The Minimum Polynomial of an Algebraic Solution of Abel's problem.

Mark van Hoeij
Department of Mathematics
Florida State University
Tallahassee, FL 32306-3027, USA
hoeij@math.fsu.edu

Abstract

Abel's problem is the question how to solve the equation $\mathrm{d}y/\mathrm{d}x = ay$ where a is an algebraic function in x. Suppose that the solution y is an algebraic function. The topic of this paper is how to calculate the minimum polynomial of y over $\mathbb{C}(x)$ without computing an expression for y in terms of a and x.

1 Introduction

Let a be an algebraic function in x. Let P be its minimum polynomial; $P(Z) \in \mathbb{C}(x)[Z]$ is a monic irreducible polynomial such that $P(a) = 0$. Consider the first order differential equation

$$\frac{\mathrm{d}y}{\mathrm{d}x} = ay \tag{1}$$

and let $y = \exp(\int a)$ be a solution of this equation. If y is an algebraic function, then $\int a = \log(y)$ is an elementary function, so then $\int a$ can be calculated because the problem of elementary integration of algebraic functions is solved, see [4, 6]. Implementations exist as well, for example Maple has an implementation of Trager's algorithm. However, this algorithm would take a very long time for the example in section 2; the result would be an expression for y in terms of a and x that would most likely be very large and hence hard to compute. The topic of this paper is how to circumvent this computational difficulty, i.e. how to calculate this minimum polynomial without first calculating an expression for y in terms of a and x.

Acknowledgments: The author would like to thank Jacques-Arthur Weil and Marius van der Put for discussions on this topic.

2 Example from differential Galois theory

In [3], van der Put and Ulmer give an explicit construction for the inverse problem in differential Galois theory for finite groups. Starting with a finite group G and a representation of G on a vector space (effectively this means: one starts with a set of matrices that generate a finite group under multiplication), they show how to find a linear differential equation $L(y) = 0$ that has as differential Galois group the group G, which acts on the solution space of $L(y) = 0$ in the same way as the representation of G one started with.

Their method is very effective; for many groups this calculation is feasible on a computer. We used their method to find an operator L with differential Galois group $G = H_{72}^{\mathrm{SL}(3)}$, a group with $3 \cdot 72 = 216$ elements. We chose a representation and generators of G that have some properties of symmetry that could be exploited to facilitate the calculation of L. This way we found the operator

$$L = a_3\partial^3 + a_2\partial^2 + a_1\partial + a_0$$

where

$$a_3 = 432(x-1)(3x^2+1)^3$$

$$a_2 = 432(21x^2 - 24x - 1)(3x^2+1)^2$$

$$a_1 = 9(3x^2+1)(4437x^3 - 5973x^2 + 171x - 683)$$

$$a_0 = 26676x^4 - 45294x^3 + 3966x^2 - 14594x - 1474$$

and the corresponding differential equation is

$$L(y) = a_3y''' + a_2y'' + a_1y' + a_0y = 0.$$

The differential Galois group of L must be the group $G = H_{72}^{\mathrm{SL}(3)}$ that we started with because of the results of van der Put and Ulmer. Any solution y of L will be an algebraic function for which the minimum polynomial has Galois group G over $\mathbb{C}(x)$. From [5] we know that for this group there must exist a solution y that is algebraic over $\mathbb{C}(x)$ of degree 27 (the degree of the minimum polynomial is 27) and furthermore $a = y'/y$ will be algebraic of degree 9 over $\mathbb{C}(x)$. Note that if one takes a random solution y of L then these degrees are most likely much higher. The algorithm given in [2] allows us to find the minimum polynomial of degree 9 of $a = y'/y$. The result is:

$P(Z) = Z^9 + 30x/(3x^2+1) \cdot Z^8 + 1/4 \cdot (1599x^2+1)/(3x^2+1)^2 \cdot Z^7 + 1/72 \cdot (223587x^3 + 15x^2 + 441x + 5)/(3x^2+1)^3 \cdot Z^6 + 1/1152 \cdot (17855019x^4 + 4800x^3 + 73962x^2 + 1600x - 21)/(3x^2+1)^4 \cdot Z^5 + 1/3456 \cdot (178134957x^5 + 119907x^4 + 1290114x^3 + 40062x^2 - 1071x + 31)/(3x^2+1)^5 \cdot Z^4 + 1/248832 \cdot (28420622685x^6 + 38312352x^5 + 323581833x^4 + 12864960x^3 - 524073x^2 + 31392x + 67)/(3x^2+1)^6 \cdot Z^3 + 1/497664 \cdot (80931106503x^7 + 191139507x^6 + 1350862263x^5 + 64704555x^4 - 3559875x^3 + 330129x^2 + 1349x - 111)/(3x^2+1)^7 \cdot Z^2 + 1/47775744 \cdot (6449857313913x^8 + 24395769216x^7 + 150200784540x^6 + 8354150784x^5 -$

