Bull. Math. Soc. Sci. Math. Roumanie
Tome 58(106) No. 2, 2015, 199–209

Scheme of cyclic 9-roots. A heuristic numerical-symbolic approach

by
Rostam Sabeti

Abstract

In this paper, a new heuristic symbolic-numerical method to derive exact form of the generators of the ideals in minimal prime decomposition of the radical of an ideal is presented. We set up the method without monodromy grouping. Application of the method on cyclic 9-roots polynomial system is given. A proof of the primality of the ideals is presented. Among many proved results, we also consider the residue class field of a typical prime ideal as the collection of well defined quotient of the elements in the direct sum $\bigoplus_{i=7}^{9} x_i\mathbb{C}[x_i] \oplus \eta\mathbb{C}[x_7, x_8] \oplus \delta\mathbb{C}[x_8, x_9] \oplus \sigma\mathbb{C}[x_7, x_9] \oplus \mathbb{C}$, where $\eta = x_7x_8$, $\delta = x_8x_9$ and $\sigma = x_7x_9$.

Key Words: Computational algebraic geometry, components of solutions, irreducible decomposition, symbolic-numerical algorithm, cyclic n-roots.
2010 Mathematics Subject Classification: Primary 14Q15, Secondary 65H10, 68W30, 13P05.

1 Introduction

Suppose $n \geq 3$ is an integer and $R = \mathbb{C}[x_1, \cdots, x_n]$ be the ring of polynomials in n variables $x_1, \cdots, x_n$ with complex coefficients. For a set $F \subset R$, we denote by $I(F)$, the ideal generated by the set F. In this paper, we fix a lexicographic (lex) monomial order $>_{\texttt{lex}}$ or $<_{\texttt{lex}}$ with $x_1 >_{\texttt{lex}} \cdots >_{\texttt{lex}} x_n$. Given a polynomial system

$$P(x) = (p_1(x), \cdots, p_n(x)) = 0 \qquad x = (x_1, \cdots, x_n) \in \mathbb{C}^n \tag{1}$$

where $p_i \in \mathbb{C}[x_1, \cdots, x_n]$, $i = 1, \cdots, n$. It is well-known (see [8] page 5) that, the affine algebraic variety V_P of the solution set of (1), which is defined by

$$V_P = V(P) = P^{-1}(0) = \{(x_1, \cdots, x_n) \in \mathbb{C}^n | P(x_1, \cdots, x_n) = 0\}$$

has a unique decomposition $V_P = V_{d_0} \cup \cdots \cup V_{d_\delta}$ into algebraic varieties V_{d_j}, $V_{d_i} \not\subset V_{d_j}$, $i \neq j$ and $\dim(V_{d_j}) = d_j$, $j = 0, \cdots, \delta$ where $0 \leq \delta \leq n-1$. Note that for $j = 0, \cdots, \delta$, V_{d_j} is the

union of d_j-dimensional components $V_{d_j} = V_{d_j}^1 \cup \cdots \cup V_{d_j}^{i_j}$, where $V_{d_j}^k \not\subset \bigcup_{l \neq k} V_{d_j}^l$, $k = 1, \cdots, i_j$. Therefore, we may write

$$V_P = \bigcup_{j=0}^{\delta} V_{d_j} = \bigcup_{j=0}^{\delta} V_{d_j}^1 \cup \cdots \cup V_{d_j}^{i_j},\ 0 \leq \delta \leq n-1,\ i_j \geq 1, \tag{2}$$

where $V_{d_j}^k$'s are called irreducible components of V_P. (2) is called irreducible decomposition of the variety V_P. In the field of numerical analysis of algebraic (polynomial) systems, we input (1) into a solver and we present a collection of points in $(\mathbb{Q}[i])^n$ within precision of a machine (see [12]) as a solution set of (1). Unlike numerical solvers, the symbolic methods which are mostly based on Gröbner basis give rise to exact solutions. In terms of the size of the systems, symbolic methods are less efficient than numerical solvers. The exact identification of V_P is the main advantages of symbolic methods. However, the computation time and the amount of memory needed is much bigger than numerical approach. As a comparison between these two approaches, the results in this paper and the one given in [7] are similar. But the time of calculation and the size of memory needed in [7] is much bigger than our approach in this paper.

For $0 \leq i \leq n$ and $x \in \mathbb{C}^n$, by solving the overdetermined system $\{P(x) = 0, \mathbf{L}_i(x) = 0\}$ with i cutting hyperplanes in $\mathbb{C}^n$ with random coefficients, we may get approximate generic points, known as witness points on irreducible components of V_P. The totality of witness points is called witness point superset. See [12] for the term. Then we consider approximate version of (2) as numerical irreducible decomposition of V_P and we write

$$W_P = \bigcup_{j=0}^{\delta} \left(W_{d_j}^1 \cup \cdots \cup W_{d_j}^{i_j} \right),\ 0 \leq \delta \leq n-1,\ i_j \geq 1. \tag{3}$$

The largest positive integer δ for which the solution set of the above overdetermined system is non-empty is called the top dimension of V_P. Practically, we solve many overdetermined systems from $i = n-1$ to lower values, until the first non-empty solution set achieved and we set the top dimension of V_P as $\delta = i$. This method seems efficient and doable for small systems. But for the large systems, this is still a very challenging problem. See [11] for more details.
For the algebraic version of the above discussion (see [9] section 2.4) that corresponds to (2), we consider the following. Any proper ideal $\mathfrak{a}$ ($\mathfrak{a} \subsetneq R$) is an (irredundant) intersection of a finite number of primary ideals as

