On formation of polynomial expressions for cyclic n-roots system for $n = 8, 9, 12, 16$

Rostam Sabeti

Department of Mathematics and Computer Science

Olivet College, 320 South Main St.

Olivet, MI, 49076, USA.

rsabeti@OlivetCollege.edu

Dedicated to Professor T.Y. Li

Abstract

Suppose G is the reduced Gröbner basis of an ideal $I \subset R = K[x_1, \cdots, x_n]$ with respect to the lexicographic monomial order. In this paper, we present and implement an algorithm to find expressions for any $f \in R$ in terms of the generators of G. Among examples, exact forms of the expressions of the defining polynomials of cyclic n-roots for $n = 8, 9, 12, 16$, are presented. Cyclic 16-roots is an unknown system for which we exhibit one of its prime ideals in its primary decomposition and in turn an expression of a defining polynomial of the system.

1 Introduction

Let K be an algebraically closed field and $R = K[x_1, \cdots, x_n]$ be the ring of polynomials in n variables $x_1, \cdots, x_n$ with coefficients in K. As usual, denote a monomial by $m = \mathbf{x}^\alpha = x_1^{i_1} \cdots x_n^{i_n} \in$

R, where $\alpha = (i_1, \cdots, i_n) \in \mathbb{Z}^n_{\geqslant 0}$ is the multi-index of m and $\deg(\mathbf{x}^\alpha) = i_1 + \cdots + i_n$ is the total degree of m. Denote by $M(R)$, the set of all monomials in R. For a polynomial $f = \sum_\alpha a_\alpha \mathbf{x}^\alpha \in R$, define $supp(f) = \{\mathbf{x}^\alpha : a_\alpha \neq 0\}$ and we call it the support of f. In this paper, we fix a lexicographic (lex) monomial order $>_{\text{lex}}$ or $<_{\text{lex}}$ with $x_1 >_{\text{lex}} \cdots >_{\text{lex}} x_n$. The initial monomial of each $f \in R$, denoted by $in_{\text{lex}}(f)$, is the biggest element in $supp(f)$. If $\eta \in M(R)$ and $f \in R$, then $\deg_\eta(f)$ is the degree of f as an element in $R[\eta]$. For example, if $f = x_1x_2^4x_3^2 + x_1^5x_2^3x_3 - x_2 \in R$ and $\eta = x_2^2x_3 \in M(R)$, then $\deg_\eta(f) = 2$. We may rewrite f as $f = x_1\eta^2 + x_1^5x_2\eta - x_2 \in R[\eta]$. Notice that, if we consider the above order, then $in_{\text{lex}}(f) = x_1^5x_2^3x_3$. For an ideal I in R, a finite set $G = \{g_1, \cdots, g_r\}$ of elements of I is the reduced Gröbner basis of I if (a) the ideal $\langle\{in_{\text{lex}}(f) : 0 \neq f \in I\}\rangle$ is generated by $in_{\text{lex}}(g_1), \cdots, in_{\text{lex}}(g_r)$ (b) each g_i is monic and (c) for $i \neq j$, none of the monomials of $supp(g_j)$ is divisible by $in_{\text{lex}}(g_i)$. For more information and proof of uniqueness see [11] page 32.

Throughout the paper, $G = \{g_1, \cdots, g_r\}$ stands for the reduced Gröbner basis of I with respect to the above lex monomial order. With the notation above, for $f \in R$, we write $f = f_1g_1 + \cdots + f_rg_r + f'$, where $f_1, \cdots, f_r, f' \in R$ and call it an *expression* of f in terms of g_i's. We also refer $(f_1, \cdots, f_r)$ as an expression of f. Expressions are the outputs of division (or reduction) algorithms. In [9] page 334, it is properly established that, there are two types of division algorithms, *determinate* and *indeterminate*. A determinate division algorithm is the one that gives rise to a *unique expression* with certain algebraic characteristics. Another version of standard (determinate) division algorithm is of the form given in [1] page 28.

Remark 1. (Why do we need an algorithm to evaluate expressions?) At the time of derivation of the primary ideals of positive dimension in primary decomposition of cyclic 12-roots in [12] (in this case, it is proved that those ideals in [12] are prime), the author encountered the following problem:

> Suppose an ideal $I := \langle h_1, \cdots, h_n\rangle$ with exact form of generators $h_1, \cdots, h_n$ is given. By exact we mean a polynomial that has no approximate coefficient. Also, let $\bar{I} = \langle g_1, \cdots, g_r\rangle$ be another ideal with the computed exact generators (output

of an algorithm). We want to test that whether $\bar{I}$ is one of the ideals in primary decomposition of I or not. Since we must have $I = \bar{I} \cap \cdots$, at least we must be able to prove that $I \subset \bar{I}$, or in turn for all $1 \leqslant i \leqslant n$, $h_i \in \bar{I}$.

This means that we have a type of ideal membership problem. A straightforward method to deal with this problem is to use a computer algebra software (CAS) like MAPLE and specifically the command **normalf** in its built-in Gröbner basis package. For the examples that are given is section 3, an attempt to use a CAS was failed. Another method is to exploit a version of the usual division algorithm (given in [1] page 28). This approach may easily get complicated in cases where the number of monomials in the support of the current h_i that is divisible by the current $in_{\text{lex}}(g_k)'s$ is big. And this happens for the case of large scale cyclic n-roots problem. However, this paper presents an algorithm that reduces the number of algebraic (symbolic) operations in the usual division algorithm.

The main algorithm is presented in section 2 and section 3 and appendix are devoted to main examples.

2 Main algorithm

Fix $\eta \in M(R)$ and define $R_\eta = \{f \in R : \forall m \in supp(f); \eta \nmid m\}$ and let $\eta R = \{\eta f : f \in R\} = (\eta)$ be the principle ideal generated by η in R. Clearly, $f \in R_\eta$ if and only if $\deg_\eta(f) = 0$. The next lemma expresses a very simple and straightforward fact about a representation of $f \in R[\eta]$.

