How my computer find all the solutions of Cyclic 9

Jean-Charles Faugère[1]
LIP6/CNRS Université Paris VI
case 168, 4 pl. Jussieu, F-75252 Paris Cedex 05
E-mail: jcf@calfor.lip6.fr
January 31, 2000

Abstract

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.

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 [6, 7, 5]. The title of this paper refer of course to the papers [3, 8]. We quote from this 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 idea is exactly the opposite since we want to use the computer and the program as black boxex[1] to find all the solutions.

In this paper we do not use the symmetry of the problem for computing the solutions (even if we give a trick at the end of the paper to speed up the computation and to reduce the number of solutions by 9). We use the symmetry for the classification of the solutions.

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 hand and software computations [5]. 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 [2, 16] 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 [3, 8].

[1] We will see that it is almost the case in our program, since we have to give a hint to the NTL in order to be able to factorize a big univariate polynomial.

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 a little trick to reduce the number of solutions. We begin by recalling the following lemma (see also [2, 16]):

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

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

is a solution of cyclic n as soon as $(y_0,\cdots,y_{n_1-1})^{n_2} = 1$. We are doing the proof only in the case $n=9$. We set

$\{x_1 = y_0, x_4 = jy_0, x_7 = j^2y_0, x_2 = y_1, x_5 = jy_1, x_8 = j^2y_1, x_3 = y_2, x_6 = jy_2, x_9 = j^2y_2\}$

and all the equations of cyclic 9 can be rewritten $y_0{}^3y_1{}^3y_2{}^3j^9 - 1 = 0$
$j^7(j^2+j+1)y_0{}^2y_1{}^2y_2{}^2(y_1\,y_2 + y_2\,y_0 + y_0\,y_1) = 0$
$j^5(j^2+j+1)y_0{}^2y_1{}^2y_2{}^2(j^2y_2 + j^2y_0 - jy_2 + jy_1 - jy_0 + y_2 + y_0) = 0$
$y_0{}^2y_1{}^2y_2{}^2j^3(j^2-j+1)(j^2+j+1)^2 = 0$
$j^2(j^2+j+1)y_0\,y_1\,y_2\quad(j^4y_1\,y_2 - y_1\,y_2\,j^3 + j^3y_2\,y_0 + j^3y_0\,y_1 - y_0\,j^2y_2 + y_1\,y_2\,j + y_2\,jy_0 - jy_0\,y_1 + y_0\,y_1) = 0$
$j(j^2+j+1)y_0\,y_1\,y_2\,(j^4y_2 - y_2\,j^3 + j^3y_1 + j^3y_0 - j^2y_1 + jy_2 + jy_1 - jy_0 + y_0) = 0$
$y_0\,y_1\,y_2\,(j^2-j+1)(j^2+j+1)^2 = 0$
$(j^2+j+1)(j^2y_0\,y_1 + j^2y_1\,y_2 + y_2\,jy_0 - jy_0\,y_1 - y_1\,y_2\,j + y_0\,y_1 + y_1\,y_2) = 0$
$(j^2+j+1)(y_0+y_1+y_2) = 0$

and since $j^2+j+1=0$ all the equations are equal to zero. Moreover, in the case $n=9$, we have found a solution of dimension 2 and degree $2*9=18$ $\square$

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 *We have the following decomposition into irreducible varieties:*

$$V = \cup_{i=1}^{113} V_i$$

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	$1, \dots, 18$	$19, \dots, 36$	$37, \dots, 54$
number	18	18	18
dimension	0	0	0
degree	2	4	12
index	$55, \dots, 63$	$64, \dots, 99$	$100, \dots, 108$
number	9	36	9
dimension	0	0	0
degree	24	48	216
index	$109, 110$	$111, \dots, 113$	
number	2	3	
dimension	0	2	
degree	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 [9, 10, 11, 13] computation but try to split the ideal in early stages; with this algorithm implemented in the Gb [15] and FGb [14] 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 such a paper we give an alternate (and longer) proof. First we compute a Gröbner basis for a DRL ordering as explained in [17]: it takes 15 days and the size of the result is 1.6 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:

