The Use of p-adic Numbers in Calculating Symmetries of Evolution Equations

Peter H. van der KAMP

Faculty of Sciences, Division of Mathematics & Computer Science, Vrije Universiteit,
De Boelelaan 1081a, 1081 HV, Amsterdam, The Netherlands
E-mail: peter@few.vu.nl

There exist equations with generalized symmetries that do not have infinitely many general-
lized symmetries. We explain how to prove such a fact using p-adic numbers and calculate
examples using symbolic calculus.

1 Introduction

The title of this text is the same as the title of the talk I gave at the conference “Symmetry in
Nonlinear Mathematical Physics 2001”. It is a misleading title. P-adic numbers are not used
in calculating symmetries. They are used to prove that certain (infinitely many) symmetries do
not exist. The material presented here is not new, it can be found in [8, 9], but the exposition is.

It was observed and conjectured, cf. [6, 5, 7], that the existence of one (or a few) symmetries
implies the existence of infinitely many symmetries. This turned out not to be the case. The
first equation with finitely many symmetries was found by Bakirov [1]:

\[ u_t = 5u_4 + v_0^2, \quad v_t = v_4 \]

has a sixth order symmetry

\[ u_t = 11u_6 + 5v_0v_2 + 4v_1^2, \quad v_t = v_6, \]

where the \(i^{th}\) \(x\)-derivative of \(v_0\) is denoted \(v_i\). It was shown (with extensive computer algebra
computations) that there are no other symmetries up to order 53. The authors of [2] proved
using p-adic numbers that the system of Bakirov does not possess another symmetry at any
higher order.

Have a look at the following points in the complex plane, see Fig. 1. You see 2745 points
inside the upper half unit circle. Let us associate to every such a point \(r\) a new evolution
equation

\[ u_t = (1 + r^4)u_4 + v_0^2, \quad v_t = (1 + r)^4v_4. \]  \(1\)

We show that all these equations have one higher order generalized symmetry.

2 The symmetry condition

Let \(K(v), S(v)\) be polynomials that are quadratic in \(v_0\) and its \(x\)-derivatives \(v_i\). The Lie-bracket,
see [10], between

\[ u_t = a_1u_n + K(v), \quad v_t = a_2v_n \]
Figure 1. Roots of $G$-functions that correspond to almost integrable fourth order Bakirov like equations.

and

$$u_t = b_1 u_m + S(v), \quad v_t = b_2 v_m$$

vanishes when

$$a_1 D^n S(v) - a_2 S(v) v_n = b_1 D^m K(v) - b_2 D K(v) v_m,$$

where total differentiation is done by

$$D = \partial_x + \sum_{i=0}^{\infty} v_{i+1} \partial_{v_i}$$

and the Fréchet derivative is given by the operator

$$D_K(v) = \sum_{i=0}^{\infty} \partial_{v_i} K(v) D^i.$$

We will solve this equation (2) using the symbolic calculus, which was first developed in [4]. The Gel’fand–Dikiĭ transformation

$$v_i v_j \mapsto \frac{\xi^i \xi^j + \xi^i \xi^j}{2}$$

maps every quadratic polynomial $P(v)$ to $P(\xi_1, \xi_2)$. It has the properties

- $DP(v) \mapsto (\xi_1 + \xi_2) P(\xi_1, \xi_2)$,
- $D_{P(v)} v_n \mapsto (\xi_1^n + \xi_2^n) P(\xi_1, \xi_2)$.