$580059306x^4 + 73858176x^3 + 437148x^2 - 72576x + 505)/(3x^2+1)^8 \cdot Z + 1/644972544 \cdot (32112055562886x^9 + 182329225533x^8 + 1005364927404x^7 + 63398867400x^6 - 5314028328x^5 + 869144634x^4 + 6682932x^3 - 1669824x^2 + 23490x - 127)/(3x^2+1)^9$.

Let a be a root of $P(Z)$. Then the algebraic function a is of the form y'/y for some solution y of L that is algebraic of degree 27. Hence, for this algebraic function a we know that equation (1) has an algebraic solution y of degree 27. If we can calculate the minimum polynomial of the solution y of equation (1), then we have obtained a polynomial with Galois group G over $\mathbb{C}(x)$. Take $d = 27/9 = 3$, so $\tilde{y} = y^d$ must be in $\mathbb{C}(x,a)$, see section 3. Now $\tilde{y}$ is a solution of $\tilde{y}' = da\ \tilde{y}$, and once $\tilde{y}$ is computed we find $y = \tilde{y}^{1/d}$. If we can calculate the minimum polynomial $Q(Z)$ of $\tilde{y}$, then $Q(Z^d)$ is the minimum polynomial of y. However, calculating in $\mathbb{C}(x,a) \simeq \mathbb{C}(x)[Z]/(P(Z))$ is clearly very costly because $P(Z)$ is so large. So obtaining the polynomial Q below would be hard if we would first have to to compute the solution $\tilde{y}$ of $\tilde{y}' = da\ \tilde{y}$ in terms of a and x, i.e. if we had to find an expression for $\tilde{y}$ in $\mathbb{C}(x,a)$. The following is the minimum polynomial of a solution y of $y' = ay$.

$Q(Z^3) = Z^{27} - 168/(3x^2+1)^5 \cdot Z^{18} + 405(1+x)/(3x^2+1)^7 \cdot Z^{15} - 636/(3x^2+1)^{10} \cdot Z^9 - 324(1+x)/(3x^2+1)^{12} \cdot Z^6 - 243/4 \cdot (1+x)^2/(3x^2+1)^{14} \cdot Z^3 - 8/(3x^2+1)^{15}$.

We verified that the Galois group of this polynomial over $\mathbb{C}(x)$ is indeed $H_{72}^{\mathrm{SL}(3)}$ using the monodromy command in Maple V Release 6.

An alternative method to calculate the minimum polynomial of an algebraic solution for such a differential equation is given in [1], section 5.1.7.

3 Review of the problem

Since $y = \exp(\int a)$ we will make some remarks about the Risch/Trager integration algorithm for $\int a$. At some point in this algorithm the residues (see also section 6) of a are computed. In our case $a = y'/y$ where we assume y to be an algebraic function, so these residues must be rational numbers. So the $\mathbb{Z}$-basis of the residues will contain only 1 element, so in our case there will be only 1 divisor D in the integration algorithm. A difficult problem in the integration is how to decide if D is a torsion divisor, and if so, how to bound the torsion index. The solution of this problem involves reducing of the curve modulo two prime numbers and computing the torsion index on the reduced curves. If y is algebraic, then $\int a = \log(y)$ is an elementary function, and since the integration algorithm can find elementary integrals it will find an elementary expression for $\int a$, which will be of the form $\int a = r \cdot \log(A)$ where $r \in \mathbb{Q}$ and $A \in \mathbb{C}(x,a)$. If $r = n/d$ then $y^d = A^n \in \mathbb{C}(x,a)$. So we see that when y is an algebraic function, then $y^d \in \mathbb{C}(x,a)$ for some integer d. The denominator d of r depends on the torsion index of the divisor D, see also section 6. So it can be calculated and implementations exist, but it is nevertheless a difficult problem. In fact, Risch was able to give a complete decision procedure for elementary integration once the problem of bounding this torsion index was solved.