$$f_1 = x_5 x_9 - x_6 x_8$$

$$f_2 = x_3 + x_6 + x_9$$

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 $u f_1 = 1$ 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 [18, 16] of I_2, I_3 (7 hours). Then we use the lextriangular algorithm [19] 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 3.7a [22]. 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 [1] 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 (we have to set *manually* a pruning parameter to 30 which is an upper bound of the maximum size of allocable memory). From this point all the components are in triangular form $[x_1^{\alpha_1} + h_1(x_1, \ldots, x_9), \ldots, x_8^{\alpha_8} + h_8(x_8, x_9), h_9(x_9)]$ 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 (see figure 3.9 to see all the components a this step) 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. $\square$

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

2.2 Decomposition with 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.

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. $\square$

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 amd 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

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

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_6. 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:

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

We can try to simplify $g_9^{(6)}(x_9)$: we remark that $\beta W_6 \subset V$ 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_6 for $\alpha^6 + \alpha^3 + 1 = 0$ is not irreducible, or in other words (since $x_7 = 1$) that the univariate polynomia $g_9^{(6)}(x_9)$ 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 in $\tilde{W}_6$ 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

$g_9^{(6)} = {x_9}^8 + (5\,\alpha^2 + 2 - 5\,\alpha + 5\,\alpha^5)\,{x_9}^7 + (-20\,\alpha^2 - 15\,\alpha^5 - 22 + 20\,\alpha + 5\,\alpha^4)\,{x_9}^6 + (-15\,\alpha + 15\,\alpha^2 + 9 + 5\,\alpha^5 - 10\,\alpha^4)\,{x_9}^5 + (5 - 10\,\alpha - 10\,\alpha^4 + 10\,\alpha^2)\,{x_9}^4$
$+ (-15\,\alpha + 15\,\alpha^2 + 9 + 5\,\alpha^5 - 10\,\alpha^4)\,{x_9}^3 + (-20\,\alpha^2 - 15\,\alpha^5 - 22 + 20\,\alpha + 5\,\alpha^4)\,{x_9}^2$
$+ (5\,\alpha^2 + 2 - 5\,\alpha + 5\,\alpha^5)\,x_9 + 1 = 0$

This representation of the solutions is not satisfactory since $degree(W_6) = 24$ 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 the minimum polynmial of $\alpha + \frac{1}{\alpha} = cos(\alpha) = cos(\frac{2\Pi}{9})$ (we have $8\gamma^3 - 6\gamma + 1 = 0$). 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 find:

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

the next equation is $c(x_9)^2 - s(x_9)^2 = 4$ and for all the other variables $i \in \{1, 2, 3, 4, 5, 6, 8\}$:

$$c(x_i) = P_i(c(x_9), \gamma)$$
$$s(x_i) = Q_i(s(x_9), \gamma)$$

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 $k \in \{0, 1, 2\}$ 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 check we check (numerically for instance) that all the other coordinates are also of modulus one and that we have the following pattern:

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

and there is no simple algebraic relation between the coordinates.

3.6 Degree 48

W_8 can be represented by one of the Gröbner basis $G_{48}, \dots, G_{56}$; 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 re-change the ordering 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 $G_{100}, \dots, G_{108}$, so that (up to renumbering) $V_{100+i} = \sigma_0^i V_{100}$. It is easy to show by computation that we have also

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

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): $z_1, \dots, z_{216}$ (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 $\{1, \dots, 216\}$ 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 $k \in \{1, \dots, 216\}$. 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 [4] 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}:

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

where all the σ_j are permutations of $\{1, \dots, 216\}$. 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 $(x_8, \ldots, x_1, x_9) \in W_{14}$ (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 $e_2 = x_1 x_2 + \cdots$ 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, $Q_{12}(E^9)$.

