FINDING ALL THE SOLUTIONS OF CYCLIC 9 USING GRÖBNER BASIS TECHNIQUES.

JEAN-CHARLES FAUGÈRE*
LIP6/CNRS Université Paris VI
case 168, 4 pl. Jussieu, F-75252 Paris Cedex 05
E-mail: jcf@calfor.lip6.fr

We show how computer algebra methods based on Gröbner basis computation and implemented in the program FGb enable us to compute all the solution of the Cyclic 9 problem a previously untractable problem. There are one type of infinite solutions of dimension two and 6156 isolated points without multiplicities.

1 Introduction

The main purpose of this paper is to show how today efficient computer algebra programs and algorithms can find *automatically* all cyclic 9-roots [1,2,3]. The title of this paper refer of course to the papers [4,5]. We quote from these papers:

"This paper presents some tricks which may be used when solving a system of algebraic equations which is too complex to be handled directly by a symbolic algebra system". Here the goal is exactly the opposite since we want to use the computer and the programs as black boxes.

In this paper we do not use the symmetry of the problem for computing the solutions but we use the symmetry for the classification of the solutions.

Then Cyclic n problem is (with the convention $x_{n+1} = x_1, x_{n+1} = x_2, \ldots$):

$$(C_n) \qquad (f_1, \ldots, f_{n-1}, f_n = 1) \text{ where } f_i = \sum_{j=1}^{n} \prod_{k=j}^{k+i-1} x_k$$

The Cyclic n has become a standard benchmark for polynomial system solving and has now a long history. We would like to stress the close relationship of some algebraic systems occuring in optimal design of filter banks. Cyclic n can be solved for $n \leq 7$ by the most efficient computer algebra systems, but for $n = 8$ it requires human interaction and software computations [3]. The case $n = 9$ is a very challenging problem because it is

- a non zero dimensional system: we recall that if m^2 divides n then C_n is at least of dimension $m-1$ (see [6,7] and lemma 1.1). So for $n = 9$ we know that C_9 is of dimension at least 2.

- a difficult system: with classical Buchberger algorithm it was impossible to compute a Gröbner basis of C_9 even for a total degree ordering. Very recently we propose a new algorithm for computing Gröbner basis F_4 and it takes 15 days with this algorithm to compute a DRL Gröbner basis. The result request 1.7 Giga bytes on the hard disk. Consequently it is difficult to "solve" completely this problem. By solving, in this paper, we mean give a concise list of solution as in [4,5]. Since the first version of this paper we have developped new algorithms for computing Gröbner bases and it is now possible to solve the Cyclic 10 problem: it is a zero dimensional system of degree 34940. But the Cyclic 9 is still more interesting and in some sense more difficult since it is not zero-dimensional.

The plan of this paper is as follows: in the first section we explain how to obtain a decomposition into irreducible components mainly by using the FGb program and the NTL library. We then provide in the second section a complete classification of all the solutions of Cyclic 9 using the symmetries. The last section contains the classification of the solutions by their multiplicities. We begin by recalling the following lemma (see also [6,7]):

Lemma 1.1 *If m^2 divides n, then the dimension of C_n is at least $m-1$.*

Proof We set $n_1 = m$, and $n_2 = \frac{n}{n_1}$. We choose j to be a n_2 th primitive root of unity (for instance $j = e^{\frac{2i\pi}{n_2}}$), then we claim that

$$S_{n_1,j}(y_0,\ldots,y_{n_1-1}) = (y_0,y_1,\ldots,y_{n_1-1},\ \ jy_0,\ldots,jy_{n_1-1},j^2y_0,\ldots,\\ j^2y_{n_1-1},\ldots,j^{n_2-1}y_0,\ldots,j^{n_2-1}y_{n_1-1})$$

is a solution of cyclic n as soon as $(y_0,\cdots,y_{n_1-1})^{n_2} = 1$. The end of the proof is a simple substitution to check that the original equations are satisfied.

Moreover, in the case $n = 9$, we have found a solution of dimension 2 and degree $2*9 = 18$. □

2 Decomposition into irreducible varieties

Let I be the ideal generated by the equations C_9 and V the associated variety, that is to say the complex roots of C_9.