Lemma 1 *With the above notation, if $f \in R$, then there exists an integer $r \geqslant 0$ and $\bar{f}_0, \bar{f}_1, \cdots, \bar{f}_r \in R_\eta$ such that $f = \sum_{i=1}^{r} \eta^i \bar{f}_i + \bar{f}_0$.*

Proof: Given a $m \in M(R)$, let i be the maximal power of η that divides m, so $m = m'\eta^i$, where $m' \in R_\eta$. Since any polynomial is a sum of constants times monomials, the lemma follows easily.□

Now let $g = \eta + \Lambda \in R$ with $\eta = in_{\text{lex}}(g)$ and hence $\Lambda \in R_\eta$.

Theorem 1 *With the above notation, for $f \in R$ with $\eta \mid in_{lex}(f)$, there is $f_g \in R$ such that $f_{red} = f - (f_g)g \in R_\eta$.*

Proof: As a consequence of lemma 1, we set $f^1_{red} = f = \sum_{i=1}^{r_1} \eta^i \bar{f}^1_i + \bar{f}^1_0 = \eta \sum_{i=1}^{r_1} \eta^{i-1} \bar{f}^1_i + \bar{f}^1_0$ where $\bar{f}^1_i$'s are given as in lemma 1. Define $f^1_g = \sum_{i=1}^{r_1} \eta^{i-1} \bar{f}^1_i$ and f^2_{red} and consider as

$$f^2_{red} = f^1_{red} - (f^1_g)g = \eta \sum_{i=1}^{r_1} \eta^{i-1} \bar{f}^1_i + \bar{f}^1_0 - (\eta + \Lambda) \sum_{i=1}^{r_1} \eta^{i-1} \bar{f}^1_i = -\sum_{i=1}^{r_1} \eta^{i-1} \Lambda \bar{f}^1_i + \bar{f}^1_0.$$

Now for $i = 1, \cdots, n$, for all $\lambda \in supp(\Lambda)$ and for all $m_i \in supp(\bar{f}^1_i)$, since $\lambda <_{\text{lex}} \eta$, we have $\lambda m_i <_{\text{lex}} \eta m_i$ and in turn $\lambda \eta^{i-1} m_i <_{\text{lex}} \eta^i m_i$. Since $in_{\text{lex}}(f^2_{red})$ is a monomial of the form and $\lambda \eta^{i-1} m_i$ and $in_{\text{lex}}(f^1_{red})$ is a monomial of the form $\eta^i m_i$, the former inequality shows that $in_{\text{lex}}(f^2_{red}) <_{\text{lex}} in_{\text{lex}}(f^1_{red})$. By lemma 1, we express f^2_{red} as $f^2_{red} = \sum_{i=1}^{r_2} \eta^i \bar{f}^2_i + \bar{f}^2_0$ with appropriate nonnegative integer r_2 and $\bar{f}^2_0, \bar{f}^2_1, \cdots, \bar{f}^2_{r_2} \in R_\eta$. We repeat the above reduction process and we find $f^2_g = \sum_{i=1}^{r_2} \eta^{i-1} \bar{f}^2_i$ and f^3_{red} such that $in_{\text{lex}}(f^3_{red}) <_{\text{lex}} in_{\text{lex}}(f^2_{red})$. We continue this process and obtain sequences of polynomials f^{j-1}_g and f^j_{red}'s with strictly decreasing sequence $\cdots <_{\text{lex}} in_{\text{lex}}(f^j_{red}) <_{\text{lex}} \cdots <_{\text{lex}} in_{\text{lex}}(f^2_{red}) <_{\text{lex}} in_{\text{lex}}(f^1_{red}) = in_{\text{lex}}(f)$. Since $\eta \mid in_{\text{lex}}(f)$, then for some integer $k > 0$, we reach $\deg_\eta(f^k_{red}) = 0$. This means $f^k_{red} \in R_\eta$. In this situation, we let $f_g = f^1_g + \cdots + f^{k-1}_g$. Therefore,

$$\begin{aligned} f_{red} = f^k_{red} &= f^{k-1}_{red} - (f^{k-1}_g)g \\ &= f^{k-2}_{red} - (f^{k-2}_g)g - (f^{k-1}_g)g = f^{k-2}_{red} - (f^{k-2}_g + f^{k-1}_g)g \\ &\vdots \\ &= f^1_{red} - (f^1_g + \cdots + f^{k-1}_g)g = f - (f_g)g, \end{aligned} \tag{1}$$

as desired. □

Example 1. Let $K = \mathbb{C}$ and $\eta = x_1x_2 \in M(R)$, $f, g \in R = \mathbb{C}[x_1, x_2, x_3]$ with $g = x_1x_2 + x_3 = \eta + \Lambda$ and $f^1_{red} = f = x_1x_2(x_1^2 + x_2x_3) - x_1x_3 = \eta \bar{f}^1_1 + \bar{f}^1_0$ where $\Lambda = x_3$, $\bar{f}^1_1 = x_1^2 + x_2x_3$ and $\bar{f}^1_0 = -x_1x_3$. Let $f^1_g = x_1^2 + x_2x_3 = \bar{f}^1_1$ and

$$\begin{aligned} f_{red}^2 &= f_{red}^1 - (f_g^1)g = \eta\bar{f}_1^1 + \bar{f}_0^1 - (\eta+\Lambda)\bar{f}_1^1, \\ &= -\Lambda\bar{f}_1^1 + \bar{f}_0^1, \\ &= -x_1^2x_3 - x_1x_3 - x_2x_3^2 \in R_\eta. \end{aligned}$$