In this paper we will not show how to calculate an upper bound for d or even how to check if the solution y of equation (1) is indeed algebraic. We will simply assume that y is algebraic and that d is already known, which is true in the application in sections 2 and 8. Under these assumptions, $\tilde{y} = y^d$ is a solution of

$$\frac{\mathrm{d}\tilde{y}}{\mathrm{d}x} = da\ \tilde{y} \tag{2}$$

and $\tilde{y} \in \mathbb{C}(x, a)$, so $\tilde{y}$ can be expressed in terms of x and a. If $Q(Z) \in \mathbb{C}(x)[Z]$ is the minimum polynomial of $\tilde{y}$ then the minimum polynomial of y is $Q(Z^d)$. Now $\mathbb{C}(x, \tilde{y}) \subset \mathbb{C}(x, a)$, but since $a = y'/y = \frac{1}{d}\tilde{y}'/\tilde{y} \in \mathbb{C}(x, \tilde{y})$ the inclusion is an equality, so

$$\mathbb{C}(x)[Z]/(Q(Z)) \simeq \mathbb{C}(x, \tilde{y}) = \mathbb{C}(x, a) \simeq \mathbb{C}(x)[Z]/(P(Z)).$$

Suppose P is not just defined over $\mathbb{C}$, but over a smaller field of constants $C \subset \mathbb{C}$. In this paper we take $C = \mathbb{Q}$, but our method applies to other fields C of characteristic 0 as well. So assume that P is defined over $\mathbb{Q}$, in other words: $P(Z) \in \mathbb{Q}(x)[Z]$ instead of in $\mathbb{C}(x)[Z]$. Then the function A that can be computed by Trager's algorithm will also be defined over $\mathbb{Q}$. So $A \in \mathbb{Q}(x, a)$, and hence for the corresponding y we have $\tilde{y} = y^d \in \mathbb{Q}(x, a)$. So if P is defined over $\mathbb{Q}$, and if equation (1) has an algebraic solution, then it must also have an algebraic solution which has a minimum polynomial over $\mathbb{C}(x)$ that is defined over $\mathbb{Q}$.

If $c \in \mathbb{C}^*$ and $Q(Z)$ is the monic minimum polynomial of $\tilde{y}$ over $\mathbb{C}(x)$, then denote by $Q_c(Z) = c^n Q(Z/c)$ the monic minimum polynomial of $c\tilde{y}$ over $\mathbb{C}(x)$. Here n is the degree of Q, which is the same as the degree of P. Non-trivial solutions $\tilde{y}$ of equation (2) are unique up to constant factors in $\mathbb{C}^*$. So if P is defined over $\mathbb{Q}$, and $Q(Z) \in \mathbb{C}(x)[Z]$ is the monic minimum polynomial of some solution $\tilde{y}$ of equation (2), then there exists a constant c such that $Q_c(Z) \in \mathbb{Q}(x)[Z]$.

So if we would have a minimum polynomial Q of some a solution $\tilde{y}$, then it is easy to find a minimum polynomial Q_c of another solution $c\tilde{y}$ of equation (2) such that Q_c is defined over $\mathbb{Q}$, as follows. If the polynomial $Q(Z)$ can be written as a polynomial $Q'(Z^{d'})$ with $d' > 1$ then replace Q by Q'. After that, the set S of all i from 1 to n for which the coefficient of Z^{n-i} is not zero is a set of integers for which the greatest common divisor equals $g = 1$. For $i \in S$, the coefficient of Z^{n-i} in Q_c is of the form $c^i \beta_i R_i$ with $\beta_i \in \mathbb{C}^*$ and $R_i \in \mathbb{Q}(x)$. Now take $i_1, \ldots, i_l \in S$ and integers $m_1, \ldots, m_l$ for which $m_1 i_i + \cdots m_l i_l = 1$. Such $m_j \in \mathbb{Z}$ exist because $g = 1$. Then the product of $(c^{i_j}\beta_{i_j})^{m_j}$ equals $c\gamma$ for some $\gamma \in \mathbb{C}^*$, and we can take $c = 1/\gamma$. For example, the polynomial on page 88 in [1] can be transformed in this way into a polynomial defined over $\mathbb{Q}$.

Note that for the minimum polynomial $Q(Z)$ of $\tilde{y}$ can in fact not be written as $Q'(Z^{d'})$ with $d' > 1$, because then if z is a root of $Q'(Z)$ we would have $a = \frac{1}{d'd} z'/z \in \mathbb{C}(x, z)$ but $\mathbb{C}(x, z)$ can not contain a because its degree over $\mathbb{C}(x)$ is the degree of $Q'(Z)$, which is smaller than the degree of a.