Therefore equation (2) reads symbolically

$$G_n[a](\xi_1, \xi_2) S(\xi_1, \xi_2) = G_m[b](\xi_1, \xi_2) K(\xi_1, \xi_2),$$

where the so called $G$-functions are given by the polynomials

$$G_n[a](\xi_1, \xi_2) = a_1(\xi_1 + \xi_2)^n - a_2(\xi_1^n + \xi_2^n)$$

which can easily be solved

$$S = \frac{G_m[b](\xi_1, \xi_2)}{G_n[a](\xi_1, \xi_2)} K$$

if $G_n[a](\xi_1, \xi_2)$ divides $G_m[b](\xi_1, \xi_2)$. 
3 Common roots

We call \( \alpha \) a root of \( f(\xi_1, \xi_2) \) if \( (\xi_1 - \alpha \xi_2) \) divides \( f(\xi_1, \xi_2) \). If \( \alpha \) is a root of \( G_n[\alpha](\xi_1, \xi_2) \) then
\[
\frac{a_1}{a_2} = \frac{1 + r^n}{(1 + r)^n} = \frac{1 + (1/r)^n}{(1 + 1/r)^n}
\]
and hence \( 1/r \) is a root as well. A point \( s \) is another root if
\[
U_n(r, s) = G_n[1 + r^n, (1 + r)^n](s, 1)
\]
vanishes, i.e.
\[
(1 + r)^n + (r + rs)^n - (1 + s)^n - (s + rs)^n = 0.
\] (3)

The functions \( G_n[1 + r^n, (1 + r)^n](\xi_1, \xi_2) \) and \( G_m[1 + r^m, (1 + r)^m](\xi_1, \xi_2) \) have a common set of roots \( \{ \frac{1}{r}, s, \frac{1}{s} \} \) if the resultant of \( U_n(r, s) \) and \( U_m(r, s) \) with respect to \( s \) vanishes. This gives a very effective way to find equations with symmetries.

**Example 1.** We tread the Bakirov system. The resultant of \( U_4(r, s) \) and \( U_6(r, s) \) is
\[
R = 2r^4 + 10r^3 + 15r^2 + 10r + 2.
\]
The ratio of eigenvalues of the system is
\[
\frac{1 + r^4}{(1 + r)^4} \mod R = 5.
\]
The ratio of eigenvalues of the symmetry is
\[
\frac{1 + r^6}{(1 + r)^6} \mod R = 11.
\]
The quadratic part of the system is chosen \( K(v) = v^2_0 \mapsto 1 \), the quadratic part of the symmetry is calculated
\[
S = \frac{G_6[11, 1](\xi_1, \xi_2)}{G_4[5, 1](\xi_1, \xi_2)} = 5\xi_1^2 + \xi_2^2 + 4\xi_1\xi_2 \mapsto 5v_2v_0 + 4v_0^2.
\]
Remark that we could have chosen any function \( K(v) \).

We have calculated all resultants between \( U_4(r, s) \) and \( U_m(r, s) \), where \( 4 < m < 155 \). We added their degrees and divided by four to obtain 2745, the number of fourth order equations with a symmetry of order less than 155. All zero points are numerically calculated and plotted in Fig. 1. The points on the curve throught \(-1\), together with the points on the real line and the unit circle, are mapped to real values by
\[
r \mapsto \frac{1 + r^4}{(1 + r)^4}.
\]
For the other we get complex eigenvalue ratios. The curve throught \(-1\) is the set of zeropoints of
\[
x^4 + 3x^3 + 4x^2 + 3x + 1 + (3x + 2x^2)y^2 + y^4
\]
which appears as a factor of \( U_4(x + iy, x - iy) \). A big question here is where the other curve comes from or at least how to describe it.
The resultants between $U_4(r, s)$ and $U_m(r, s)$ with respect to $s$, where $8 < m < 12$,

\[ r^4 + 8r^3 + 12r^2 + 8r + 1, \]
\[ 14r^4 + 58r^3 + 87r^2 + 58r + 14, \]
\[ 3r^8 + 22r^7 + 69r^6 + 130r^5 + 159r^4 + 130r^3 + 69r^2 + 22r + 3. \]

You do not want to see the rest of the list. To indicate the size of the expressions involved, the resultant between $U_4(r, s)$ and $U_{154}(r, s)$ has degree 148 and coefficients that have 63 digits.

4 No more symmetry

We now ask the question whether a given equation has more than one symmetry. A $p$-adic method allows us to conclude that there exist only a finite number of symmetries. It is extremely powerful in our context. The method is based on the fact that if some equation does not have a solution in some $p$-adic field then it cannot have a solution in $\mathbb{C}$. Moreover the method reduces the number of orders that need to be checked to a finite number.