Example 2. Let $K = \mathbb{C}$ and $\eta = x_1^2x_2 \in M(R)$, $f, g \in R = \mathbb{C}[x_1, x_2, x_3]$ with $g = x_1^2x_2 - x_1x_2 + x_2x_3 = \eta + \Lambda$ and $f_{red}^1 = f = x_1^2x_2(x_1^3 - x_1^2 + x_1x_3) - x_1x_2x_3 = \eta\bar{f}_1^1 + \bar{f}_0^1$ where $\Lambda = -x_1x_2 + x_2x_3$, $\bar{f}_1^1 = x_1^3 - x_1^2 + x_1x_3$ and $\bar{f}_0^1 = -x_1x_2x_3$. Let $f_g^1 = x_1^3 - x_1^2 + x_1x_3$ and

$$\begin{aligned} f_{red}^2 &= f_{red}^1 - (f_g^1)g \\ &= (x_1^5x_2 - x_1^4x_2 + x_1^3x_2x_3 - x_1x_2x_3) - \\ &\quad (x_1^3 - x_1^2 + x_1x_3)(x_1^2x_2 - x_1x_2 + x_2x_3), \\ &= x_1^4x_2 - x_1^3x_2x_3 - x_1^3x_2 + 2x_1^2x_2x_3 - x_1x_2x_3^2 - x_1x_2x_3, \\ &= x_1^2x_2(x_1^2 - x_1x_3 - x_1 + 2x_3) - x_1x_2x_3^2 - x_1x_2x_3. \end{aligned}$$

As we see, $\deg_\eta(f_{red}^2) = \deg_\eta(f_{red}^1) = 1$ while $f_{red}^2 <_{\text{lex}} f_{red}^1$. This evidently results that unlike f_{red}^j's, the integer sequence $\deg_\eta(f_{red}^j)$'s does not constitute a strictly decreasing one. The reader should notice that, eventually and according to the proof of the Theorem 2.2, the sequence $\deg_\eta(f_{red}^j)$'s tends to zero. We continue by setting $\bar{f}_1^2 = x_1^2 - x_1x_3 - x_1 + 2x_3$, $\bar{f}_0^2 = -x_1x_2x_3^2 - x_1x_2x_3$ and $f_{red}^2 = \eta\bar{f}_1^2 + \bar{f}_0^2$. Let $f_g^2 = x_1^2 - x_1x_3 - x_1 + 2x_3 = \bar{f}_1^2$, then

$$\begin{aligned} f_{red}^3 &= f_{red}^2 - (f_g^2)g = f_{red}^1 - (f_g^1)g - (f_g^2)g = f_{red} - (f_g^1 + f_g^2)g \\ &= \eta\bar{f}_1^2 + \bar{f}_0^2 - (\eta+\Lambda)\bar{f}_1^2 = -\Lambda\bar{f}_1^2 + \bar{f}_0^2, \\ &= (x_1x_2 - x_2x_3)(x_1^2 - x_1x_3 - x_1 + 2x_3) - x_1x_2x_3, \\ &= x_1^2x_2(x_1 - 2x_3 - 1) + 2x_1x_2x_3 + x_2x_3^2x_1 - 2x_2x_3^2. \end{aligned}$$

We continue by taking $f_g^3 = x_1 - 2x_3 - 1$ as:

$$\begin{aligned}
f_{red}^4 &= f_{red}^3 - (f_g^3)g = f_{red}^1 - (f_g^1)g - (f_g^2)g - (f_g^3)g = f - (f_g^1 + f_g^2 + f_g^3)g \\
&= \eta(x_1 - 2x_3 - 1) + 2x_1x_2x_3 + x_2x_3^2x_1 - 2x_2x_3^2 - (\eta + \Lambda)(x_1 - 2x_3 - 1) \\
&= -\Lambda(x_1 - 2x_3 - 1) + 2x_1x_2x_3 + x_2x_3^2x_1 - 2x_2x_3^2, \\
&= (x_1x_2 - x_2x_3)(x_1 - 2x_3 - 1) + 2x_1x_2x_3 + x_2x_3^2x_1 - 2x_2x_3^2 \\
&= x_1^2x_2 + x_1x_2x_3^2 - x_1x_2x_3 - x_1x_2 + x_2x_3 \\
&= \eta + x_1x_2x_3^2 - x_1x_2x_3 - x_1x_2 + x_2x_3.
\end{aligned}$$

We continue by taking $f_g^4 = 1$ as:

$$\begin{aligned}
f_{red}^5 &= f_{red}^4 - (f_g^4)g = f - (f_g^1 + f_g^2 + f_g^3 + f_g^4)g \\
&= \eta + x_1x_2x_3^2 - x_1x_2x_3 - x_1x_2 + x_2x_3 - (\eta + \Lambda) \\
&= -\Lambda + x_1x_2x_3^2 - x_1x_2x_3 - x_1x_2 + x_2x_3, \\
&= x_1x_2x_3^2 - x_1x_2x_3 \in R_\eta.
\end{aligned}$$

Therefore, by taking $f_g = f_g^1 + f_g^2 + f_g^3 + f_g^4$ and $f_{red} = x_1x_2x_3^2 - x_1x_2x_3$ we have $f_{red} = f - (f_g)g$.

Algorithm 1 (REDUCTION)

Input: $f, g \in R$, $g := \eta + \Lambda$ with $\eta = in_{\text{lex}}(g)$ and $\eta \mid in_{\text{lex}}(f)$.

Output: $f_g \in R$ and the reduced form of f as $f_{red} := f - (f_g)g$ such that

$$in_{\text{lex}}(f_{red}) <_{\text{lex}} in_{\text{lex}}(f) \text{ and } in_{\text{lex}}(f) = in_{\text{lex}}((f_g)g).$$

Step 0: Initialize $f_{red} := f$ and $f_g := 0$. Set $F := \{m \in supp(f_{red}) : \eta \mid m\}$.