$Q_{12}(X) = X^{12}+6601155911730349056*X^{11}+29509519705111019942761001003148 9024*$
$X^{10}+22317522260425598367751293884805188830675828368998 4*X^9+52900128306765472092306656192394103026078509206804716588650987520*$
$X^8+1458793789079151930936248787101923067322412426838691911392143222286991684429414 4*$
$X^7-5442412131282622518914473166074019012331571163477990623299833355255725905738207617905747558 4*$
$X^6+556995631580569608834273566053172862969357839767615486913701422976473836560588061262734276846290364006 40*$
$X^5+2022865343696074837066188639312366450285700556782449921249866722159868666244986649436734924349331571807383952902062 08*$
$X^4+28132546576169839092828405477951714462242418545635642328154033829639630974190861186943953456812164458421275886092871498150707 20*$
$X^3+1046149309680490605185534154073983943647351973760193228691739149829943901833042238004611620363427110250337654087110951726107066515639500 8*$
$X^2+5101218322392121114052691308942811294877407843752132037795445301069423393019471729861117525028566307719644945365075205146053613966717676005883904*$
$X+249965998746713928460073092555398531952626975758253259960803642413979543815136010894364196888749886787183257143407812679369602688685366791530086400 0000000$

Following a suggestion of D. Lazard [20], it is even possible to split the field defined by $Q_1 2$ using the program Kant [21] through the Magma [12] 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. We define first two new operators:

Definition 3.1 *If* $x = (x_1, \ldots, x_9)$ *then*

$$x \uparrow k = (x_1, x_{1+(k \; mod \; 9)}, \ldots, x_{1+((8k) \; mod \; 9)})$$

and

$$\tilde{x} = (x_1 x_2, \ldots, x_8 x_9, x_9 x_1)$$

Wet set

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

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}
- $\left\{\sigma_0^i e^{\frac{2j\pi}{9}} R_k \mid i, j \in \{1, \ldots, 9\}\ k \in \{1, \ldots, 6\}\right\}$ 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 $C = \left\{\sigma_0^i e^{\frac{2j\pi}{9}} C_k \mid i, j \in \{1, \ldots, 9\}\ k \in \{1, 2, 3\}\right\}$; all the 486 complex solutions are obtained by taking C and $\bar{C}$ the complex conjugates.

3.9 Summary of the results

Theorem 3.1 *If V is a variety, set $\sigma_0 = (1, 2, 3, 4, 5, 6, 7, 8, 9)$, $\sigma' = \sigma_0^{-1}$, $\mathcal{O}(V) = \{\sigma_0^j V \mid j = 0, \ldots, 8\}$ and $\mathcal{O}'(V) = \{e^{\frac{2j\imath\pi}{9}} V \mid j = 0, \ldots, 8\}$ then*

$$V\mathcal{O}'(\mathcal{O}(W_1 \cup W_2 \cup W_6)) \cup \mathcal{O}(W_{12}) \cup W_{13} \cup \sigma'(W_{13}) \cup S_{3,e^{2\imath\pi}3}$$

and the number of isolated points is $9.9.(2 + 2 + 24) + 9.216 + 2.972 = 6156$.

Remark 3.2 *The size of $W_1 \cup W_2 \cup W_6 \cup W_{12} \cup W_{13}$ is 379 kbytes.*

4 Use of an elementary trick

If it is not easy to use fully the symmetry in the cyclic n problem but it is possible to divide the number of solutions by n and to reduce significantly the CPU time: we remark that the system defining cyclic n is homogeneous if we remove the equation $x_1 \cdots x_n = 1$. We introduce new variable $y_i = \frac{x_i}{x_9}$ for $i = 1, \ldots, 8$ and we divide the ith equation by x_9^i:

$$\tilde{C}_9 \left\{ \begin{array}{l} y_1 + \cdots + y_8 + 1 = 0 \\ \cdots \\ y_1y_2y_3y_4y_5y_6y_7y_8 + y_1y_2y_3y_4y_5y_6y_7 \\ \quad +y_1y_2y_3y_4y_5y_6y_8 + \cdots = 0 \end{array} \right.$$