2.1 General decomposition

Theorem 2.1 *The solutions of Cyclic* 9 *can be decomposed in $V = \cup_{i=1}^{113} V_i$. More precisely, for each variety V_i we have computed a lexicographic Gröbner basis G_i. Moreover all the components are zero dimension except V_i for $i \in \{111,112,113\}$ which are components of dimension* 2 *and degree* 6*.*

index	$1,\ldots,18$	$19,\ldots,36$	$37,\ldots,54$	$55,\ldots,63$
number	18	18	18	9
dimension	0	0	0	0
degree	2	4	12	24
index	$64,\ldots,99$	$100,\ldots,108$	$109,110$	$111,\ldots,113$
number	36	9	2	3
dimension	0	0	0	2
degree	48	216	972	6

that is to say C_9 is a two dimensional variety of degree 18 *with* 6156 *isolated points.*

Proof The proof of this theorem is done by computer algebra. The first and most straightforward method is to use an algorithm for computing such a decomposition (decomposition into primes, triangular systems, ...); unfortunately the size of cyclic 9 (and even cyclic 8) is far beyond the capacities of all the current implementation. For this reason we have developed a new very efficient algorithm called F_7 for computing decomposition into primes of an ideal: the algorithm rely heavily on Gröbner basis [8,9,10,11] computation but try to split the ideal in early stages; with this algorithm, implemented in the Gb [12] and FGb [13] programs, it takes 3 days on a PC Pentium II (400 Mhz with 512 Mega bytes of memory) to compute the decomposition. In view of the fact that this algorithm is not yet published and cannot be described in a short paper we give an alternate (and longer) proof. First we compute a Gröbner basis for a DRL ordering as explained in [14]: it takes 15 days and the size of the result is 1.7 Giga bytes. Then we have to separate the non zero dimensional components: let I be the ideal generated by the equations of Cyclic 9, we can use the known solutions given by lemma 1.1 or use the first polynomials given by F_7:

$$f_1 = x_5x_9 - x_6x_8 \;\; f_2 = x_3 + x_6 + x_9$$

then we can use the decomposition $\sqrt{I} = I_1 \cap I_2 \cap I_3 = \sqrt{I+(f_1,f_2)} \cap \sqrt{(I+(f_1)) : (f_2^\infty)} \cap \sqrt{(I) : (f_1^\infty)}$. Of course there is possibly some redundancy in this decomposition. Computing a lexicographic Gröbner of I_1 is straightforward from the original equation and it is obvious to check that it is exactly the component given by lemma 1.1. In order to compute $I : (f_1^\infty)$ we add a new variable $u > x_1 > \cdots > x_9$ and a new equations $uf_1 = 1$ and we compute a Gröbner for an elimination ordering with u as the first block (about 10 hours). We proceed in the same way for computing $(I+(f_1)) : (f_2^\infty)$ (20 minutes of CPU time). From this first computations we find that I_2 (resp. I_3) is a zero dimensional ideal of degree 469 (resp. 6156). Since we have now only zero dimensional systems we can use standard tools to change the ordering to compute lexicographic Gröbner bases [15,7] of I_2, I_3 (7 hours). Then we use the lextriangular algorithm [16] implemented in Gb to obtain a

decomposition into triangular systems. To find prime components in this decomposition we need to factorize some univariate polynomials: we use the powerful package NTL 5.1 [17]. All the factorization are done easily (less than 10 minutes) except for one polynomial $P(x_9)$ of degree 972 which was untractable (this is a "Swinerton Dyer" example). Very recently a new algorithm [18] was implemented by V. Shoup in NTL and it takes only 32 min 57 sec and 1.3 Giga bytes of memory to factor P on a alpha workstation 500 Mhz. With an even more recent algorithm of M. van Hoeij it takes less than one minute. From this point all the components are in triangular form $\left[x_1^{\alpha_1}+h_1(x_1,\ldots,x_9),\ldots,x_8^{\alpha_8}+h_8(x_8,x_9),h_9(x_9)\right]$ with h_9 an irreducible polynomial. We need now to factorize in algebraic extension: this is done simply by factorizing with NTL a primitive element of each component (fortunately all the components are close to the shape lemma form, that is to say $\sum_{i=1}^{8}\alpha_i$ is small). We have to remove duplicated components which can be very easily done since two identical components have exactly the same lexicographic Gröbner basis. The total time for decomposing the I_2 and I_3 represent less than 20% of the time for computing a DRL Gröbner basis. □

Remark 2.1 *The size of this decomposition in text format is* 2.5 *Mega bytes.*

2.2 Decomposition using the symmetry

For any polynomial p in $x_1,\ldots,x_N$ and any permutation σ, set $\sigma.p = p(x_{\sigma(1)},\ldots,x_{\sigma(N)})$. If F is finite subset, then $\sigma(F)=\{\sigma(v):\ \forall v\in F\}$. In the rest of the paper $\sigma_0=(1,2,3,4,5,6,7,8,9)$ is the cyclic permutation.