Now Q_c is defined over a smaller field of constants than Q and so it will be a smaller expression, which usually means that it can be computed more quickly. Therefore, if $\tilde{y}$ is a solution of equation (2), we want to compute the minimum polynomial Q_c of $c\tilde{y}$ without computing Q. Now the question is, given a solution $\tilde{y}$, how to compute c when we do not yet have Q. A solution $\tilde{y}$ can be represented by calculating a power series expansion for it at a point $x = b$, so $\tilde{y}$ is expressed as a (truncation of) an element of the ring of formal power series $\mathbb{C}[[x-b]]$. Then the condition on c is that Q_c is defined over $\mathbb{Q}$. This condition will make c unique up to factors in $\mathbb{Q}^*$.

So the main problem is the following: Given an algebraic solution $\tilde{y} \in \mathbb{C}[[x-b]]$ of equation (2), how to find a constant $c \in \mathbb{C}^*$ such that the minimum polynomial of $c\tilde{y}$ over $\mathbb{C}(x)$ is defined over $\mathbb{Q}$. Our method for finding c will at the same time find rational functions $P_1, \ldots, P_n \in \mathbb{Q}(x)$ from which the minimum polynomial of $c\tilde{y}$ can be constructed using elementary polynomials.

4 Elementary polynomials

Let $x_1, x_2 \ldots, x_n$ be variables and consider the polynomial

$$F = (Z - x_1)(Z - x_2) \cdots (Z - x_n).$$

We can write F as

$$F = Z^n + (-1)^1 E_1 Z^{n-1} + (-1)^2 E_2 Z^{n-2} + \cdots + (-1)^n E_n Z^0$$

where $E_i(x_1, \ldots, x_n)$ is the i'th elementary polynomial in the variables $x_1, \ldots, x_n$. Now define the i'th power polynomial $P_i(x_1, \ldots, x_n)$ as $x_1^i + x_2^i + \ldots x_n^i$. It is a classical result that $E_1, \ldots, E_n$ can be expressed in terms of $P_1, \ldots, P_n$ and vice versa, and it is also known how to compute these expressions. For example, $E_1 = P_1$ and $E_2 = (P_1^2 - P_2)/2$. A particularly short and efficient method to compute these expressions is given by the following Maple commands:

```
F:=Z^n+add((-1)^i*E[i]*Z^(n-i),i=1..n);
evala(Trace( RootOf(F,Z)^i ));
```

When i and n are integers and $1 \le i \le n$ then the above commands give P_i as an expression in terms of $E_1, \ldots, E_i$. By back substitution we can then also express E_i as a polynomial in $P_1, \ldots, P_i$.

The minimum polynomial Q that we are looking for is of the form

$$Q = (Z - y_1) \cdots (Z - y_n) \in \mathbb{C}(x)[Z]$$

where $\tilde{y} = y_1$ is an algebraic solution of equation (1) and where $y_1, \ldots, y_n$ are the conjugates of y_1 over $\mathbb{C}(x)$. The coefficient of Z^{n-i} in this polynomial Q equals $(-1)^i E_i(y_1, \ldots, y_n)$. However, instead of calculating the E_i we will calculate the rational functions $P_i(y_1, \ldots, y_n) = y_1^i + \cdots + y_n^i \in \mathbb{C}(x)$. As explained above, the $E_i(y_1, \ldots, y_n)$ can be expressed in terms of these $P_i(y_1, \ldots, y_n)$, and so we obtain Q. Note that $P_i(y_1, \ldots, y_n) \in \mathbb{C}(x)$ is the trace of $\tilde{y}^i$ taken over the algebraic extension $\mathbb{C}(x) \subset \mathbb{C}(x, \tilde{y})$.

5 Taking the trace, continuation of the example.

Let $\tilde{y}$ be an algebraic solution of equation (2), so $\tilde{y} \in \mathbb{C}(x, \tilde{y}) = \mathbb{C}(x, a)$. Let $y_1 = \tilde{y}$ and let $y_2, \ldots, y_n$ be the conjugates of y_1 over $\mathbb{C}(x)$. Then $P_i(y_1, \ldots, y_n)$ is a rational function, it is the trace of $\tilde{y}^i$ over the algebraic extension $\mathbb{C}(x) \subset \mathbb{C}(x, a)$. How to calculate this trace?

To do this we would need to have some representation for $\tilde{y}$ that we can compute with. As mentioned before, an expression for $\tilde{y}$ in terms of a and x is costly to compute, so we will use a power series expansion for $\tilde{y}$ instead. Take a point $b \in \mathbb{C}$ such that $x = b$ is not a branch point nor a pole of the algebraic function a. After substituting $x + b$ for x we may assume that $b = 0$. So then $x = 0$ is not branch point of a, in other words x divide the discriminant of the monic minimum polynomial P of a. And $x = 0$ is not a pole of a, which means that $x = 0$ is not a pole of any of the coefficients of P. Then, when we calculate the Puiseux expansions at $x = 0$, we obtain n power series expansions $a_1, \ldots, a_n \in \mathbb{C}[[x]]$ for the algebraic function a. These $a_1, \ldots, a_n$ are the roots of P as a polynomial in Z, i.e. $P = (Z - a_1) \cdots (Z - a_n)$.