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r, \tag{4}$$

where the $\mathfrak{q}_i$'s are primary ideals and $\mathfrak{p}_1 = \sqrt{\mathfrak{q}_1}, \cdots, \mathfrak{p}_r = \sqrt{\mathfrak{q}_r}$ are distinct associated prime ideals. Irredundancy means, none of the $\mathfrak{q}_i$'s contains the intersection of the others. If there is no other prime ideal between a prime ideal $\mathfrak{p}$ and $\mathfrak{a}$ with $\mathfrak{p} \supset \mathfrak{a}$, except $\mathfrak{p}$ itself, we say $\mathfrak{p}$ is a minimal prime ideal of $\mathfrak{a}$. (4) is called irredundant (reduced or minimal) primary decomposition of $\mathfrak{a}$. Corresponding to (4), we may set up the following

$$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r. \tag{5}$$

Clearly, $\mathfrak{p}_i$'s are minimal prime ideals of $\mathfrak{a}$. Any other prime ideal of $\mathfrak{a}$ is called embedded prime ideal associated with $\mathfrak{a}$. Let $\mathfrak{a} = I(p_1, \cdots, p_n)$, then (4) expresses the minimal primary decomposition of $I(p_1, \cdots, p_n)$. Also (5) is the minimal prime decomposition of $\sqrt{I(p_1, \cdots, p_n)} = I(V_P)$.

Let $(x_1, \cdots, x_n) \in \mathbb{C}^n$ and for positive integer i, define $r_n(i)$ as the positive remainder of i on division by n (identify $r_n(qn) = n$ for $q \in \mathbb{N}$). In majority of the works in the literature, the solution set of the polynomial equations $h_1 = 0, \cdots, h_{n-1} = 0, h_n = n$ given by

$$h_i = \sum_{j=1}^{n} \prod_{k=j}^{j+i-1} x_{r_n(k)}; \qquad 1 \leq i \leq n, \tag{6}$$

is called cyclic n-roots. For some history of this system see [2, 3, 11] and references therein. Recently, an extended application of cyclic n-roots system has been analyzed in a study of Toeplitz matrices (see [10]).

Throughout, we interchangeably use a simplified notation as $H_i = h_i$, for $i = 1, \cdots, n-1$ and $H_n = \frac{1}{n} h_n$. Let $IC_n = I(H_1, \cdots, H_n)$ be the ideal generated by the defining polynomials $H_1, \cdots, H_n$ of cyclic n-roots. Denote by V_{C_n}, the affine algebraic variety of the solution set of $\{H_1 = 0, \cdots, H_n = 0\}$. For positive integers $\delta, i_0, i_1, \cdots, i_\delta$ and $0 = d_0 < d_1 < \cdots < d_{\delta-1} < d_\delta < n-2$ suppose

$$I(V_{C_n}) = \sqrt{IC_n} = \bigcap_{j=0}^{\delta} \left(C_{d_j}^{n,1} \cap \cdots \cap C_{d_j}^{n,i_j} \right), \tag{7}$$

be the minimal prime decomposition of $I(V_{C_n})$, where $\dim(C_{d_j}^{n,k_j}) = d_j$, $j = 0, 1, \cdots, \delta$; $k_j = 1, \cdots, i_j$. Since $V_{C_n} \subset V(H_1, H_n)$, then $d_\delta < n-2$.

Example 1. Set $n = 4$ in (6). For the first time, cyclic 4-roots has been studied in [6]. Direct expansion shows that,

$$\begin{array}{lcl} H_1 & = & (x_1 + x_3) + (x_2 + x_4), \\ H_2 & = & x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1 = (x_1 + x_3)(x_2 + x_4) \\ H_3 & = & x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_1 + x_4x_1x_2 = x_1x_3(x_2 + x_4) + x_2x_4(x_1 + x_3), \\ H_4 & = & x_1x_2x_3x_4 - 1 = x_1x_2x_4(x_1 + x_3) - x_1^2x_2(x_2 + x_4) + (x_1x_2 + 1)(x_1x_2 - 1). \end{array} \tag{8}$$

Suppose

$$\begin{array}{lcl} C_1^{4,1} & = & I(x_1 + x_3, x_2 + x_4, x_1x_2 + 1), \\ C_1^{4,2} & = & I(x_1 + x_3, x_2 + x_4, x_1x_2 - 1). \end{array}$$

First, we verify that $V(IC_4) = V(C_1^{4,1}) \cup V(C_1^{4,2})$. Using (8), if we set $H_2 = 0$, then $(x_1 + x_3)(x_2 + x_4) = 0$ and in turn $x_1 + x_3 = 0$ or $x_2 + x_4 = 0$. This fact with $H_1 = H_3 = H_4 = 0$ imply $V(IC_4) \subset V(C_1^{4,1}) \cup V(C_1^{4,2})$. For the other inclusion, notice that according to (8), by vanishing the set of generators of $C_1^{4,1}$ or $C_1^{4,2}$, we get $H_1 = H_2 = H_3 = H_4 = 0$. In order to prove that $C_1^{4,1}$ and $C_1^{4,2}$ are prime ideals of dimension one in $\mathbb{C}[x_1, x_2, x_3, x_4]$, we may present

an argument quite similar to the one given for Lemma 3. Since $C_1^{4,1}$ and $C_1^{4,2}$ are prime and hence radical, we write

$$C_1^{4,1} \cap C_1^{4,2} = \sqrt{C_1^{4,1}} \cap \sqrt{C_1^{4,2}} = \sqrt{C_1^{4,1} \cap C_1^{4,2}}. \tag{9}$$