Definition 2.1 *A solution $u=(u_1,\ldots,u_9)$ of Cyclic* 9 *is invariant by*

Shift	$\sigma_0 u=(u_9,u_1,\ldots,u_8)$
Mult	*if* $\beta^9=1$, $\beta u=(\beta u_1,\ldots,\beta u_9)$
Association	$\tilde{u}=(u_1u_2,\ldots,u_8u_9,u_9u_1)$
backward	$\leftarrow u=(x_8,x_7,\ldots,x_1,x_9)$
$\uparrow$	$u\uparrow k=(u_1,u_{1+k},u_{1+2k},\ldots,u_{1+8k})$
conjugate	$\overline{u}=(\overline{u_1},\ldots,\overline{u_9})$

We say that u is essentially real if $u=\beta v$ where all the components of v are real numbers and $\beta^9=1$.

Theorem 2.2 *For all $k\in\{1,\ldots,12\}$, for all $i\in\{0,\ldots,8\}$ we have $V_{i+9k-8}=\sigma_0^i V_{9k-8}$ and $\sigma(V_{109})=V_{109}$ and $\sigma(V_{110})=V_{110}$. Moreover G_{9k-8}, G_{109} and G_{110} are in shape lemma form.*

Remark 2.1 *The fact that all the components can be represented by a lexicographic Gröbner basis is a remarkable fact since Cyclic n without decomposition is very far from being shape lemma !*

Proof This is done simply by substituting the variables $x_i \to x_{i+1}$, $x_9 \to x_1$ and recomputing a Gröbner basis: for all G_j we apply the substitution, compute a lexicographic Gröbner basis and then we identify the new component in the list of theorem 2.1. □

In the rest of the paper $G'_k = G_{9k-8}$, $G'_{13} = G_{109}$, $G'_{14} = G_{110}$ and W_k are the corresponding varieties. Since all the G'_k are in shape lemma for we can fix the notation $G'_k = \left[g_9^{(k)}(x_9), x_8 - g_8^{(k)}(x_9), \ldots, x_1 - g_1^{(k)}(x_9)\right]$.

3 Classification of the solutions

We proceed degree by degree beginning with the non zero dimensional and low degree varieties found in theorem 2.2.

3.1 Non zero dimensional components

Since we found only 3 components of dimension 2 and degree 6 it is obvious from lemma 1.1 that $S_{3,j}$ with $j \in \{e^{\frac{2\imath\pi}{3}}, e^{-\frac{2\imath\pi}{3}}\}$ describe all the non zero dimensional components.

Remark 3.1 *The solution* $(1, \alpha, \alpha^2, \ldots, \alpha^8)$ *where* $\alpha^9 = 1$*, which is always a solution of the cyclic n problem, is a member of this infinite component.*

3.2 Degree 2

It is straightforward from the Gröbner basis of G'_1 and G'_2 to identify the following patterns:

$$W_1 = \left(\frac{1}{a}, 1, -\frac{1}{a}, -a, 1, a, \frac{1}{a}, 1, a\right) \text{ with } a^2 + 3a + 1 = 0$$

and

$$W_2 = \left(1, 1, 1, 1, 1, 1, \frac{1}{a}, a\right) \text{ with } a^2 + 7a + 1 = 0$$