In the example in section 2 we get

$$a_1 = a_{1,0}x^0 + a_{1,1}x^1 + a_{1,2}x^2 + \cdots$$

where $a_{1,0} = \alpha$, where α is a root of
$1289945088x^9 + 322486272x^7 + 89579520x^6 - 23514624x^5 + 11570688x^4 + 347328x^3 - 287712x^2 + 13635x - 254$.

The coefficient $a_{1,1}$ of x^1 is:
$a_{1,1} = 5760\alpha^8 - 960\alpha^7 + 1320\alpha^6 + 440/3 \cdot \alpha^5 - 3605/18 \cdot \alpha^4 + 225/4 \cdot \alpha^3 - 18037/2592 \cdot \alpha^2 - 4705/1944 \cdot \alpha - 6463/1944$,

and for the next coefficients $a_{1,2}, \ldots$ we find similar expressions. The expansions $a_2, \ldots, a_9$ in this example are the conjugates of a_1 over $\mathbb{Q}$.

Now for each i we need a solution $y_i \in \mathbb{C}[[x]]$ of the equation

$$y_i' = da_i \; y_i.$$

Recall that $d = 3$ in this example. We can find solutions by calculating a series expansion for $y_i = \exp(d \int a_i)$. But this expression is only determined up to a constant factor. Simply choosing a value for that constant factor does not work, as will be explained below. Suppose for example we choose this constant factor by taking the constant term of the y_i to be 1. Then we have

$$y_1 = 1 + da_{1,0}x^1 + \frac{1}{2}(da_{1,1} + (da_{1,0})^2)x^2 + \cdots$$

and then $y_2, \ldots, y_9$ will be the conjugates of y_1 over $\mathbb{Q}$, which means that to obtain these $y_2, \ldots, y_9$ one has to replace the algebraic number α with its conjugates over $\mathbb{Q}$. However, for this choice of $y_1, \ldots, y_9$ the product $(Z - y_1) \cdots (Z - y_9)$ will *not* be an element of $\mathbb{C}(x)[Z]$. The reason is the following: The minimum polynomial $Q(Z)$ of y_1 over $\mathbb{C}(x)$ can be calculated (although it is not efficient to do so) and the result will be defined over $\mathbb{Q}(\alpha)$ because y_1 is defined over $\mathbb{Q}(\alpha)$. It is unlikely that it will be defined over $\mathbb{Q}$, and indeed, in this example it is not. Hence $Q(Z)$ is not equal to $(Z-y_1)\cdots(Z-y_9)$, because the latter is defined over $\mathbb{Q}$. So $(Z-y_1)\cdots(Z-y_9)$ is not equal to the minimum polynomial $Q(Z)$ of y_1, even though it has y_1 as a root and is of the right degree. This implies that it is not an element of $\mathbb{C}(x)[Z]$. And this in turn implies that the $P_i(y_1,\ldots,y_9)$ are not elements of $\mathbb{C}(x)$, at least not all of them.

So if we calculate $P_i(y_1,\ldots,y_9)$, which is the trace of y_1^i over the extension $\mathbb{Q}((x)) \subset \mathbb{Q}(\alpha)((x))$, we will get a power series in $P_i \in \mathbb{Q}[[x]]$ and not all of these (for $i = 1,\ldots,9$) will be rational functions. Most likely none of them will be a rational function. So we see that simply taking the constant term of the y_i to be 1 did not work. The y_i need to be multiplied by constants in such a way that the P_i will be rational functions, and this is the condition we will use to determine the constant c.

Since $Q(Z)$ is defined over $\mathbb{Q}(\alpha)$, the number c we need to have $Q_c(Z) \in \mathbb{Q}(x)[Z]$ is an element of $\mathbb{Q}(\alpha)$, so we can write

$$c = k_0\alpha^0 + \cdots k_8\alpha^8$$

where $(k_0,\ldots,k_8)$ is an unknown element of $\mathbb{Q}^9$, and it is unique up to factors in $\mathbb{Q}^*$. Now $Q_c(Z)$ has cy_1 as a root, and since $Q_c(Z)$ is defined over $\mathbb{Q}$, the conjugates of cy_1 over $\mathbb{Q}$ are roots of $Q_c(Z)$ as well. To find the coefficients of $Q_c(Z)$ we need to compute $P_i(cy_1,\ldots)$, where the dots stand for the conjugates over $\mathbb{Q}$. This $P_i(cy_1,\ldots)$ is the trace of $(cy_1)^i$ taken over $\mathbb{Q} \subset \mathbb{Q}(\alpha)$.