On the other hand, (8) shows that $IC_4 \subset C_1^{4,1} \cap C_1^{4,2}$. Thus, by (9),

$$\sqrt{IC_4} \subset \sqrt{C_1^{4,1} \cap C_1^{4,2}} = C_1^{4,1} \cap C_1^{4,2}. \tag{10}$$

For the other side, we write $C_1^{4,1} = \sqrt{C_1^{4,1}} = I(V(C_1^{4,1}))$, $C_1^{4,2} = \sqrt{C_1^{4,2}} = I(V(C_1^{4,2}))$ and we have (by Nullstellensatz)

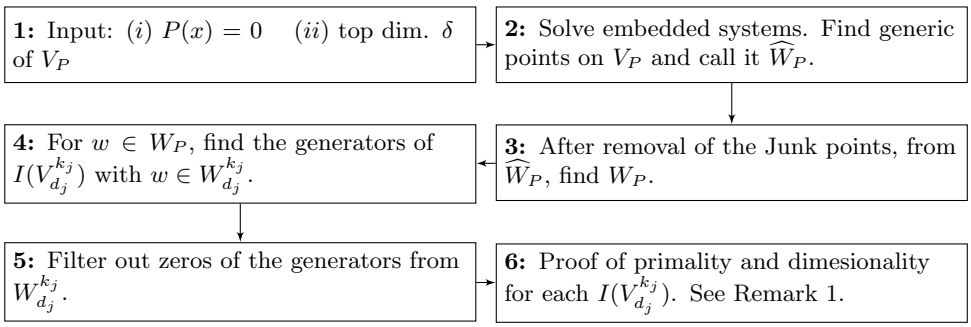
$$\begin{aligned} C_1^{4,1} \cap C_1^{4,2} &\subset I(V(C_1^{4,1})) \cap I(V(C_1^{4,2})) \\ &= I(V(C_1^{4,1}) \cup V(C_1^{4,2})) \\ &= I(V(IC_4)) = \sqrt{IC_4}. \end{aligned} \tag{11}$$

Two relationships (10) and (11) imply that $\sqrt{IC_4} = C_1^{4,1} \cap C_1^{4,2}$, which is the minimal prime decomposition of $\sqrt{IC_4} = I(V_{C_4})$. As a result, $I(V_{C_4})$ does not have any prime component on dimension zero. So, we may state that for $I(V_{C_4})$ the data in (7) are $\delta = 1$, $i_1 = 1$, $d_1 = 1$ and $i_0 = 0$.

In section 2, we discuss our new method in this paper and its distinction with a previously documented method in [11]. After presentation of the main algorithm 1 as a major difference between the method in this paper and the one given in [11], we give a typical numerical data. At last we discuss some facts about scheme of cyclic 9-roots in section 3 which includes proofs of primality and dimensionality of the calculated ideals in (13). Last section describes an open problem.

2 A heuristic Numerical-Symbolic algorithm

In many aspects the method in this paper is similar to the one given in [11]. A diagram of the method in this paper is depicted below.



In section 1, we discussed how to find the top dimension δ of V_P. Here, we consider the *embedded system* number (8) in [11]. It is the main part of cascade of homotopies. Then we follow the same procedure as in [11]. Since numerical analysis of monodromy is not well theorized, therefore the need for an algorithm that avoids the monodromy step is evident. So, as a major exception in our approach in this paper with the one given in [11] is that **we do not use monodromy grouping**. See [12] for more details and the origin of the theory. Here, we actually use three major softwares. They are all at the research level and written in FORTRAN90. The author's developed numerical software HHom4PsA which is an improved version of Hom4PS-2.0 (see [11] for details about the added components) and works for identification of higher dimensional components and is equipped with correction of algebraic numbers and is powered by JunkRemove (another package to remove extra generic points on a specific dimension).

Basically, in [11] two algorithms have been presented. In section 2.1 in [11], we described the role of monodromy grouping. This part constitutes step 2 in the main algorithm in [11] (i.e; algorithm 2 in [11]). To replace this part with the new idea, we propose the following algorithm that shows a major improvement in the process. We also consider the theory of deficiency pattern of rank deficient matrices proposed and developed in [11]. This theory is the core part of the procedure to find the exact form of the generators. In the following algorithm 1, we denote it by **Exact-generator**. Also in order to calculate more sample points on an numerical irreducible component we use the same routine **Sample** as in [11].