3.3 Degree 4

So far we have not used the fact that if $(x_1, \ldots, x_n)$ is a solution then $\beta(x_1, \ldots, x_n) = (\beta x_1, \ldots \beta x_n)$ is also a solution if $\beta^9 = 1$. We define βW to be $\{\beta w \mid w \in W\}$. Since we are working with decomposition into irreducible components we should factorize $\beta^9 - 1 = (\beta - 1)(\beta^2 + \beta + 1)(\beta^6 + \beta^3 + 1)$. For any Gröbner basis G in the list of

theorem 2.1 such that the univariate equation in x_9 is $x_9^2+x_9+1$ or $x_9^6+x_9^3+1$ we introduce new variables $x_1 > \cdots > x_9 > y_1 > \cdots > y_9$ and we add the equations $y_i x_9 = x_1$, $i = 1,\ldots,8$, $y_9 = 1$. Then we compute a lexicographical Gröbner and we take the intersection with $\mathbb{Q}[y_1,\ldots,y_9]$; we note $\frac{G}{x_9}$ the resulting Gröbner basis.

It is straightforward to see that $g_9^{(3)}(x_9) = g_9^{(4)}(x_9) = x_9^2+x_9+1$ (to be fully rigorous we have to search this univariate polynomial in all the Gröbner bases $G_{19},\ldots,G_{36}$). We check that $\frac{G'_3}{x_9} = G'_1$ and that $\frac{G'_4}{x_9} = G'_2$. Consequently there is no new solution of degree 4.

3.4 Degree 12

In exactly the same way we see that $g_9^{(5)}(x_9) = g_9^{(6)}(x_9) = x_9^6+x_9^3+1$, and we check that $\frac{G'_5}{x_9} = G'_2$ and that $\frac{G'_6}{x_9} = G'_1$.

3.5 Degree 24

We study the variety W_7. We have a polynomial $g_9^{(6)}(x_9)$ of degree 24. We compute a DRL Gröbner basis of G'_6 in order to find algebraic relation and we keep only low degree equations:

$$\sum_i x_i = 0, x_2x_3 = 1, x1x_4 = 1, x_6x_8 = 1, x_5x_9 = 1, x_7 = 1$$

We have thus discovered the pattern of this component:

$$(\frac{1}{x_4}, \frac{1}{x_3}, x_3, x_4, \frac{1}{x_9}, \frac{1}{x_8}, 1, x_8, x_9)$$

We can try to simplify $g_9^{(6)}(x_9)$: we remark that $\beta W_7 \subset V$ for $\beta^9 = 1$; from the observation that $\beta^9-1 = (\beta-1)(\beta^2+\beta+1)(\beta^6+\beta^3+1)$ we should find in the decomposition of theorem 2.1 some varieties of degree $2\times 24 = 48$ and $6\times 24 = 144$. Since it is not the case for 144 we conclude that the variety αW_7 for $\alpha^6+\alpha^3+1=0$ is not irreducible, or in other words (since $x_7 = 1$) that the univariate polynomial $g_9^{(6)}(x_9)$ is not irreducible over $\mathbb{Q}(\alpha)$. We add a new variable α and the equation $\alpha^6+\alpha^3+1=0$ to G'_6 and we decompose the resulting variety $\tilde{W}_6$ in $U_1\cup U_2\cup U_3$. All the U_i are of degree 48. We can keep only one factor, say U_1 and we find

$$\begin{aligned} g_9^{(6)} = {} & {x_9}^8 + \left(5\alpha^2+2-5\alpha+5\alpha^5\right){x_9}^7 + \left(-20\alpha^2-15\alpha^5-22+20\alpha+5\alpha^4\right){x_9}^6 + \\ & \left(-15\alpha+15\alpha^2+9+5\alpha^5-10\alpha^4\right){x_9}^5 + \left(5-10\alpha-10\alpha^4+10\alpha^2\right){x_9}^4 \\ & + \left(-15\alpha+15\alpha^2+9+5\alpha^5-10\alpha^4\right){x_9}^3 + \left(-20\alpha^2-15\alpha^5-22+20\alpha+5\alpha^4\right){x_9}^2 \\ & + \left(5\alpha^2+2-5\alpha+5\alpha^5\right)x_9 + 1 = 0 \end{aligned}$$