Step 1: REPEAT

Step 1.1: Update $f_g := f_g + \sum_{m \in F} (\frac{m}{\eta})$; $f_{red} := f_{red} - (f_g)g$ and

$F := \{m \in supp(f_{red}) : \eta \mid m\}$.

UNTIL $F = \varnothing$.

Step 2: Output (f_{red}, f_g).

Algorithm 2 (MAIN)

Input: The reduced Gröbner basis $G = \{g_1, \cdots, g_r\}$ of an ideal I and $f \in R$. Also let

$$\eta_i = in_{\text{lex}}(g_i),\ i = 1, \cdots, r.$$

Output: Unique expression $(f_1, \cdots, f_r)$ with unique remainder $f' \in R_{\eta_1} \cap \cdots \cap R_{\eta_r}$.

Step 0: Initialize the expression $(f_1, \cdots, f_r) := (0, \cdots, 0)$, $f' := 0$, $f_{red} := f$ and

$$Ind\_Set := \{k : 1 \leqslant k \leqslant r \text{ such that } in_{\text{lex}}(g_k) \mid in_{\text{lex}}(f_{red})\}.$$

Step 1: REPEAT

Step 1.1: Let $1 \leqslant l \leqslant r$ be such that

$$in_{\text{lex}}(g_l) = \max_{\text{lex}}\{in_{\text{lex}}(g_k) : \exists k \in Ind\_Set\}.$$

Step 1.2: Let (f_{red}, f_{g_l}) =REDUCTION(f_{red}, g_l).

(Notice that f_{red} in the argument of REDUCTION is different from f_{red} on the left hand side.)

Step 1.3: Update $f_l = f_l + f_{g_l}$ and in turn $(f_1, \cdots, f_r)$. Update $f = f_{red}$ and $Ind\_Set := \{k : 1 \leqslant k \leqslant r \text{ such that } in_{\text{lex}}(g_k) \mid in_{\text{lex}}(f_{red})\}$

UNTIL $Ind\_Set = \varnothing$

Step 2: Set $f' = f_{red}$.

Step 3: Output $(f_1, \cdots, f_r)$ and f'.

Theorem 2 *With the notation given in the algorithm* 2, *it terminates in finitely many steps and is correct. Moreover, the expression* $f = f_1 g_1 + \cdots + f_r g_r + f'$ *is unique and* $f' \in R_{\eta_1} \cap \cdots \cap R_{\eta_r}$.

Proof: For a fixed $1 \leqslant k \leqslant r$, according to the proof of Theorem 1, the initial monomial of the current f_{red}, on reduction with respect to η_k, reduces until $\deg_{\eta_k}(f_{red}) = 0$. This process holds for every k with $1 \leqslant k \leqslant r$. Since the number of k's and the number of stages of the processes are finite, the algorithm stops at a point where none of the monomials in $supp(f_{red})$ is divisible by any of $\eta_k := in(g_k)$'s. Therefore the termination follows. At this stage, we exit the REPEAT-UNTIL loop and we set $f' = f_{red} \in R_{\eta_1} \cap \cdots \cap R_{\eta_r}$. The correctness of the algorithm is the result of (1) in the proof of the Theorem 1. The classical methodology for the uniqueness of the output of such algorithms is given once in [9] page 335 (third paragraph). Similar reasoning holds in our case, in the sense that Step 1.1 gives rise to a unique l and in turn f_{red} will be uniquely determined (by the procedure outlined in the proof of the Theorem 1) as the output of REDUCTION. Therefore the expression in the ouput is unique and the algorithm is a determinate one.

3 Cyclic n-roots $n = 8, 9, 12, 16$

For $n \geqslant 3$, cyclic n-roots is a series of benchmark notorious polynomial systems [6]. The general form of cyclic n-roots polynomial system is $H_1^n = 0, \cdots, H_{n-1}^n = 0, H_n^n = n$ where for $1 \leqslant i \leqslant n$,

$$H_i^n = \sum_{j=1}^{n} \prod_{k=j}^{j+i-1} x_k,$$

and also identify $x_{n+1} = x_1, x_{n+2} = x_2, \cdots$. In this section we need the constant $\omega = \frac{1}{2} - i\frac{\sqrt{3}}{2}$.

The research on cyclic n-roots problem has been initiated by pioneering works of G. Björck, R. Fröberg and J. Backelin. They partially used a computer algebra software to find concise lists of solutions of cyclic n-roots for $n \leqslant 7$, [5, 7]. Cyclic 8-roots was studied by G. Björck and R. Fröberg in [8]. They ended up with a characterization of the solution set of cyclic 8-roots which consists of 16 components, eight of which are of degree 16 and eight of degree 2 and 1152 isolated roots. With an extensive use of computer algebra softwares, in 2001, J. C. Faugère [10] determined the solution set of cyclic 9-roots, which has 6 components of dimension 2 and degree 3 plus 6642 isolated roots. Currently, two numerical-symbolic approaches deal with the problem of symbolic-numerical identification of higher dimensional solution variety of cyclic n-roots polynomial system. (a) The novel method in [12] that is directly aimed to exact identification of the defining polynomials of all prime ideals of positive dimension in primary decomposition of cyclic 12-roots. This method starts with an initial set of true witness points (after removal of so-called junk points) on each components and continues to produce more sample points on the irreducible component. The extra sample points make a numerical rank-deficient generic matrix, for each type of generators of a given degree, i.e, linear, quadratic etc. At this stage of the method almost everything is considered numerically. By finding a so-called deficiency pattern of these matrices, one can retrieve good approximations of the exact form of the coefficients of the defining polynomials of the prime ideal. (b) In a series of publications [2, 3, 4, 13], Jan Verschelde and a research team under his leadership extensively use the concept of tropism to identify the solution set of cyclic n-roots system for various integers n. As an example, they exploit a symmetry in these systems to conclude that the space curves of cyclic 12-roots are quadrics. Also, coefficients of the corresponding puiseux series expansions are found.