Algorithm 1. **Main Generator**
Input: A set $W_P = \bigcup_{j=0}^{\delta} W_{d_j} = \bigcup_{j=0}^{\delta}(W_{d_j}^1 \cup \cdots \cup W_{d_j}^{i_j})$
of pure generic (witness) points on V_P
Output: The exact generators for ideals $I(V_{d_j}^k)$
where $j = 1, \cdots, \delta$ and $k = 1, \cdots, i_j$.
Step 0: (Notation) For $w \in W$, denote by V_w, an irreducible
component of V_P with $w \in V_w$.
Step 1: For j from 1 to δ
Step 1.1: Set $i_j = 0$.
REPEAT
Step 1.2: Pick $w \in W_{d_j}$. Update $W_{d_j} = W_{d_j} - \{w\}$.
Step 1.3: Call **Sample** to generate enough sample
points on V_w. We collect them in the set C.
Step 1.4: Call **Exact-generator** to find the generators
of $I(V_w)$. Denote the generators by $q_1^w, \cdots, q_r^w$.
Step 1.5: Use the polynomials $q_1^w, \cdots, q_r^w$ to filter out
all $w_0 \in W$ such that $w_0 \in V_w$ and update W_{d_j}.
Step 1.6: Set $i_j = i_j + 1$ and $I(V_{d_j}^{i_j}) = I(V_w)$.
UNTIL $W_{d_j} = \varnothing$.
End For **Loop**$_j$

Remark 1. The calculation of linear generators is via deficiency pattern of rank deficient generic matrices. Actually the coefficients are approximate zero vectors of the generic matrices.

Therefore, if we approximate the coefficients to the nearest algebraic number (of a specific degree, see below), then we may consider approximate linear generators as exact ones of the corresponding ideal.

Actually, in algorithm 1, the outputs have already been identified by $I(V_{d_j}^k); j = 1, \cdots, \delta; k = 1, \cdots, i_j$. More precisely, we start off from a chosen witness point w in W_P. This w is an approximation of a generic point v on some $V_{d_j}^k$ for an appropriate j and k. Using the chosen w, we find the exact generators of an ideal $\tilde{I}_{d_j}^k$. These generators would eliminate some other w's in W_P. The number of the eliminated w's is equal to the degree of $\tilde{I}_{d_j}^k$. After all w's in W_P are used, we reach the following set of ideals

$$\tilde{I}_{d_j}^k; \;\; j = 1, \cdots, \delta; k = 1, \cdots, i_j,$$

with calculated exact generators. The theoretical analysis must be done to prove that they are prime ideals and $\dim(\tilde{I}_{d_j}^k) = d_j$ for a given j and k. For dimension zero, suppose we have i_0 isolated roots $(z_1^k, \cdots, z_n^k) \in \mathbb{C}^n; \;\; k = 1, \cdots, i_0$. Equivalently, we have i_0 prime ideals

$$\tilde{I}_{d_0}^k = \tilde{I}_0^k = I(x_1 - z_1^k, \cdots, x_n - z_n^k) \in \mathbb{C}^n; \; k = 1, \cdots, i_0.$$

Our goal is to conclude that

$$I(V_{d_j}^k) = \tilde{I}_{d_j}^k; \;\; j = 0, \cdots, \delta; k = 1, \cdots, i_j,$$

so that we can write

$$I(V_P) = \bigcap_{j=0}^{\delta} (I(V_{d_j}^1) \cap \cdots \cap I(V_{d_j}^{i_j})).$$

To this end, suppose we prove that

$$I(p_1, \cdots, p_n) \subset J = \bigcap_{j=0}^{\delta} (\tilde{I}_{d_j}^1 \cap \cdots \cap \tilde{I}_{d_j}^{i_j}). \tag{12}$$

Then $\sqrt{I(p_1, \cdots, p_n)} \subset \sqrt{J} = J$. This implies $I(V_P) \subset J$ and in turn $V(J) \subset V_P$. As we discussed above, J and $V(J)$ have been constructed using witness points on W_P and these witness points have their own corresponding exact generic points on V_P. In construction of J, we used all witness points in W_P. Therefore, in exact calculation, we heuristically imply that, there is no point left in $V_P - V(J)$. As a final step, we make a heuristic conclusion

$$\sqrt{I(p_1, \cdots, p_n)} = I(V_P) = \bigcap_{j=0}^{\delta} (I(V_{d_j}^1) \cap \cdots \cap I(V_{d_j}^{i_j})).$$

Verification of the inclusion in (12), depends on the system involved. We refer the reader to the appendix for the expressions that result (12) for cyclic 9-roots.

Let $\omega = \frac{1}{2} - i\frac{\sqrt{3}}{2}$. In what follows we give some data of a typical application of the method presented in this paper for cyclic 9-roots. After the first work of the author on this issue in

[11], this example shows another successful application of our method. With $\delta = 2$ in (7), we consider the following generic cutting hyperplanes

$$\begin{aligned} L_1(x_1, \cdots, x_9) &= (0.09 + 0.313i)x_1 + (0.093 + 0.49i)x_2 + \cdots, \\ L_2(x_1, \cdots, x_9) &= (0.032 + 0.29i)x_1 + (0.056 + 0.22i)x_2 + \cdots, \end{aligned}$$

and the following set of random coefficients

$$\begin{aligned} \lambda_{1,1} &= 0.929 + 0.31i, \\ \lambda_{1,2} &= 0.104 + 0.02i. \\ \vdots \quad & \vdots \qquad \vdots \end{aligned}$$

With the above setting, a calculated set of generic (witness) points $\widehat{W}_2 = \{w_1, \cdots, w_{18}\} \subset \mathbb{C}^{11}$ consist of 18 points on dimension 2 or higher is given. On this dimension the output of JunkRemove is $J_2 = \varnothing$. So the 18 points are pure generic points. As an example, w_1 is given below

$$\begin{aligned} w_1 = (&-0.539 + 1.477i, 1.586 - 0.0308i, -0.130 - 0.378i, -1.01 - 1.206i, \\ &-0.767 + 1.389i, 0.393 + 0.077i, 1.548 - 0.27i, -0.819 - 1.358i, \\ &-0.263 + 0.302i, 0 + 0i, 0 + 0i). \end{aligned}$$