This representation of the solutions is not satisfactory since $degree(W_7) = 24$ and we have now 48 solutions. We remark that the coefficient of x_9^7 can be rewritten $5\alpha^2+2-5\alpha+5\alpha^5 = 2-5\left(\alpha+\frac{1}{\alpha}\right)$ and similarly for the other coefficients. Thus $g_9^{(6)}$ is invariant if replace α by $\bar{\alpha}$ the complex conjugate of α. So we replace $\mathbb{Q}(\alpha)$ by $\mathbb{Q}(\gamma)$ where γ is a root of the minimum polynomial of $\alpha+\frac{1}{\alpha} = cos(\alpha) = cos(\frac{2\pi}{9})$ (hence γ is a root of $8x^3-6x+1 = (x-cos(\frac{2\pi}{9}))(x-cos(\frac{4\pi}{9}))(x-cos(\frac{8\pi}{9}))$). We note also that $g_9^{(6)}$ is a self reciprocal polynomial and we add the new variable $c(x_i) = x_i+\frac{1}{x_i}$ and $s(x_i) = x_i-\frac{1}{x_i}$. We recompute a new decomposition in 3 varieties of degree 24 and we found:

$H(x_9) = c(x_9)^4 + \left(20\gamma^2+10\gamma-8\right)c(x_9)^3 + \left(-60\gamma^2-40\gamma+4\right)c(x_9)^2 + \left(-40\gamma^2+23\right)c(x_9)+120\gamma^2+100\gamma-9 = 0$

the next equation is $c(x_9)^2 - s(x_9)^2 = 4$ and for all the other variables $i \in \{1,2,3,4,5,6,8\}$ we introduce in the same way $c(x_i) = P_i(c(x_9),\gamma)$, $s(x_i) = Q_i(s(x_9),\gamma)$. We give P_8:

$3924989c(x_8) = -2339596\,c(x_9)^3\gamma^2 - 2784\,c(x_9)^3\gamma + 1252564\,c(x_9)^3 + 3678516\,c(x_9)^2\gamma^2 - 2271060\,c(x_9)^2\gamma - 2028597\,c(x_9)^2 + 36734620\,c(x_9)\gamma^2 + 6538322\,c(x_9)\gamma - 23201914\,c(x_9) + 20909524\,\gamma^2 + 8944278\,\gamma - 17802043$

For all $\gamma = cos(\frac{2^k\pi}{9})$ and $k \in \{1,2,3\}$ we check that $H(c(x_9))$ has four real roots $c(x_9) = r_j^{(k)}$: $-2 < r_1^{(k)} < r_2^{(k)} < 2$ and $2 < |r_3^{(k)}| < |r_4^{(k)}|$ and we can compute $s(x_9) = \pm\sqrt{c(x_9)^2-4}$ and we find two real roots when $j = 3,4$ and two complex roots of modulus one when $j = 1,2$. In the first case it is obvious (since we have a shape lemma form) that all the other coordinates are reals. In the second case we check (numerically for instance) that all the other coordinates are also of modulus one.

For the pattern $(\frac{1}{x_4},\frac{1}{x_3},x_3,x_4,\frac{1}{x_9},\frac{1}{x_8},1,x_8,x_9)$ it is obvious that the length of the association is 3.

3.6 Degree 48

W_8 can be represented by one of the Gröbner basis $G_{48},\ldots,G_{56}$; among these Gröbner bases we find one, say G'_8, such that the univariate polynomial is $x_9^6+x_9^3+1$. We compute $\frac{G'_8}{x_9}$ and we find G'_7. (since the direct computation of the lexicographical Gröbner basis is a little more difficult we can first change the ordering of G'_8 from lexicographical to DRL with the algorithm F_2 or FGLM, then add new variables and the new equations, compute a DRL Gröbner and finally change the ordering again to obtain a lexicographical Gröbner basis). In exactly the same way we find $\frac{G'_9}{x_9} = \frac{G'_{10}}{x_9} = G'_7$. We find also $\frac{G'_{11}}{x_9} = G'_7$ with the polynomial $x_9^2+x_9+1$. There is no new solution of degree 48.

3.7 Degree 216

The study of W_{12} is much more difficult: first we compute a DRL Gröbner but we do not find interesting algebraic relation of small degree. We know from theorem 2.2 that W_{12} can be represented by $G_{100}, \ldots, G_{108}$, so that (up to renumbering) $V_{100+i} = \sigma_0^i V_{100}$. It is easy to show by computation that we have also

$$e^{\frac{2k\pi}{9}} V_{100} = V_{101+k} \quad k \in \{1,\ldots,8\}$$

Since it is not possible to find patterns as usual it is necessary to give a name to all the roots of $g^{(12)}(x_9)$ (all the roots are complex): $z_1, \ldots, z_{216}$ (the choice of the indices is arbitrary).