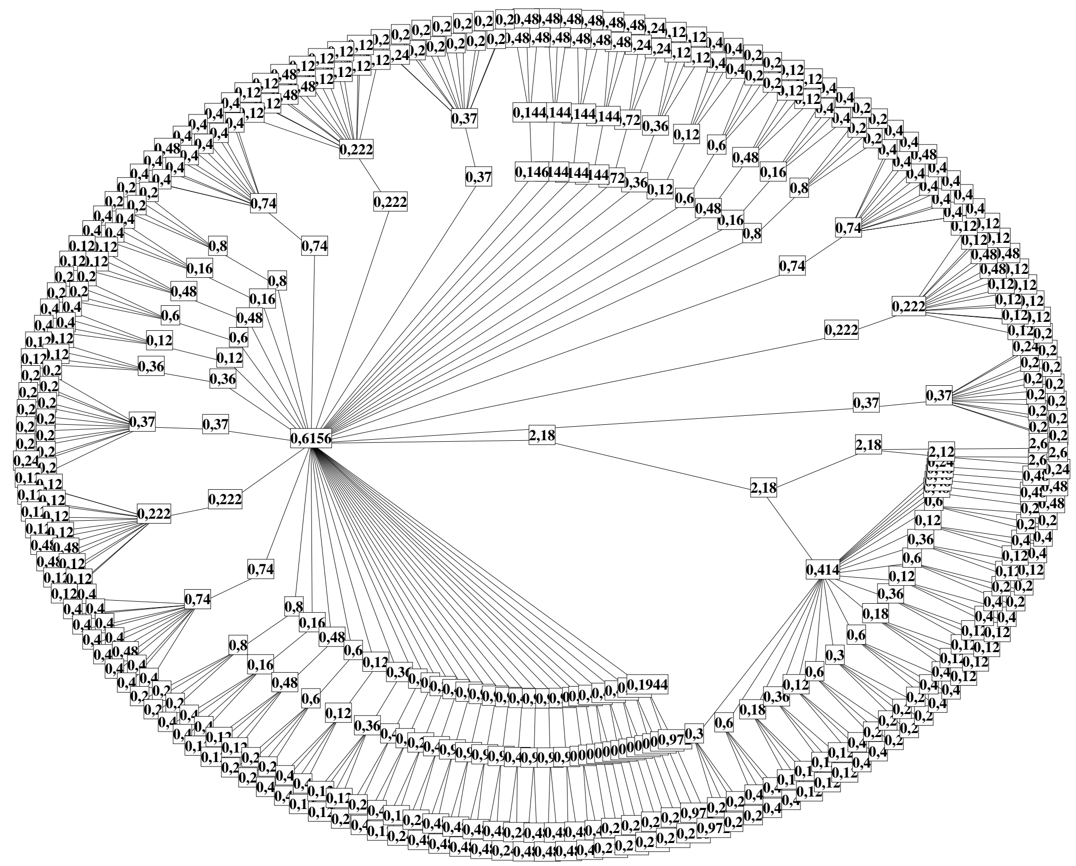

Figure 1: decomposition into primes; $\boxed{\text{d,D}}$ means a component of dimension d and degree D.

We must add another equation to specify that $y_i \neq 0$. The trick consists in adding a new variable and adding the equation of low degree

$$uy_5y_6y_7y_8 = 1$$

With this trick we divide the computation time by 2 or 3 and divide the number of solutions by 9 (experimentations on a PC Pentium II 400 Mhz).

	C_8	$\tilde{C}_8$	C_9	$\tilde{C}_9$
F_7	463.9 s	150.9 s	3 days	1.5 days

5 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 an open question.

Acknowledgement I greatly appreciate that I had access to the computers of UMS Medicis 658 and I want to express my appreciation to Joël Marchand. I am deeply indebted to Paul Zimmermann and Victor Shoup for factoring the big polynomial of degree 972.