Remark 2. The following set of examples discusses cyclic n-roots for $n = 8, 9, 12, 16$. Only the case $n = 12$ is extensively studied via a symbolic-numerical algorithm in [12]. The complete identification for $n = 9$ in [10] is purely symbolic. To some extent, the same is true for $n = 8$ (please see [8]). It turns out that the problem of identification of cyclic n-roots for $n = 8, 9$ by a symbolic-numerical algorithm (as the one given in [12]) has special considerations. This problem for $n = 16$ is of somewhat different nature. They are all in the list of current research of the author. By this time, the form of the ideals involved in these cases are identified. Adding the discussion about the derivation of all ideals for each case of $n = 8, 9$ or $n = 16$ may easily make the size of this work to double or even triple of the current size. Beside, the exposition of the derivations and the problems involved are of different type in comparison with the problem in this work. Thus, to continue our discussion in this paper, we select the following ideal for the case $n = 8$:

$\mathbf{I}^{\mathbf{C_8}} = \langle x_1 + x_6, x_2 + x_5, x_3 + x_8, x_4 + x_7, q, u, p\rangle$,

where $q = -2x_1x_2 + x_1x_3 - x_1x_4 - x_2x_3 + x_2x_4 - 2x_3x_4$, $u = x_1x_2x_3x_4 + 1$ and $p = x_1x_3x_4 - x_2x_3x_4 - x_3 + x_4$, and the following ideal for $n = 16$:

$$\mathbf{I}^{\mathbf{C_{16}}} = \langle x_1 + ix_5, x_2 + ix_6, x_3 + ix_7, x_4 + ix_8, x_1 + x_9, x_2 + x_{10}, x_3 + x_{11}, x_4 + x_{12},$$
$$x_1 - ix_{13}, x_2 - ix_{14}, x_3 - ix_{15}, x_4 - ix_{16}, x_1x_2x_3x_4 - 1\rangle.$$

From the following list of six ideals of dimension 2 for $n = 9$:

$$
\begin{aligned}
I_1 &= \langle x_1 + \bar{\omega}x_7, x_1 + \omega x_4, x_2 + \bar{\omega}x_8, x_2 + \omega x_5, x_3 + \bar{\omega}x_9, x_3 + \omega x_6, x_1x_2x_3 + \omega\rangle,\\
I_2 &= \langle x_1 + \bar{\omega}x_7, x_1 + \omega x_4, x_2 + \bar{\omega}x_8, x_2 + \omega x_5, x_3 + \bar{\omega}x_9, x_3 + \omega x_6, x_1x_2x_3 + \bar{\omega}\rangle,\\
I_3 &= \langle x_1 + \bar{\omega}x_7, x_1 + \omega x_4, x_2 + \bar{\omega}x_8, x_2 + \omega x_5, x_3 + \bar{\omega}x_9, x_3 + \omega x_6, x_1x_2x_3 - 1\rangle,\\
I_4 &= \langle x_1 + \omega x_7, x_1 + \bar{\omega}x_4, x_2 + \omega x_8, x_2 + \bar{\omega}x_5, x_3 + \omega x_9, x_3 + \bar{\omega}x_6, x_1x_2x_3 + \omega\rangle,\\
I_5 &= \langle x_1 + \omega x_7, x_1 + \bar{\omega}x_4, x_2 + \omega x_8, x_2 + \bar{\omega}x_5, x_3 + \omega x_9, x_3 + \bar{\omega}x_6, x_1x_2x_3 + \bar{\omega}\rangle,\\
I_6 &= \langle x_1 + \omega x_7, x_1 + \bar{\omega}x_4, x_2 + \omega x_8, x_2 + \bar{\omega}x_5, x_3 + \omega x_9, x_3 + \bar{\omega}x_6, x_1x_2x_3 - 1\rangle,
\end{aligned}
$$

we select $\mathbf{I}^{\mathbf{C_9}} := I_4$. For $n = 12$ we pick the following ideal from the list given in [12]. For the notation $\mathbf{I}^{\bar{\omega}}_{C_{11}}$ please see [12].

$$
\begin{aligned}
\mathbf{I}^{\mathbf{C_{12}}} := \mathbf{I}^{\bar{\omega}}_{C_{11}} = \langle & x_1 - \omega x_3, x_2 - \omega x_4, x_1 + \omega x_5, x_2 - x_6, x_1 + x_7, x_2 + x_8, x_1 + \omega x_9,\\
& x_2 + \omega x_{10}, x_1 - \omega x_{11}, x_2 + x_{12}, x_1x_2 + \bar{\omega}\rangle.
\end{aligned}
$$

All expressions given in this series of examples, including many others are saved in several MAPLE files. For symbolic verification of the expressions they are available upon request.

<u>***(i)*** $\boldsymbol{n = 8}$.</u> Let $\mathbf{I}^{\mathbf{C_8}} = \langle x_1 + x_6, x_2 + x_5, x_3 + x_8, x_4 + x_7, q, u, p\rangle$, be defined as in the above remark. With the lex order $x_6 >_{\text{lex}} x_5 >_{\text{lex}} x_8 >_{\text{lex}} x_7 >_{\text{lex}} x_1 >_{\text{lex}} x_2 >_{\text{lex}} x_3 >_{\text{lex}} x_4$, using MAPLE, the Gröbner (not reduced) basis of $\mathbf{I}^{\mathbf{C_8}}$ is $G_8 = \{q_1, \cdots, q_{12}\}$, where

