrow k = 0, 1, 4, 6$. When $k = 6$ we check that $b = (r^6+1)/(r+1)^6 = 11$ and f divides indeed $11(x+1)^6 - x^6 - 1$. $\diamond$

We finally remark that the method sketched in this section works also for other cases. When $(a, b, n, m) = (29, 3599, 4, 10)$ we can take $p = 491$. When $(a, b, n, m) = (11, 14867171, 4, 28)$ or $(a, b, n, m) = (1/3, 78719/81, 4, 16)$ we can take $p = 101$.

References

[Bak91] I.M. Bakirov. On the symmetries of some sysem of evolution equations. Technical report, 1991.

[Beu97] F. Beukers. On a sequence of polynomials. *Journal of Pure and Applied Algebra*, 117 & 118:97–103, 1997.

[Bil94] A.H. Bilge. A system with a recursion operator but one higher local symmetry. *Lie Groups and their Applications*, 1(2):132–139, 1994.

[Fok87] A.S. Fokas. Symmetries and integrability. *Studies in Applied Mathematics*, 77:253–299, 1987.

[GD75] I.M. Gel'fand and L.A. Dikii. Asymptotic behaviour of the resolvent of Sturm-Liouville equations and the algebra of the Korteweg-de Vries equations. *Russian Math. Surveys*, 30(5):77–113, 1975.

[Lec53] C. Lech. A note on recurring sequences. *Arkiv. Mat.*, 2:417–421, 1953.

[Olv93] P.J. Olver. *Applications of Lie Groups to Differential Equations*, volume 107 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, (Second Edition) 1993.

[SW97] J.A. Sanders and J.P. Wang. On the integrability of polynomial scalar evolution equations. Technical Report WS-476, Vrije Universiteit Amsterdam, Amsterdam, 1997.

[TQ81] G.Z. Tu and M.Z. Qin. The invariant groups and conservation laws of nonlinear evolution equations-an approach of symmetric function. *Scientia Sinica*, 14(1):13–26, 1981.