The next step is to cut the original system (6) by one hyperplane. No generic point found on dimension one which means $W_1 = \varnothing$. And finally, the set of numerical solutions of (6) on dimension zero (certified by JunkRemove) consist of 6642 isolated solutions. We enter algorithm 1 with $W = W_0 \cup W_2$. Now the loop in algorithm 1 just applies on W_2 and will result the exact form of the generators of the ideals given in equations (13). So we enter the For Loop in algorithm 1 by picking up an element of W_2, say w_1 (Step 1.2). Out of this choice the routine **Sample** generates generic points on V_{w_1} (see Step 1.3 in algorithm 1 for the notation). In algorithm 1, we (via **Exact-generator**) calculate the generators of $I_1 = I(V_{w_1})$ as $x_1 + \omega x_7, x_2 + \omega x_8, x_3 + \omega x_9, \cdots$ and we use these polynomials to filter all generic points in W_2 that satisfy them. Only three generic points satisfy and we continue the process with the rest of 15 points in W_2, until we find all of the ideals in (13). A typical approximate coefficients of linear generators follows:

$$\begin{aligned} a_1 &= (1.00000000, 0.00000000) &\to\ & x_1 \\ a_7 &= (0.50000000, -0.86602540) &\to\ & \omega x_7 \\ a_2 &= (1.00000000, 0.00000000) &\to\ & x_2 \\ a_8 &= (0.50000000, -0.86602540) &\to\ & \omega x_8 \\ a_3 &= (1.00000000, 0.00000000) &\to\ & x_3 \\ a_9 &= (0.50000000, -0.86602540) &\to\ & \omega x_9. \end{aligned}$$

We justify our approximation of $(0.50000000, -0.86602540) \approx \omega$ based on Backelin's result in [1] which states infinite solution for cyclic n-roots when n has a square prime factor. In our case of cyclic 9-roots, the existence of an infinite solution set is established with coefficients of the linear forms as primitive 3^{rd} root of unity. The following set of six ideals are the prime

ideals in the minimal prime decomposition of $I(V_{C_9}) = \sqrt{IC_9}$,

$$\begin{array}{l} C_2^{9,1} = I(x_1+\bar{\omega}x_7, x_1+\omega x_4, x_2+\bar{\omega}x_8, x_2+\omega x_5, x_3+\bar{\omega}x_9, x_3+\omega x_6, x_1x_2x_3+\omega) \\ C_2^{9,2} = I(x_1+\bar{\omega}x_7, x_1+\omega x_4, x_2+\bar{\omega}x_8, x_2+\omega x_5, x_3+\bar{\omega}x_9, x_3+\omega x_6, x_1x_2x_3+\bar{\omega}) \\ C_2^{9,3} = I(x_1+\bar{\omega}x_7, x_1+\omega x_4, x_2+\bar{\omega}x_8, x_2+\omega x_5, x_3+\bar{\omega}x_9, x_3+\omega x_6, x_1x_2x_3-1) \\ C_2^{9,4} = I(x_1+\omega x_7, x_1+\bar{\omega}x_4, x_2+\omega x_8, x_2+\bar{\omega}x_5, x_3+\omega x_9, x_3+\bar{\omega}x_6, x_1x_2x_3+\omega) \\ C_2^{9,5} = I(x_1+\omega x_7, x_1+\bar{\omega}x_4, x_2+\omega x_8, x_2+\bar{\omega}x_5, x_3+\omega x_9, x_3+\bar{\omega}x_6, x_1x_2x_3+\bar{\omega}) \\ C_2^{9,6} = I(x_1+\omega x_7, x_1+\bar{\omega}x_4, x_2+\omega x_8, x_2+\bar{\omega}x_5, x_3+\omega x_9, x_3+\bar{\omega}x_6, x_1x_2x_3-1). \end{array} \tag{13}$$

The symbolic method used in [7] took 15 days and the amount of memory needed was 1.7 gigabyte. In comparison with the method in [7], our method just took less than 3 hours and the amount of memory needed was negligible. The expressions given in the appendix certify that $IC_9 \subset C_2^{9,i}; i = 1, \cdots, 6$. In Lemma 3, we prove that $C_2^{9,i}$'s are all prime ideals. The number of isolated roots of cyclic 9-roots has been counted to 6642 in $\mathbb{C}^9$. We summarize the data in (7) for cyclic 9-roots as $\delta = 2$, $i_2 = 6$, $i_1 = 0$ and $i_0 = 6642$.

3 Results on scheme of Cyclic 9-roots

Consider a typical ideal in the above prime decomposition of cyclic 9-roots $C_2^{9,1}$. With respect to lex-order $x_1 >_{\text{lex}} \cdots >_{\text{lex}} x_9$, the reduced Gröbner basis of $C_2^{9,1}$ is $\mathfrak{p} = I(g_1 = x_1 + \omega x_7, g_2 = x_2 + \omega x_8, g_3 = x_3 + \omega x_9, g_4 = x_4 + \bar{\omega}x_7, g_5 = x_5 + \bar{\omega}x_8,\ g_6 = x_6 + \bar{\omega}x_9, h = x_7x_8x_9 + \omega)$. Let $R = \mathbb{C}[x_1, \cdots, x_9]$. To the rest of the discussion, we consider the following monomials: $\eta = x_7x_8,\ \delta = x_8x_9,\ \sigma = x_7x_9$. Also, for $f \in R$, denote by $\overline{f}^{\mathfrak{p}}$ the remainder of f on division by $\mathfrak{p}$. Also define $Rem(\mathfrak{p}) = \{\overline{f}^{\mathfrak{p}} : f \in A\}$.