$$
\begin{aligned}
q_1 &= x_6 + x_1;\ q_2 = x_5 + x_2;\ q_3 = x_8 + x_3;\ q_4 = x_7 + x_4;\\
q_5 &= 2x_1x_2 - x_1x_3 + x_1x_4 + x_2x_3 - x_2x_4 + 2x_3x_4\\
q_6 &= x_1x_3^2 + x_1x_4^2 + 2x_1 - x_2x_3^2 - x_2x_4^2 - 2x_2 - 2x_3^2x_4 + 2x_3x_4^2 - 2x_3 + 2x_4\\
q_7 &= x_1x_3x_4 - x_2x_3x_4 - x_3 + x_4\\
q_8 &= x_1x_4^3 + 2x_1x_4 - x_2x_4^3 - 2x_2x_4 + 2x_3x_4^3 - x_3x_4 + x_4^2 - 2\\
q_9 &= x_2^2x_3^2 + x_2^2x_4^2 + 2x_2^2 + 2x_2x_3^2x_4 - 2x_2x_3x_4^2 + 2x_2x_3 - 2x_2x_4 + 2x_3x_4 + 2\\
q_{10} &= x_2^2x_3x_4 + x_2x_3 - x_2x_4 + 1\\
q_{11} &= x_2^2x_4^3 + 2x_2^2x_4 - 2x_2x_3x_4^3 + x_2x_3x_4 - x_2x_4^2 + 2x_2 + 2x_3x_4^2 - x_3 + 2x_4\\
q_{12} &= 2x_3^2x_4^2 - x_3^2 + 2x_3x_4 - x_4^2 - 2.
\end{aligned}
$$

In the reduction process of this nonreduced Gröbner basis case, we must take care of the leading coefficients of q_5 and q_{12}. We write

$$\begin{aligned} H_4^8 = f_{red}^1 &= x_6(x_3x_4x_5 + x_4x_5x_7 + x_5x_8x_7 + x_7x_8x_1) + x_1x_2x_3x_4 + x_2x_3x_4x_5 \\ &\quad + x_7x_8x_1x_2 + x_8x_1x_2x_3. \end{aligned}$$

Since $in_{\text{lex}}(q_1) = x_6$ let $f_{q_1} = x_3x_4x_5 + x_4x_5x_7 + x_5x_8x_7 + x_7x_8x_1$, then

$$\begin{aligned} f_{red}^2 &= f_{red}^1 - (f_{q_1})q_1 \\ &= x_5(x_2x_3x_4 - x_3x_4x_1 - x_4x_7x_1 - x_7x_8x_1) + x_1x_2x_3x_4 + x_7x_8x_1x_2 \\ &\quad + x_8x_1x_2x_3 - x_7x_8x_1^2. \end{aligned}$$

Similarly, with $in_{\text{lex}}(q_2) = x_5$, $in_{\text{lex}}(q_3) = x_8$ and $in_{\text{lex}}(q_4) = x_7$, we have

$$\begin{aligned} f_{q_2} &= x_2x_3x_4 - x_3x_4x_1 - x_4x_7x_1 - x_7x_8x_1, \\ f_{q_3} &= 2x_7x_1x_2 + x_1x_2x_3 - x_7x_1^2, \\ f_{q_4} &= x_1x_2x_4 - 2x_1x_2x_3 + x_1^2x_3. \end{aligned}$$

At this stage to the end, the general feature of the Do-While in algorithm 2 shows up. Set

$$\begin{aligned} f_{red}^5 &= f_{red}^1 - (f_{q_1}q_1 + f_{q_2}q_2 + f_{q_3}q_3 + f_{q_4}q_4), \\ &= -x_1^2x_3x_4 - x_1x_2x_3^2 + 4x_1x_2x_3x_4 - x_1x_2x_4^2 - x_2^2x_3x_4, \\ &= x_1x_3x_4(4x_2 - x_1) - x_1x_2x_3^2 - x_1x_2x_4^2 - x_2^2x_3x_4. \end{aligned}$$

Notice that $in_{\text{lex}}(f_{red}^5) = x_1^2x_3x_4$ is divisible by $in_{\text{lex}}(q_7) = x_1x_3x_4$. So far, members of the basis that constitute a so-called chain of reduction $q_1 \to q_2 \to q_3 \to q_4 \to q_7$ evidently are q_1, q_2, q_3, q_4, q_7. Let $f_{q_7}^0 = 4x_2 - x_1$ and

$$\begin{aligned} f_{red}^7 &= f_{red}^5 - (f_{q_7})q_7, \\ &= x_1x_2(-x_3^2 - x_3x_4 - x_4^2) - x_1x_3 + x_1x_4 + 3x_2^2x_3x_4 + 4x_2x_3 - 4x_2x_4. \end{aligned}$$

Now $in_{\text{lex}}(f_{red}^7) = x_1x_2x_3^2$ is divisible only by $in_{\text{lex}}(q_5) = x_1x_2$. Set
$f_{q_5} = \frac{1}{2}(-x_3^2 - x_3x_4 - x_4^2)$ and calculate

$$\begin{aligned} f^8_{red} &= f^7_{red} - (f_{q_5})q_5, \\ &= -0.5x_1x_3^3 - x_1x_3 + 0.5x_1x_4^3 + x_1x_4 + 3x_2^2x_3x_4 + 0.5x_2x_3^3 + 4x_2x_3 \\ &\quad -0.5x_2x_4^3 - 4x_2x_4 + x_3^3x_4 + x_3^2x_4^2 + x_3x_4^3. \end{aligned}$$

The subsequent reduction

$$\begin{aligned} f^9_{red} &= f^8_{red} - (f_{q_6})q_6, \\ &= 0.5x_1x_3x_4^2 + 0.5x_1x_4^3 + x_1x_4 + 3x_2^2x_3x_4 - 0.5x_2x_3x_4^2 + 3x_2x_3 - 0.5x_2x_4^3 \\ &\quad -4x_2x_4 + 2x_3^2x_4^2 - x_3^2 + x_3x_4^3 + x_3x_4, \end{aligned}$$

holds with $f_{q_6} = -0.5x_3$. Let $f^1_{q_7} = 0.5x_4$. Then

$$\begin{aligned} f^{10}_{red} &= f^9_{red} - (f^1_{q_7})q_7, \\ &= 0.5x_1x_4^3 + x_1x_4 + 3x_2^2x_3x_4 + 3x_2x_3 - 0.5x_2x_4^3 - 4x_2x_4 + 2x_3^2x_4^2 - x_3^2 \\ &\quad +x_3x_4^3 + 1.5x_3x_4 - 0.5x_4^2. \end{aligned}$$