By inspecting the Gröbner basis we remark that the univariate polynomial (the unknown is x_9) in G_{100} and in $G_{103} = \sigma_0^4 G_{100}$ are the same; we conclude immediately that there exists a permutation α of $\{1,\ldots,216\}$ such that $(x_1,x_2,x_3,z_{\alpha(k)},x_5,x_6,x_7,x_8,z_k) \in W_{12}$ for $k \in \{1,\ldots,216\}$. Moreover we can deduce that all the other univariate polynomials have the same roots than $g^{(12)}(x_9)$ multiplied by some $e^{\frac{2k\pi}{9}}$. With the help of the mpsSolve [19] program we can compute all the complex roots of $g^{(12)}(x_9)$ with guaranteed numerical approximation (we take 100 digits), then plug in these values in the other coordinates; we can identify the value of k for each coordinate of W_{12}:

$$\left(z_{\sigma_1(k)}e^{\frac{\pm 2\pi}{3}}, z_{\sigma_2(k)}e^{\frac{\pm 4\pi}{9}}, z_{\sigma_3(k)}e^{\frac{\pm 2\pi}{3}}, z_{\sigma_4(k)},\right.$$
$$\left. z_{\sigma_5(k)}e^{\frac{\pm 8\pi}{9}}, z_{\sigma_6(k)}e^{\frac{\pm 4\pi}{9}}, z_{\sigma_7(k)}e^{\frac{\pm 2\pi}{3}}, z_{\sigma_8(k)}e^{\frac{\pm 8\pi}{9}}, z_k\right)$$

where all the σ_j are permutations of $\{1,\ldots,216\}$. It is also possible to represent x_1,x_2,x_3,x_5 and x_8 as a product of two roots $z_{i_1}z_{i_2}$ and x_6,x_7 as a product of 3 roots $z_{j_1}z_{j_2}z_{j_3}$. Describing in a better way these permutations is still an open issue.

3.8 Degree 972

At first glance it may seem surprising that we have only two components of degree 972. But by theorem 2.2 we know that $\sigma_0 W_{13} = W_{13}$ so that all the univariate in all the variables $x_1, \ldots, x_9$ are the same. We deduce that all the coordinates $x_1,\ldots,x_9$ are permutations of the same set of roots. In G'_{13} and G'_{14} we remark that $g_i^{(13)}(x_9) = g_{9-i}^{(14)}(x_9)$ for $i \in \{1,\ldots,8\}$, so that if $(x_1,\ldots,x_9) \in W_{13}$ then $\leftarrow x = (x_8,\ldots,x_1,x_9) \in W_{14}$ (read backward the solution) or with our notations $\sigma' W_{13} = W_{14}$ with $\sigma' = (9,8,7,6,5,4,3,2,1)$. The invariance by multiplication by a

9th root of unity is obvious since $g_9^{(13)}(x_9) = P_{108}(x_9^9)$ where P_{108} is an irreducible and self reciprocal polynomial of degree 108 and $g_i^{(13)}(x_9) = x_9 Q_i(x_9^9)$ for $i \in \{1,\ldots,8\}$.

It is possible to simplify the expression of P_{108}: since all the coordinates have the same minimal polynomial we introduce a new variable E (we choose the ordering $x_1 > \cdots > x_9 > E$) and a new equation $E - e_2$ where $e_2 = x_1x_2 + \cdots$ is the elementary symmetric function of degree 2 in $x_1,\ldots,x_9$. We compute a new lexicographical Gröbner basis and find a univariate polynomial in E, $Q_{12}(E^9)$.

$$Q_{12}(X) = X^{12} + 660115591173034905 6X^{11} + \cdots$$

Following a suggestion of D. Lazard [20], it is even possible to split the field defined by Q_{12} using the program Kant [21] through the Magma [22] interface: let u,v be two new variables then we have a polynomial in u,v,E of degree 2 in E, a polynomial in u,v of degree 3 in u and a univariate polynomial of degree 2 in v.