Lemma 1. $Rem(\mathfrak{p}) = \bigoplus_{i=7}^{9} x_i\mathbb{C}[x_i] \oplus \eta\mathbb{C}[x_7, x_8] \oplus \delta\mathbb{C}[x_8, x_9] \oplus \sigma\mathbb{C}[x_7, x_9] \oplus \mathbb{C}$.

Proof: Since $\mathfrak{p}$ is a reduced Gröbner basis, then for $f \in A$, none of the monomials in $supp(\overline{f}^{\mathfrak{p}})$ is divisible by any of the initial monomials $in_{\text{lex}}(g_i) = x_i$ $(i = 1, \cdots, 6)$ or $in_{\text{lex}}(h) = x_7x_8x_9$. Therefore, the form of monomials in $supp(\overline{f}^{\mathfrak{p}})$ are as follows:

$$\begin{array}{c} 1, x_i, x_i^2, \cdots \text{ for } i = 7, 8, 9 \\ x_7^k x_8^l, x_7^k x_9^l, x_8^k x_9^l \text{ for integers } k, l > 0, \end{array}$$

and these result the claim. □

For the primality of $\mathfrak{p}$, we mimic the proof given in proposition 6 page 197 of [4], with different exposition.

Lemma 2. *Let $Z = V(rs) \subset \mathbb{C}^2$. Consider the rational parametrization of $V(\mathfrak{p})$ as $F : \mathbb{C}^2 \backslash Z \to \mathbb{C}^9$ with $F(r, s) = (\frac{\omega}{rs}, -r, -s, \frac{1}{rs}, -\bar{\omega}r, -\bar{\omega}s, \frac{-\omega}{rs}, r, s)$. Then*

$$\mathfrak{p} = \{\phi \in R : \phi \circ F = 0\}.$$

Proof: Simple calculations show that $g_i \circ F = 0$ for $i = 1, \cdots, 6$ and $h \circ F = 0$. Therefore, $\mathfrak{p} \subset \{\phi \in R : \phi \circ F = 0\}$. Let $\phi \in R$ with $\phi \circ F = 0$. Write $\phi = \phi_{\mathfrak{p}} + \overline{\phi}^{\mathfrak{p}}$, where $\phi_{\mathfrak{p}} \in \mathfrak{p}$ and $\overline{\phi}^{\mathfrak{p}} \in Rem(\mathfrak{p})$. Now $0 = \phi \circ F = \phi_{\mathfrak{p}} \circ F + \overline{\phi}^{\mathfrak{p}} \circ F = \overline{\phi}^{\mathfrak{p}} \circ F$. Since $\hat{\phi}(r,s) = \overline{\phi}^{\mathfrak{p}}(F(r,s)) = 0$ for all $(r,s) \in \mathbb{C}^2 \backslash Z$, then we may take an integer N large enough such that $(rs)^N \hat{\phi}$ (this clears the denominators) can be considered as a polynomial that vanishes on $\mathbb{C}$ (an infinite ring). Thus $\hat{\phi} = 0$ which in turn implies $\overline{\phi}^{\mathfrak{p}} = 0$. The result follows. □

Lemma 3. *$\mathfrak{p}$ is a prime ideal in R of dimension 2.*

Proof: By Lemma 2, $\mathfrak{p} = \{\phi \in R : \phi \circ F = 0\}$. Let $\phi_1, \phi_2 \in R$ with $\phi_1 \cdot \phi_2 \in \mathfrak{p}$, $\deg \phi_1 = M$ and $\deg \phi_2 = N$. Then $\deg(\phi_1 \cdot \phi_2) = M + N$ and $(rs)^{M+N}(\phi_1 \circ F) \cdot (\phi_2 \circ F) = 0$. Notice that this implies the product of polynomials $(rs)^M(\phi_1 \circ F)$ and $(rs)^N(\phi_2 \circ F)$ is zero in R. Since R is an integral domain (if the ring K is an integral domain then so is $K[x_1, \cdots, x_n]$), then one of them must be zero. We deduce that, $\phi_1 \in \mathfrak{p}$ or $\phi_2 \in \mathfrak{p}$. The above parametrization shows that $V(\mathfrak{p})$ is parametrized by two parameters r and s and hence $\dim(V) = \dim(\mathfrak{p}) = 2$. □

The following is a detailed form of the facts given in page 35 of [5].

Lemma 4. *For $f, g \in R$, we have $\overline{\overline{f}^{\mathfrak{p}} \cdot \overline{g}^{\mathfrak{p}}}^{\mathfrak{p}} = \overline{f \cdot g}^{\mathfrak{p}}$.*