We continue by setting $f_{q_8} = 0.5$ and

$$f^{11}_{red} = f^{10}_{red} - (f_{q_8})q_8 = 3x_2^2x_3x_4 + 3x_2x_3 - 3x_2x_4 + 2x_3^2x_4^2 - x_3^2 + 2x_3x_4 - x_4^2 + 1.$$

For $f_{q_{10}} = 3$ we have

$$f^{12}_{red} = f^{11}_{red} - (f_{q_{10}})q_{10} = 2x_3^2x_4^2 - x_3^2 + 2x_3x_4 - x_4^2 - 2.$$

At last, $f_{q_{12}} = 1$ results $f^{13}_{red} = f^{12}_{red} - (f_{q_{12}})q_{12} = 0$. Therefore,

$$H^8_4 = f^{11}_{red} - (f_{q_{10}})q_{10} = 2x_3^2x_4^2 - x_3^2 + 2x_3x_4 - x_4^2 - 2.$$

Using any computer algebra system, the above process can be verified symbolically. One may verify that

$$\begin{aligned} H^8_4 &= f_{q_1}q_1 + f_{q_2}q_2 + f_{q_3}q_3 + f_{q_4}q_4 + f_{q_5}q_5 + f_{q_6}q_6 + (f^0_{q_7} + f^1_{q_7})q_7 + f_{q_8}q_8 \\ &\quad +f_{q_{10}}q_{10} + f_{q_{12}}q_{12}, \end{aligned}$$

is indeed an expression of H_4^8. The so-called chain of reduction in this process would be $q_1 \to q_2 \to q_3 \to q_4 \to q_7 \to q_5 \to q_6 \to q_7 \to q_8 \to q_{10} \to q_{12}$.

(ii) $\boldsymbol{n = 9.}$ We implement algorithm 2 on $\mathbf{I^{C_9}}$ and we find the expression corresponding to H_4^9. With respect to the lex order $x_1 >_{\text{lex}} \cdots >_{\text{lex}} x_9$, the reduced Gröbner basis of $\mathbf{I^{C_9}}$ is:

$$\widetilde{G}_4^9 = \{g_1 = x_1 + \omega x_7, g_2 = x_2 + \omega x_8, g_3 = x_3 + \omega x_9, g_4 = x_4 + \bar{\omega} x_7,$$
$$g_5 = x_5 + \bar{\omega} x_8, g_6 = x_6 + \bar{\omega} x_9, h = x_7 x_8 x_9 + \omega\}.$$

We start by setting:

$$\begin{aligned} f_{red}^1 &= H_4^9 = x_1x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_6 + x_4x_5x_6x_7 + x_5x_6x_7x_8 \\ &\quad + x_6x_7x_8x_9 + x_7x_8x_9x_1 + x_8x_9x_1x_2 + x_9x_1x_2x_3, \\ &= x_1(x_2x_3x_4 + x_2x_3x_9 + x_2x_8x_9 + x_8x_7x_9) + x_2x_3x_4x_5 + x_3x_4x_5x_6 \\ &\quad + x_4x_5x_6x_7 + x_5x_6x_7x_8 + x_6x_7x_8x_9. \end{aligned}$$

Let $f_{g_1} = x_2x_3x_4 + x_2x_3x_9 + x_2x_8x_9 + x_8x_7x_9$ and $f_{red}^2 = f_{red}^1 - (f_{g_1})g_1$. Then we have

$$\begin{aligned} f_{red}^2 &= f_{red}^1 - (f_{g_1})g_1 \\ &= x_2(x_3x_4x_5 - \omega(x_3x_4x_7 + x_3x_7x_9 + x_8x_7x_9)) \\ &\quad + x_3x_4x_5x_6 + x_4x_5x_6x_7 + x_5x_6x_7x_8 + x_6x_7x_8x_9 - \omega x_7^2x_8x_9. \end{aligned}$$

Then we let $f_{g_2} = x_3x_4x_5 - \omega(x_3x_4x_7 + x_3x_7x_9 + x_8x_7x_9)$ and we continue the process to find $f_{red}^3, f_{red}^4, \cdots$. We have the following:

$$\begin{aligned} f_{g_3} &= x_5x_6x_4 - \omega x_4x_5x_8 - \bar{\omega} x_4x_7x_8 - \bar{\omega} x_7x_8x_9, \\ f_{g_4} &= x_5x_6x_7 - \omega x_5x_6x_9 - \bar{\omega} x_5x_8x_9 + x_7x_8x_9, \\ f_{g_5} &= -\bar{\omega} x_6x_7^2 + x_6x_7x_8 + x_6x_7x_9 - \omega x_7x_8x_9, \\ f_{g_6} &= -\omega x_7^2x_8 - \bar{\omega} x_7x_8^2 + \omega x_7x_8x_9. \end{aligned}$$

It can be verified that $(f_{g_1}, f_{g_2}, f_{g_3}, f_{g_4}, f_{g_5}, f_{g_6}, 0)$ is an expression for H_4^9.