We can separate the roots of P_{108} in two sets of same size: $r_1 < \cdots < r_{54}$ the real roots, and $\{z_1,\ldots,z_{54}\}$ the complex roots. Let

$$R_1 = (r_1, r_{30}, r_{54}, r_{25}, r_9, r_{23}, r_{11}, r_{40}, r_{21})$$

we compute from this solution $R_{i+1} = \tilde{R}_i \uparrow 2$. We check that:

- all the coordinates of $R_1,\ldots,R_6$ are all the real roots of P_{108}.
- $R_1,\ldots,R_6$ are in W_{13}
- $\left\{\sigma_0^i e^{\frac{2j\pi}{9}} R_k \,|i,j \in \{1,\ldots,9\}\ k \in \{1,\ldots,6\}\right\}$ are all the 486 essentially real solutions of W_{13}.

We study now the complex solutions: let $\{u_1,\bar{u_1},u_2,\bar{u_2},u_3,\bar{u_3}\}$ be the subset of $\{z_1,\ldots,z_{54}\}$, the complex roots of modulus one. For the complex solutions the pattern of W_{13} is

$$\left(|x_1| = 1, \frac{1}{\bar{x_9}}, \frac{1}{\bar{x_8}}, \frac{1}{\bar{x_7}}, \frac{1}{\bar{x_6}}, x_6, x_7, x_8, x_9\right)$$

If C_i is the solution corresponding to $x_1 = u_i$, $i = 1,2,3$, we set $C = \left\{\sigma_0^i e^{\frac{2j\pi}{9}} C_k \,|i,j \in \{1,\ldots,9\}\ k \in \{1,2,3\}\right\}$; all the 486 complex solutions are obtained by taking C and $\bar{C}$ the complex conjugates.

3.9 Number of solutions with multiplicities

The calculations we have done up to now have only taken into account the algebraic *variety* and not the ideal itself. So we have lost the multiplicities of the solutions. In this section we will prove that there are 6642 isolated points with multiplicities. All the computations are independant of the other sections so it is also a way to check the results.

Proposition 3.1 *Let I an ideal and g a polynomial. If $I : g^s = I : g^{s+1} = I : g^\infty$ then*

$$I = (I + (g^s)) \cap (I : g^s)$$

Further inspection of the $S_{3,j}$ components (dimension 2) reveals the fact that $x_3 + x_6 + x_9$ is a an invariant. (This polynomial was also used in the proof of theorem 2.1). So we take $g_0 = x_3 + x_6 + x_9$ and $I = (f_1, \ldots, f_8, f_9 - 1)$ the original system of equations.

We first compute the ideal quotient $(I : g_0)$ by the standard algorithm (see [11] p. 195). We found an ideal of dimension 0 and degree 6642. Then we compute $I : g_0^\infty$ by computing $(I + (1 - t * g_0)) \cap k[x_1, \ldots, x_9]$ (see [11] ex 8) and we found also an ideal of dimension 0 and degree 6642. So we conclude that in our case

$$(I : g_0) = (I : g_0^\infty) \text{ and} I = (I : g_0) \cap (I + (g_0))$$

The computation of $(I + (g_0))$ is so simple that we obtain immediately a decomposition in 3 components of dimension 2.

The other part $I_1 = (I : g_0^\infty)$ is more difficult and we sketch the proof: we introduce a new variable t and the new ideal $I_2 = I_1 + (t - \sum_{i=1}^{9} i x_i)$. We compute $J_2 = I_2 \cap \mathbb{Q}[x_9, t]$ and we check that J_2 is still a zero dimensional ideal of degree 6642 (in other words $x_i = H_i(x_9, t)$ where H_i is a bivariate polynomial, $i = 1, \ldots, 8$). We compute a lexicographical Gröbner basis of J_2 and we found

$$J_2 = \left(x_9^2 + \ldots, U^2(t)(x_9 + \ldots), U^2(t)V(t)\right)$$

where U and V are square-free univariate polynomials (moreover $gcd(U, V) = 1$). V is of degree 5994 and U of degree 162. We use the fast Primary Decomposition algorithm [23] for two variables:

$$J_2 = (x_9 + \ldots, V(t)) \cap \left((x_9 + \ldots)^2, U^2(t)\right)$$

Theorem 3.1 *The number of isolated points of the Cyclic 9 problem*

5994	*solutions of multiplicity 1*
162	*solutions of multiplicity 4*
*6642=5994+4*162*	*all solutions with multiplicities*
6156=5994+162	*all solutions without multiplicities*