We can calculate, see section 6, rational functions $B_i \in \mathbb{Q}(x)$ and integers N_i such that $P_i(cy_1,\ldots)/B_i$, which is a priori an infinite power series in x, will be a polynomial in x of degree at most N_i. So the coefficients of powers of x higher than N_i in this power series should vanish. For each i this gives us infinitely many homogeneous polynomial equations of degree i in the unknowns $k_0,\ldots,k_8$. Combined, they are necessary and sufficient conditions, because these P_i are rational functions if and only if all of those excess powers of x have coefficient 0. Since every polynomial ideal is finitely generated, we can find a sufficient equations by only computing the coefficients of x^j for $N_i < j < M$ when M is a sufficiently large integer (just keep increasing M until sufficient conditions are obtained to determine $(k_0,\ldots,k_8)$ up to a constant factor). In most examples, including this one, we already obtain sufficient equations if we only consider the equations for $i = 1$, which are linear equations. So in this example we do not need to solve non-linear equations, because the linear equations already determine $(k_0,\ldots,k_8)$ up to a constant factor. This constant factor can simply be chosen in $\mathbb{Q}$. Then we find $c = k_0\alpha^0 + \cdots k_8\alpha^8 \in \mathbb{Q}(\alpha)$, and after that we only need to compute the coefficients of x^j of $P_i(cy_1,\ldots)/B_i$ for $j = 0,\ldots,N_i$ to determine the value of $P_i/B_i \in \mathbb{Q}[x]$. Multiplying these polynomials by B_i gives P_i, and then $Q_c(Z)$ can be determined as explained in section 4.

If the case $i = 1$ would not determine $(k_0,\ldots,k_8)$ up to a constant, we can usually still avoid having to solve non-linear polynomial equations. Write

$c^i = c_{i,0}\alpha^0 + \cdots c_{i,8}\alpha^8$. Then $c_{i,j}$ can be expressed as a homogeneous polynomial in $k_0, \ldots, k_8$ of degree i. Now the condition that $P_i(cy_1, \ldots)$ is a rational function translates in homogeneous polynomial equations of degree i in the variables $k_0, \ldots, k_8$, but can also be presented as linear equations in $c_{i,0}, \ldots, c_{i,8}$. Suppose that these linear equations determines $(c_{i,0}, \ldots, c_{i,8})$ up to a constant factor for two coprime values of i. This is very likely to happen. Take for example $i = 3$ and $i = 5$. Then we can, solving just linear equations, determine c^3 up to a factor in $\mathbb{Q}$, and c^5 up to a factor in $\mathbb{Q}$, so then $c = (c^3)^2/c^5$ can be determined up to a factor in $\mathbb{Q}$. We can choose that factor and we find again a value for c in $\mathbb{Q}(\alpha)$. Then we can calculate $P_i(cy_1, \ldots)$ like before by calculating the trace of $(cy_1)^i$ over $\mathbb{Q}((x)) \subset \mathbb{Q}(\alpha)((x))$. Like before, P_i/B_i is then a polynomial in $\mathbb{Q}[x]$ of degree at most N_i. To determine that polynomial we need to calculate P_i up to accuracy $N_i + 1$ (which means modulo x^{N_i+1}). From that we can calculate P_i/B_i modulo x^{N_i+1}. This gives us the polynomial P_i/B_i, multiplying by B_i then give us $P_i \in \mathbb{Q}(x)$.

Note that in our example all the Puiseux expansions $a_1, \ldots, a_9$ were conjugated over $\mathbb{Q}$. So the number m in the algorithm in section 7, which is the number of conjugacy classes, equals 1. For most points $b \in \mathbb{Q}$, the number of conjugacy classes for the Puiseux expansions at $x = b$ will be $m = 1$. However, if we choose a point $x = b$ where $m > 1$, the method still works in more or less the same way. In that case we have one value for c in each conjugacy class, and then P_i is a sum over traces, one trace for each conjugacy class. The total number of unknowns in $\mathbb{Q}$ in these c's will still be n, the degree of $P(Z)$. See section 7 for more details.