References

[1] ABBOTT, J., SHOUP, V., AND ZIMMERMANN, P. Factorization in $\mathbb{Z}[x]$: The Searching Phase. submitted to Issac 2000, 2000.

[2] BACKELIN J. Square multiples n give infinitely many cyclic n–roots. Tech. Rep. 8, Reports Matematiska Institutionen, Stockholms Universitet, 1989.

[3] BACKELIN J. AND FRÖBERG R. How we proved that there are exactly 924 cyclic 7-roots. In *ISSAC' 91* (July 1991), S. M. Watt, Ed., ACM, pp. 103–111.

[4] BINI, D., AND FIORENTINO, G. Mpsolve. Tech. rep., University of Pisa, 1999.

[5] BJÖRCK, G., AND FRÖBERG, G. A faster way to count the solution of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots. *Journal of Symbolic Computation 12*, 3 (September 1991), 329–336.

[6] BJÖRK, G. Functions of modulus one on $\mathbf{Z}_p$ whose Fourier transforms have constant modulus. In *Proceedings of Alfred Haar Memorial Conference, Budapest, Colloquia Mathematica Societatis János Bolyai* (1985), 49, pp. 193–197.

[7] BJÖRK, G. Functions of modulus 1 on $\mathbf{Z}_n$, whose Fourier transforms have constant modulus, and "cyclic n-roots". In *Recent Advances in Fourier Analysis and its Applications*, J.S. Byrnes and J.F. Byrnes, Ed., vol. 315 of *Ser. C: Math. Phys. Sci., Kluwer*. NATO Adv. Sci. Inst., 1989, pp. 131–140.

[8] BJÖRK, G., AND FRÖBERG. Methods to "divide out" certain solutions from systems of algebraic equations, applied to find all cyclic 8-roots. preprint 1993, 1993.

[9] BUCHBERGER B. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* PhD thesis, Innsbruck, 1965.

[10] BUCHBERGER B. An Algorithmical Criterion for the Solvability of Algebraic Systems. *Aequationes Mathematicae 4*, 3 (1970), 374–383. (German).

[11] BUCHBERGER B. A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner Basis. In *Proc. EUROSAM 79* (1979), vol. 72 of *Lect. Notes in Comp. Sci.*, Springer Verlag, pp. 3–21.

[12] CANNON J. *The Magma Computational Algebra System 2.20-7*, Feb 1998. `http://www.maths.usyd.edu.au:8000/u/magma/`.

[13] COX, D., LITTLE, J., AND O'SHEA, D. *Ideals, Varieties and Algorithms*. Springer Verlag, New York, 1992.

[14] FAUGÈRE J.C. *FGb a software for solving polynomial systems.* `https://fgb.medicis.polytechnique.fr/`.

[15] FAUGÈRE J.C. *On line documentation of Gb*. avalaible on the WEB `http://calfor.lip6.fr/˜jcf`.

[16] FAUGÈRE J.C. *Résolution des systèmes d'équations algébriques*. PhD thesis, Université Paris 6, Feb. 1994.

[17] FAUGÈRE J.C. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra 139*, 1–3 (June 1999), 61–88.

[18] FAUGÈRE, J.C., GIANNI, P., LAZARD, D. AND MORA T. Efficient Computation of Zero-Dimensional Gröbner Basis by Change of Ordering. *Journal of Symbolic Computation 16*, 4 (October 1993), 329–344.

[19] LAZARD, D. Solving zero-dimensional algebraic systems. *Journal of Symbolic Computation 13*, 2 (February 1992), 117–132. available by anonymous ftp posso.lip6.fr.

[20] LAZARD, D., AND VALIBOUZE, A. Computing subfields: reverse of the primitive element problem. *Progress in Mathematics 109* (1992), 163–176.

[21] POHST, M. E. Kant v4 software version 1.9. Tech. rep., Technische Universitaet Berlin, 1998.

[22] SHOUP, V. *NTL 3.7 a, a Library for doing Number Theory*, 1999. `http://www.shoup.net/ntl`.