3.10 Summary of the results

Theorem 3.2 *If V is a variety, set $\sigma_0 = (1,2,3,4,5,6,7,8,9)$, $\sigma' = \sigma_0^{-1}$, $\mathscr{O}(V) = \{\sigma_0^j V \mid j = 0,\ldots,8\}$ and $\mathscr{O}'(V) = \{e^{\frac{2j\imath\pi}{9}} V \mid j = 0,\ldots,8\}$ then the set $V_{Cyclic\ 9}$ of all the complex solutions of cyclic 9 can be written as:*

$$V_{Cyclic\ 9} = \mathscr{O}'(\mathscr{O}(W_1 \cup W_2 \cup W_7)) \cup \mathscr{O}(W_{12}) \cup W_{13} \cup \sigma'(W_{13}) \cup S_{3,e^{\frac{2\imath\pi}{3}}}$$

and the number of isolated points is $9.9.(2+2+24)+9.216+2.972 = 6156$*. The number of isolated with multiplicities is 6642.*

Remark 3.2 *The size of $W_1 \cup W_2 \cup W_7 \cup W_{12} \cup W_{13}$ is* 379 *kbytes.*

4 Conclusion

We have presented an automatic method based on Gröbner basis computations for solving the Cyclic 9 problem. Thanks to this systematic approach we can classify *all* the solutions and removing the well known symmetries. This paper shows also that it is now possible to compute a decomposition into primes for a very difficult example. Using completely the symmetries to describe more easily the biggest components is still an open issue. How to use the symmetries to solve efficiently such a problem remains also a challenging problem.

References

1. G. Björk. In *Proceedings of Alfred Haar Memorial Conference, Budapest, Colloquia Mathematica Societatis János Bolyai*, 49, pages 193–197, 1985.
2. G. Björk. In J.S. Byrnes and J.F. Byrnes, editor, *Recent Advances in Fourier Analysis and its Applications*, volume 315 of *Ser. C: Math. Phys. Sci., Kluwer*, pages 131–140. NATO Adv. Sci. Inst., 1989.
3. G. Björck and G. Fröberg. *Journal of Symbolic Computation, 12(3):329–336, September 1991.*
4. *J. Backelin and R. Fröberg In S. M. Watt, editor,* ISSAC' 91, *pages 103–111. ACM, July 1991.*
5. *G. Björk and R. Fröberg. preprint 1993, 1993.*

6. *J. Backelin Technical Report 8, Reports Matematiska Institutionen, Stockholms Universitet, 1989.*
7. *J.C. Faugère PhD thesis, Université Paris 6, Feb. 1994.*
8. *B. Buchberger PhD thesis, Innsbruck, 1965.*
9. *B. Buchberger* Aequationes Mathematicae, 4(3):374–383, 1970. (German).
10. B. Buchberger In *Proc. EUROSAM 79*, volume 72 of *Lect. Notes in Comp. Sci.*, pages 3–21. Springer Verlag, 1979.
11. D. Cox, J. Little, and D. O'Shea. Springer Verlag, New York, 1992.
12. J.C. Faugère `http://calfor.lip6.fr/~jcf`.
13. J.C. Faugère `https://calfor.lip6.fr/`.
14. J.C. Faugère *Journal of Pure and Applied Algebra, 139(1–3):61–88, June 1999.*
15. *J.C. Faugère, P. Gianni, D. Lazard, and T. Mora.* Journal of Symbolic Computation, 16(4):329–344, October 1993.
16. D. Lazard. *Journal of Symbolic Computation, 13(2):117–132, February 1992.*
17. *V. Shoup.* `http://www.shoup.net/ntl`.
18. *J. Abbott, V. Shoup, and P. Zimmermann. Issac 2000.*
19. *D. Bini and G. Fiorentino. Technical report, University of Pisa, 1999.*
20. *D. Lazard and A. Valibouze.* Progress in Mathematics, 109:163–176, 1992.
21. M. E. Pohst. Technical report, Technische Universitaet Berlin, 1998.
22. J. Cannon `http://www.maths.usyd.edu.au:8000/u/magma/`.
23. D. Lazard *Journal of Symbolic Computation, 3(1):261–270, September 1985.*