6 Bounds on the rational functions P_i

Let y be an algebraic function with minimum polynomial $Q(Z^d)$, and let $a = y'/y$. Let b be a point in $\mathbb{C}$. The splitting field of $Q(Z^d)$ can be embedded in $\mathbb{C}(((x-b)^{1/e}))$ for some positive integer e. The roots of $Q(Z^d)$ in $\mathbb{C}(((x-b)^{1/e}))$ are called the Puiseux expansions of $Q(z^d)$. Each of these expansions is of the form

$$y = s_0(x-b)^{r_0} + s_1(x-b)^{r_1} + \cdots$$

Here the s_i are in $\mathbb{C}$ and the $r_0 < r_1 < r_2 \cdots$ are elements of $\frac{1}{e}\mathbb{Z}$.

Then $a = y'/y$ is a Puiseux series (a power series with fractional powers) in $x - b$ of the form

$$a = r_0(x-b)^{-1} + \cdots$$

so the term of a with the lowest power in $x-b$ is $r_0(x-b)^{-1}$. Given the minimum polynomial for a, we can calculate the Puiseux expansions at $x = b$. If the lowest power in $x - b$ is smaller than -1 in any of these Puiseux expansions, or if the coefficient r_0 of $(x-b)^{-1}$ is not a rational number, then $y = \exp(\int a)$ can not be an algebraic function. The coefficients of $(x-b)^{-1}$ in the Puiseux expansions are called the *residues* of a at the point $x = b$. If r is the smallest residue at $x = b$, the smallest power of $x - b$ is at least r in every Puiseux expansion of

y at $x = b$. So the smallest possible power of $x - b$ in $\tilde{y}^i = y^{id}$ or any of its conjugates is rid. Therefore, the smallest possible power of $x - b$ in the series expansion of the rational function P_i must be at least $\lceil rid \rceil$. Here the brackets denote rounding up to an integer.

Let $B_i \in \mathbb{C}(x)$, or $B_i \in \mathbb{Q}(x)$ if $P(Z)$ is defined over $\mathbb{Q}$, be the rational function

$$B_i = \prod_b (x - b)^{\lceil rid \rceil}$$

where the product is taken over all $b \in \mathbb{C}$ at which a has a pole. Then, for every $b \in \mathbb{C}$ the rational function P_i/B_i must have lowest power at least 0 when presented as a power series in $x - b$. In other words: P_i/B_i has no poles in $\mathbb{C}$, therefore it is a polynomial. We can find a degree bound N_i for this polynomial by calculating the residues of a at the point $x = \infty$.

Consider again the Puiseux series

$$a = r_0(x - b)^{-1} + \cdots$$

Take the smallest positive integer e for which this series is an element of $\mathbb{C}(((x - b)^{1/e}))$. Then the corresponding Puiseux series for $\tilde{y} = y^d$ is an element of the same field because $\mathbb{C}(x, a) = \mathbb{C}(x, \tilde{y})$. So the Puiseux expansion

$$\tilde{y} = s_0^d (x - b)^{dr_0} + \cdots$$

must also be an element of $\mathbb{C}(((x - b)^{1/e}))$, which implies that $dr_0 \in \frac{1}{e}\mathbb{Z}$. This implies that the denominator of r_0 must divide de. For each residue of a we can find a lower bound for d in this way. These lower bounds are combined by taking the least common multiple. The lower bound for d obtained in this way, multiplied by the torsion index of the divisor D in the integration algorithm, gives the actual value for d. However, it is not easy to calculate this torsion index. It is 1 (resulting in $d = 3 \cdot 1$) in the example from section 2, and it is 2 (resulting in $d = 1 \cdot 2$) in the example from section 8.

7 The algorithm

Input: A polynomial $P \in \mathbb{Q}(x)[Z]$ that is irreducible in $\mathbb{C}(x)[Z]$, and a positive integer d such that $y' = ay$ has an algebraic solution of degree dn.
Here n is the degree of P, and a is an algebraic function with P as minimum polynomial.

Output: The minimum polynomial over $\mathbb{C}(x)$ of a solution y of $y' = ay$. This minimum polynomial $Q(z^d)$ will be an element of $\mathbb{Q}(x)[Z^d]$.

Step 1. If $x = 0$ is a pole or a branchpoint of a then remedy this by substituting $x + b$ for x in P for some $b \in \mathbb{Q}$.

Step 2. Calculate the bounds B_i and N_i.

Step 3. Let M be the maximum of the numbers $N_1 + 1, N_2 + 1, \ldots, N_n + 1$ and

$n + \max(0, N_1 + 1)$.