Proof: $f, g \in R$ can be written as $f = f_{\mathfrak{p}} + \overline{f}^{\mathfrak{p}}$ and $g = g_{\mathfrak{p}} + \overline{g}^{\mathfrak{p}}$, where $f_{\mathfrak{p}}, g_{\mathfrak{p}} \in \mathfrak{p}$ and $\overline{f}^{\mathfrak{p}}$ and $\overline{g}^{\mathfrak{p}}$ are the remainders. Since $f_{\mathfrak{p}} \cdot g_{\mathfrak{p}}, \overline{f_{\mathfrak{p}}}^{\mathfrak{p}} \cdot g_{\mathfrak{p}}, \overline{g_{\mathfrak{p}}}^{\mathfrak{p}} \cdot f_{\mathfrak{p}} \in \mathfrak{p}$, we have $\overline{f_{\mathfrak{p}} \cdot g_{\mathfrak{p}}}^{\mathfrak{p}} = \overline{\overline{f_{\mathfrak{p}}}^{\mathfrak{p}} \cdot g_{\mathfrak{p}}}^{\mathfrak{p}} = \overline{\overline{g_{\mathfrak{p}}}^{\mathfrak{p}} \cdot f_{\mathfrak{p}}}^{\mathfrak{p}} = 0$. Thus,

$$\begin{aligned} \overline{f \cdot g}^{\mathfrak{p}} &= \overline{f_{\mathfrak{p}} \cdot g_{\mathfrak{p}} + \overline{f_{\mathfrak{p}}}^{\mathfrak{p}} \cdot g_{\mathfrak{p}} + \overline{g_{\mathfrak{p}}}^{\mathfrak{p}} \cdot f_{\mathfrak{p}} + \overline{f_{\mathfrak{p}}}^{\mathfrak{p}} \cdot \overline{g_{\mathfrak{p}}}^{\mathfrak{p}}}^{\mathfrak{p}} \\ &= \overline{f_{\mathfrak{p}} \cdot g_{\mathfrak{p}}}^{\mathfrak{p}} + \overline{\overline{f_{\mathfrak{p}}}^{\mathfrak{p}} \cdot g_{\mathfrak{p}}}^{\mathfrak{p}} + \overline{\overline{g_{\mathfrak{p}}}^{\mathfrak{p}} \cdot f_{\mathfrak{p}}}^{\mathfrak{p}} + \overline{\overline{f_{\mathfrak{p}}}^{\mathfrak{p}} \cdot \overline{g_{\mathfrak{p}}}^{\mathfrak{p}}}^{\mathfrak{p}} = \overline{\overline{f_{\mathfrak{p}}}^{\mathfrak{p}} \cdot \overline{g_{\mathfrak{p}}}^{\mathfrak{p}}}^{\mathfrak{p}}. \end{aligned}$$

□

The algebraic structure on $R/\mathfrak{p}$ (that makes it a $\mathbb{C}$-algebra) is given by the operations: $f, g \in R; [f] + [g] = \overline{f}^{\mathfrak{p}} + \overline{g}^{\mathfrak{p}}$ and $[f] \cdot [g] = \overline{\overline{f}^{\mathfrak{p}} \cdot \overline{g}^{\mathfrak{p}}}^{\mathfrak{p}}$. We state the following facts without proof. The proofs are straightforward verifications.

Lemma 5. *$(Rem(\mathfrak{p}), \oplus, \odot)$ is a $\mathbb{C}$-algebra with the following operations:*

$$f, g \in R; \quad \overline{f}^{\mathfrak{p}} \oplus \overline{g}^{\mathfrak{p}} \;=\; \overline{f+g}^{\mathfrak{p}} \quad \textit{and} \quad \overline{f}^{\mathfrak{p}} \odot \overline{g}^{\mathfrak{p}} = \overline{\overline{f}^{\mathfrak{p}} \cdot \overline{g}^{\mathfrak{p}}}^{\mathfrak{p}}.$$

Corollary 1. *The following are $\mathbb{C}$-subalgebra of $Rem(\mathfrak{p})$:*

$$R_i = x_i\mathbb{C}[x_i], i = 7, 8, 9; \; R_\eta = \eta\mathbb{C}[x_7, x_8]; R_\delta = \delta\mathbb{C}[x_8, x_9] \textit{ and } R_\sigma = \sigma\mathbb{C}[x_7, x_9].$$

Lemma 6. *$R/\mathfrak{p}$ is isomorphic to $Rem(\mathfrak{p})$ as $\mathbb{C}$-algebras.*

The fact that $(R\backslash\mathfrak{p})/\mathfrak{p}$ is a multiplicative subset of $R/\mathfrak{p}$ is a clear one and we may well consider the following:

Lemma 7. *We have* $((R\backslash\mathfrak{p})/\mathfrak{p})^{-1}(R/\mathfrak{p}) = \left\{\frac{f}{g} : f, g \in Rem(\mathfrak{p}); g \neq 0\right\}$.

Proof: In light of previous lemmas, we may choose the elements of $R/\mathfrak{p}$ from $Rem(\mathfrak{p})$. The elements of $((R\backslash\mathfrak{p})/\mathfrak{p})$ correspond to nonzero elements of $Rem(\mathfrak{p})$. We abuse notation and denote the equivalence classes $[f/g]$ in $((R\backslash\mathfrak{p})/\mathfrak{p})^{-1}(R/\mathfrak{p})$ by f/g. The result follows. □

4 Conclusion and future of the research

The future of the research tends to realizations of many facts in pure algebraic geometry. Among these problems we pose the following question:

According to Theorem 3.2 (d), page 17 in [8], the rational function field on $V(\mathfrak{p})$ $(K(V(\mathfrak{p})))$ is isomorphic to the field of fractions of $A/\mathfrak{p}$ which is given by the Lemma 7. Since $K(V(\mathfrak{p}))$ is defined by the set of all equivalence classes of regular functions defined on a neighborhood of $V(\mathfrak{p})$, we may well consider the restriction $K(V(\mathfrak{p}))|_{V(\mathfrak{p})}$ of all functions that are defined on the points on the variety $V(\mathfrak{p})$. The study of $K(V(\mathfrak{p}))|_{V(\mathfrak{p})}$ is an interesting problem.