$p$-adic numbers are represented by formal power series in a prime $p$

\[ a = \sum_{n \geq 0} a_n p^n \]

with $a_n \in \mathbb{Z}/p$. The field of $p$-adic numbers is called $\mathbb{Z}_p$. The invertible elements are in $\mathbb{Z}_p^\times$, they have $a_0 \neq 0$.

Not all (complex) numbers are in every $p$-adic field. The following lemma of Hensel can be used to check whether for example $\sqrt{2}$ is in $\mathbb{Z}_7$.

**Lemma 1 (Hensel).** A polynomial

\[ f(x) = \sum_{i=0}^{n} a_i x^i \quad \text{with} \quad a_i \in \mathbb{Z}_p \]

has a root $\alpha$ in $\mathbb{Z}_p^\times$ if $\exists \alpha_1 \in \mathbb{Z}/p$ such that

- $f(\alpha_1) \equiv 0 \mod p$,
- $f'(\alpha_1) \equiv 0 \mod p$.

We now formulate the lemma of Skolem that form the basis of the method.

**Lemma 2 (Skolem).** If $x_i \in \mathbb{Z}_p^\times$ then by the Fermat little theorem

\[ \exists y_i \in \mathbb{Z}_p : \ x_i^{p-1} = 1 + y_i p. \]

Let $U^m_n = \sum_{i=1} c_i y_i^m x_i^n$ for $m = 0, 1$.

- If $U^0_k \neq 0 \mod p$ then $\forall r \ U^0_{k+r(p-1)} \neq 0$,
- If $U^0_k = 0$ and $U^1_k \neq 0 \mod p$ then $\forall r > 0 \ U^0_{k+r(p-1)} \neq 0$.

Notice that equation (3) has the form $U^0_n = 0$ with $i = 4$, $c_i = (-1)^i$ and

\[ x_1 = 1 + s, \quad x_2 = 1 + r, \quad x_3 = s(1 + r), \quad x_4 = r(1 + s). \]
Example 2. We tread the Bakirov system. With the lemma of Hensel one can show that \(2r^4 + 10r^3 + 15r^2 + 10r + 2\) has two roots in \(\mathbb{Z}_{181}\). Take \(r \equiv 66 + 13p, s \equiv 139 + 29p\). Calculate modulo \(p^2\)
\[
x_1 \equiv 140 + 29p, \quad x_2 \equiv 67 + 13p, \quad x_3 \equiv 82, \quad x_4 \equiv 9 + 165p
\]
and modulo \(p\)
\[
y_1 \equiv 40, \quad y_2 \equiv 33, \quad y_3 \equiv 46, \quad y_4 \equiv 140.
\]
We have that \(m = 0, 1, 4, 6\) are the only values less than \(p - 1\) such that \(U_m^0 \equiv 0\) modulo \(p\) and that
\[
U_0^1 \equiv 78, \quad U_1^1 \equiv 173, \quad U_4^1 \equiv 169, \quad U_6^1 \equiv 162.
\]
With the lemma of Skolem we may now conclude that if there is a symmetry it has be at order 6.

It is verified that all fourth order systems (1) with a symmetry of order less than 155 have one symmetry. The proof is done automatically by a computer using the lemma of Skolem in MAPLE [3]. The hard part is finding a good prime \(p\). Once you know \(p\), the conditions are very easily checked. We list some modulo \(p\) solutions of the resultants between \(U_4(r, s)\) and \(U_m(r, s)\) for \(8 < m < 12\) in the specific fields
\[
71, \quad 72 \in \mathbb{Z}/293, \\
79, \quad 175 \in \mathbb{Z}/491, \\
26, \quad 44 \in \mathbb{Z}/53.
\]

5 Conclusion

More results in this direction can be found in [8, 9], as well as the proofs of the relevant lemmas. It is proven that there exist infinitely many evolution equations with finitely many symmetries. All systems of order \(n\) with \(4 < n < 11\) with symmetries of order \(m\) with \(n < m < n + 150\) have been calculated. Some improvements on the \(p\)-adic method have been made. These made it possible to show that among all the calculated systems there are only 3 equations with 2 symmetries, counter examples to the conjecture stated in [7, p. 255]. These systems have order 7 and their symmetries appear at order 11 and 29.