Step 4. Calculate the Puiseux expansions (up to conjugacy over $\mathbb{Q}$) of a at the point $x = 0$ up to accuracy $M - 1$. If there are m conjugacy classes, then we have truncations of m Puiseux expansions $a_1, \ldots, a_m$. Denote $a_{l,1} = a_l$ and let $a_{l,1}, a_{l,2}, \ldots, a_{l,m_l}$ denote the conjugates of $a_{l,1}$ over $\mathbb{Q}$. Let $\mathbb{Q}(\alpha_l)$ be the field over which $a_{l,1}$ is defined. Then $\{a_{l,j}\}$ is the set of n Puiseux expansions at $x = 0$.

Step 5. For l from 1 to m, calculate a series expansion of accuracy M (i.e. modulo x^M) of $y_{l,1} = \exp(\int a_l)$, such that $y_{l,1}$ has constant term 1.

Step 6. For l from 1 to m, Let $c_l = \sum_{j=0}^{m_l-1} k_{l,j}\alpha_l^j$.

Step 7. Let $P_{l,i}$ be the trace of $c_l a_{l,1}$ taken over $\mathbb{Q}$ and let $P_i = \sum_{l=1}^m P_{l,i}$.

Step 8 Calculate P_i/B_i modulo x^M for i from 1 to n.

Step 9 Equate the coefficients of x^j in P_i/B_i for $N_i < j < M$ to zero. If we are not able to find a unique (up to a constant factor) solution for $(k_{1,0}, \ldots) \in \mathbb{Q}^n$ from this then increase M and go back to step 4. Otherwise, substitute a solution in $\mathbb{Q}^n$ for the variables $k_{1,0}, \ldots$.

Step 10 Now P_i/B_i modulo x^M are elements of $\mathbb{Q}[x]$ of degree at most N_i. Multiply these polynomials by B_i to find $P_i \in \mathbb{Q}(x)$.

Step 11 Compute $Q(Z)$ as in section 4 and return $Q(Z^d)$.

8 Another example.

$$y''' + \frac{21(x^2 - x + 1)}{25(x^2 - x)^2} y' - \frac{21(2x-1)(x^2 - x + 2)}{50(x^2 - x)^3} y = 0.$$

The minimum polynomial of $a = y'/y$ for some solution y has been given in example 4.4 in [2]:

$P(Z) = Z^6 - 4(2x-1)/(x^2-x) \cdot Z^5 + 1/5 \cdot (133x^2 - 133x + 33)/(x^2-x)^2 \cdot Z^4 - 12/25 \cdot (7x-4)(2x-1)(7x-3)/(x^2-x)^3 \cdot Z^3 + 1/125 \cdot (351 - 11662x^3 + 8693x^2 + 5831x^4 - 2862x)/(x^2-x)^4 \cdot Z^2 - 4/3125 \cdot (2x-1)(9604x^4 - 19208x^3 + 14275x^2 - 4671x + 567)/(x^2-x)^5 \cdot Z + 1/12500 \cdot (16807x^4 - 33614x^3 + 24907x^2 - 8100x + 972)(2x-1)^2/(x^2-x)^6$

but the minimum polynomial of y itself had not yet been determined. The method in this paper can do this very efficiently. Starting with $P(Z)$ and $d = 2$ it only took 5 seconds of CPU time on a Pentium 266 to find the following minimum polynomial for y: $Q(Z^2) =$

$Z^{12} + 40(x^2-x)^4 Z^6 - 64(x^2-x+1)(x^2-x)^6 Z^2 + 80(x^2-x)^8$.

The example in section 2 took about 18 seconds CPU time using the code given on the following URL:

`http://www.math.fsu.edu/~hoeij/files/issac2000_H72`

References

[1] W. Fakler, Algebraische Algorithmen zur Lösung von linearen Differentialgleichungen, *Ph.D thesis*, University of Paderborn, (1998).

[2] M. van Hoeij, J-F Ragot, F. Ulmer, J-A Weil, Liouvillian solutions of linear differential equations of order three and higher. *J. Symb. Comput.* **28**, 589-609 (1999).

[3] M. van der Put, F. Ulmer, Differential equations and finite groups. *to appear in J. of Algebra*, preprint available from www.msri.org (1998).

[4] R.H. Risch, The problem of integration in finite terms. *Transactions of the AMS* **139**, 167-189, (1969).

[5] M.F. Singer, F. Ulmer, Liouvillian and algebraic solutions of second and third order linear differential equations. *J. Symb. Comput*, **16**, No. 1, 37-73, (1993).

[6] B.M. Trager, Integration of algebraic functions. Ph.D. thesis, Dept. of EECS, MIT, (1984).