Remark 2. An abstract of this paper has been presented at AMS Joint Mathematical Meeting (JMM), Baltimore MD, January 15-18 2014, AMS contributed paper session in Algebraic Geometry.

5 Appendix

We choose $C_2^{9,1}$ and we intend to present an expression for each $H_1, \cdots, H_9$ in terms of the generators of $C_2^{9,1}$. For convenience we consider the lexicographic monomial order with

$$x_4 >_{\text{lex}} x_5 >_{\text{lex}} x_6 >_{\text{lex}} x_7 >_{\text{lex}} x_8 >_{\text{lex}} x_9 >_{\text{lex}} x_1 >_{\text{lex}} x_2 >_{\text{lex}} x_3.$$

With this order, $G = C_2^{9,1}$ is the reduced Gröbner basis. Suppose

$$\begin{array}{llll} g_1 = x_1 + \bar{\omega}x_7, & g_2 = x_1 + \omega x_4, & g_3 = x_2 + \bar{\omega}x_8, & g_4 = x_2 + \omega x_5, \\ g_5 = x_3 + \bar{\omega}x_9, & g_6 = x_3 + \omega x_6, & h = x_1x_2x_3 + \bar{\omega}. & \end{array}$$

So we write

$$\begin{array}{rcl} H_1 & = & \omega(g_1 + g_3 + g_5) + \bar{\omega}(g_2 + g_4 + g_6) \\ & = & x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9. \end{array}$$

We list two other expressions of the defining polynomials of cyclic 9-roots

$$\begin{array}{rcl} H_2 & = & \omega(x_6 + x_8)g_1 + \bar{\omega}(x_3 + x_5)g_2 + \bar{\omega}(x_1 - \bar{\omega}x_9)g_3 + \omega(x_1 - \omega x_6)g_4 \\ & & +\omega(x_1 - \omega x_2)g_5 + (\omega x_2 - x_1)g_6 \\ & = & x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_6 + x_6x_7 + x_7x_8 + x_8x_9 + x_9x_1, \end{array}$$

$$\begin{array}{rcl} H_3 & = & \omega(x_5x_6 + x_6x_8 + x_8x_9)g_1 + \bar{\omega}(x_2x_3 + x_3x_5 + x_5x_6)g_2 \\ & & +(x_9 + \bar{\omega}x_6)x_1g_3 + \omega(x_3 + \omega x_6)x_1g_4, \\ & = & x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_6 + x_5x_6x_7 + x_6x_7x_8 + x_7x_8x_9 \\ & & +x_8x_9x_1 + x_9x_1x_2. \end{array}$$

Acknowledgment: The author appreciates very much of the valuable comments of the anonymous referee.

References

[1] Backelin, J., Square multiples n gives infinite many cyclic n-roots, *Reports of Matematiska Institutionen, Stockholms Universitet*, **8**, (1989), pp.1–pp.2

[2] Backelin, J. and Fröberg, R., How to prove that there are 924 cyclic-7 roots?, *Proc. ISSAC'91 (S. M. Watt, ed.) ACM* (1991), pp.103–pp.111

[3] Björck G. and Fröberg, R., Methods to "divide out" certain solutions from systems of algebraic equations, applied to find all cyclic 8-roots, *Analysis, algebra, and computers in mathematical research, Lecture Notes in Pure and Appl. Math.* **156**, *Dekker, New York*, (1992) 57–70.

[4] Cox, D., Little, J. and O'Shea, D., *Ideal, Varieties, and Algorithms*, 2^{ed} Ed., Springer-Verlag, 1997.

[5] Cox, D., Little, J. and O'Shea, D., *Using Algebraic Geometry*, Graduate Texts in Math. 185, Springer-Verlag, 1998.

[6] Davenport J., Looking at a set of equations, *Bath Computer Science, Technical report*, **87-06**, 1987.

[7] Faugére, J.C., Finding all the solutions of cyclic-9 using Gröbner basis techniques, *Computer mathematics (Matsuyama), Lecture Notes Ser. Comput.*, **9**, *World Sci. Publ., River Edge, NJ.*, (2001), pp.1–pp.12

[8] Hartshorne, R., *Algebraic Geometry*, Graduate Texts in Math. 52, Springer-Verlag, Berlin, New York, 1977.

[9] Iitaka, S., *Algebraic Geometry, An introduction to Birational Geometry of Algebraic Varieties*, Springer-Verlag, 1982.

[10] Lee, M. H. and Szöllősi, F., A note on inverse-orthogonal Toeplitz Matrices, *Electronic Journal of Linear Algebra*, **V. 26**, (2013), pp.898–pp.904

[11] Sabeti, R., Numerical-symbolic exact irreducible decomposition of cyclic-12, *LMS Journal of Computation and Mathematics*, **14**, (2011), pp.155–pp.172

[12] Sommese, A.J. and Wampler, C.W., *The numerical solution of systems of polynomials, arising in engineering and science*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.

Received: 17.09.2014

Revised: 28.01.2015

Accepted: 02.02.2015

Mathematics and Computer Science Department,
Olivet College, 320 South Main St. Olivet, MI, 49076, U.S.A
E-mail: rsabeti@olivetcollege.edu
rostamsabeti@gmail.com