(iii) $\boldsymbol{n} = \mathbf{12}$**.** We implement the algorithm 2 on $\mathbf{I}^{\mathbf{C_{12}}}$ and we find an expression for H_2^{12} as a member of $\mathbf{I}^{\mathbf{C_{12}}}$ which follows:

$$\begin{aligned} H_2^{12} &= -\bar{\omega}(x_2+x_4)g_1 + (\omega x_1 - \bar{\omega}x_5)g_2 + (\bar{\omega}x_6 - \omega x_2)g_3 + (\bar{\omega}x_1 - x_7)g_4 \\ &\quad +(x_2+x_8)g_5 + (x_9 - x_1)g_6 + \bar{\omega}(x_{10} - x_2)g_7 + (\bar{\omega}x_{11} + \omega x_1)g_8 \\ &\quad -(\bar{\omega}x_{12} + \omega x_2)g_9 + (\tfrac{3}{2} + \tfrac{i\sqrt{3}}{2})x_1 g_{10}, \\ &= x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_6 + x_6x_7 + x_7x_8 + x_8x_9 + x_9x_{10} \\ &\quad +x_{10}x_{11} + x_{11}x_{12} + x_{12}x_1, \end{aligned}$$

where $g_1 := x_1 - \omega x_3, g_2 := x_2 - \omega x_4, g_3 := x_1 + \omega x_5, g_4 := x_2 - x_6, g_5 := x_1 + x_7,$

$g_6 := x_2 + x_8, g_7 := x_1 + \omega x_9, g_8 := x_2 + \omega x_{10}, g_9 := x_1 - \omega x_{11}, g_{10} := x_2 + x_{12},$

$g_{11} := x_1x_2 + \bar{\omega}.$

(iv) $\boldsymbol{n} = \mathbf{16}$**.** The expression for H_3^{16} as a memeber of $\mathbf{I}^{\mathbf{C_{16}}}$ can be treated as in the previous cases. We have

$$\begin{aligned} H_3^{16} &= (-i(x_3x_4 + x_6x_7 + x_4x_6))h_1 + (x_4x_1 + x_1x_7 - ix_7x_8)h_2, \\ &\quad +(-ix_8x_9 + x_2x_8 + ix_1x_2)h_3 + (x_3x_9 - ix_9x_{10} + ix_2x_3)h_4, \\ &\quad +(-x_3x_4 + x_{10}x_{11} + ix_4x_{10})h_5 + (x_{11}x_{12} - ix_1x_4 - x_1x_{11})h_6, \\ &\quad +(x_1x_2 - x_2x_{12} + x_{12}x_{13})h_7 + (x_2x_3 - x_3x_{13} + x_{13}x_{14})h_8, \\ &\quad +i(x_{14}x_{15} + x_3x_4 - x_4x_{14})h_9 + (x_1x_{15} - x_4x_1 + ix_{15}x_{16})h_{10}, \\ &\quad +(x_2x_{16} - ix_1x_2 + ix_1x_{16})h_{11} + (-ix_2x_3 + ix_1x_2 + x_1x_3)h_{12} \\ &= x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_6 + x_5x_6x_7 + x_6x_7x_8 + x_7x_8x_9 + \\ &\quad x_8x_9x_{10} + x_9x_{10}x_{11} + x_{10}x_{11}x_{12} + x_{11}x_{12}x_{13} + x_{12}x_{13}x_{14} + x_{13}x_{14}x_{15} \\ &\quad +x_{14}x_{15}x_{16} + x_{15}x_{16}x_1 + x_{16}x_1x_2. \end{aligned}$$

$h_1 := x_1 + ix_5, h_2 := x_2 + ix_6, h_3 := x_3 + ix_7, h_4 := x_4 + ix_8, h_5 := x_1 + x_9,$

$h_6 := x_2 + x_{10}, h_7 := x_3 + x_{11}, h_8 := x_4 + x_{12}, h_9 := x_1 - ix_{13}, h_{10} := x_2 - ix_{14},$

$h_{11} := x_3 - ix_{15}, h_{12} := x_4 - ix_{16}, h_{13} := x_1x_2x_3x_4 - 1.$

References

[1] Adams, W. W. and Loustanau, P., *An Introduction to Gröbner Bases.* Graduate Studies in Mathematics, American Mathematical Society, 1996.

[2] Adrovic, D., *Solving Polynomial Systems With Tropical Methods.* PhD thesis, University of Illinois at Chicago, Chicago, 2012.

[3] Adrovic, D. and Verschelde, J., Computing Puiseux Series for Algebraic Surfaces. the abstract and revised manuscript. In *ISSAC 2012: Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation.* Grenoble, France. Edited by Joris van der Hoeven and Mark van Hoeij, ACM pages 20-27, July 22-25, 2012.

[4] Adrovic, D. and Verschelde, J., Polyhedral Methods for Space Curves Exploiting Symmetry Applied to the Cyclic n-roots Problem. The abstract and (revised) manuscript, Accepted for publication in the *proceedings of CASC 2013.*

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

[6] Bini, D. and Morrain, B., Polynomial test suit. Available at http://www-sop.inria.fr/saga/POL/BASE/2.multipol/cyclic.hml.

[7] Björck, G. and Fröberg, R., A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots. *Journal of Symbolic Computation,* 12, pp.329-336, 1991.

[8] 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 pp. 57-70, 1992.

[9] Eisenbud, D., *Commutative Algebra with a view toward algebraic geometry*. Springer-Verlag (paperback edition), 2004.

[10] 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. 1-12, 2001.

[11] Herzog, J. and Hibi, T. *Monomial Ideals.* Graduate Texts in Mathematics 260, Springer-Verlag, 2011.

[12] Sabeti, R. Numerical-symbolic exact irreducible decomposition of cyclic-12. *LMS Journal of Computation and Mathematics.* 14, pages: 155-172, 2011.

[13] Verschelde, J. Polyhedral Methods in Numerical Algebraic Geometry. The abstract and (revised) manuscript, In: Interactions of Classical and Numerical Algebraic Geometry. edited by Dan Bates, GianMario Besana, Sandra Di Rocco, and Charles Wampler, *Contemporary Mathematics.* 496, pages AMS, 243-263, 2009.