Groebner basis' attack to multivariate cryptography

"Seminari CrypTO"- Politecnico di Torino

Giancarlo Rinaldo

University of Messina

April 23, 2024

Table of Contents

Bibliography

Pj J. Patarin, *Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms* , International Conference on the Theory and Applications of Cryptographic Techniques,1996.

FJ J. Faugere, A. Joux, *Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases*, Annual International Cryptology Conference, 2003.

F99 J. Faugere, *A new efficient algorithm for computing Gröbner bases (F_4)*, Journal of Pure and Applied Algebra, 1999.

F04 J. Faugere, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5)*, ISSAC, 2002.

Pb B. Parisse, *Computing huge Gröbner basis like cyclic10 over $\mathbb{Q}$ with giac*, arXiv:1903.12427, 2019.

CLO D. Cox, J, Little, D. O'Shea, Ideals, Varieties, and Algorithms, Springer, UTM, 4th Edition, 2015.

Table of Contents

Digital Signatures

A Digital Signature Scheme consists of three algorithms:

- $\mathrm{KeyGen}(\kappa) \to (k, P)$: given a security parameter κ generates a public key P and a secret key k.
- $\mathrm{Sign}(m, k) \to s$: given a message m and the secret key k, computes a digital signature s of m.
- $\mathrm{Ver}(m, s, P) \to r$: given a message m, a signature s and the public key P, it outputs whether or not s is a valid signature of m.

Post-Quantum Cryptography

In the last years, lot of effort was put into Post-Quantum Cryptography, that is, algorithms designed to be resistant even against attacks using quantum computers. Post-Quantum Cryptography includes:

- Multivariate Cryptography;
- Code-based Cryptography;
- Hash-based Cryptography;
- Lattice-based Cryptography;
- Supersingular Elliptic Curve Isogeny Cryptography.

Multivariate Cryptography

Multivariate Cryptography is based on the following problem:

Multivariate Quadratic Problem (MQ Problem)

Let K be a field and let $p_1, \ldots, p_m \in K[x_1, \ldots, x_n]$ be m quadratic polynomials in n variables. The MQ Problem consists in finding a solution $(\alpha_1, \ldots, \alpha_n) \in K^n$ of the system:

$$\begin{cases} p_1(x_1, \ldots, x_n) = 0, \\ \vdots \\ p_m(x_1, \ldots, x_n) = 0. \end{cases}$$

NIST PQC Competition

In 2016, the National Institute of Standards and Technology (NIST) started a competition to select the Post-Quantum cryptosystems more fit for standardization. Two Multivariate Public Key Cryptosystems were proposed:

- **Rainbow**, based on a multi-layer version of the Unbalanced Oil & Vinegar scheme;
- **GeMSS** (Great Multivariate Short Signature) based on $HFEv-$.

Table of Contents

Hidden Field Equations (HFE)

Idea behind HFE Cryptosystem

We wish to construct a seemingly random system of polynomial equations after composing several maps that are easy to invert. The seemingly random system of equations is our public key, while the underlying composition is the secret key. We use equations induced by field extension to reach the goal.

Hidden Field Equations (HFE)

HFE was invented by Patarin in 1996 [Pj].

- The design of *HFE* depends on a parameter D which determines the efficiency of the cryptosystem.
- The paper [FJ] presents algebraic attacks based on Grobner basis.
- The HFE cryptosystem can also be generalized producing:
  - *HFE*− (HFE-Minus);
  - $HFE^{\pm}$ (HFE-Plus-Minus);
  - *HFEv*;
  - *HFEv*−

  The last two variants are constructed by combining the idea of *Oil-Vinegar* and the *Minus method*.

Basic HFE

Let $\mathbb{F}$ be a finite field with cardinality q, where q is the power of a prime p, and let $g(x) \in \mathbb{F}[x]$ be an irreducible polynomial of degree n. Let $\mathbb{E}$ be an extension of $\mathbb{F}$ of degree n, $\mathbb{E} \cong \mathbb{F}[x]/g(x)$.
Let ϕ be the standard $\mathbb{F}$-linear map that identifies $\mathbb{E}$ with $\mathbb{F}^n$:

$$\phi : \mathbb{E} \to \mathbb{F}^n$$

$$\sum_{i=0}^{n-1} a_i x^i \to (a_0, \ldots, a_{n-1}).$$

where x is a primitive root of $g(x)$.

Central Polynomial

The fundamental idea of *HFE* is to find a polynomial $F(X) \in \mathbb{E}[X]$, denoted the *central polynomial*, which can be easily inverted, and then find the representation of this polynomial as a map from $\mathbb{F}^n$ to $\mathbb{F}^n$. The central map has the following form:

$$F : \mathbb{E} \to \mathbb{E}$$

$$X \to \sum_{i=0}^{r_2-1} \sum_{j=0}^{i} a_{ij} X^{q^i+q^j} + \sum_{i=0}^{r_1-1} b_i X^{q^i} + c,$$

where $a_{ij}, b_i, c \in \mathbb{E}$ random, $r_1, r_2 \in \mathbb{N}$ are chosen such that $\deg F \leq D$ and we fix $X = x_1 + x_2 x + \cdots + x_n x^{n-1}$, $x_i \in \mathbb{F}$.

Central Polynomial

After applying F on X we obtain the following element in $\mathbb{E}$,

$$F(X) = f_1 + f_2 x + \cdots + f_n x^{n-1},$$

where f_i depends on $(x_1, \ldots, x_n)$ and are quadratic.
By applying ϕ we define $F' = \phi \circ F \circ \phi^{-1}$:

$$\begin{aligned} F' : \mathbb{F}^n &\to \mathbb{F}^n \\ (x_1, \ldots, x_n) &\to (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) . \end{aligned}$$

Observation

We note that F' represents the central polynomial in its multivariate representation over $\mathbb{F}^n$, while F denotes the central polynomial in its univariate representation over $\mathbb{E}$.

Final HFE construction

Let S, T be two affine invertible transformations over $\mathbb{F}^n$.
The final system of polynomials produced by the HFE construction is:

$$P : \mathbb{F}^n \to \mathbb{F}^n$$
$$P = S \circ F' \circ T = S \circ \phi \circ F \circ \phi^{-1} \circ T.$$

Observation

The transformations S, T are crucial for the cryptosystem, as they are used to hide the structure of the central polynomial.

HFE Cryptosystem

- **Public Key:** it includes the following information:
  - The field $\mathbb{F}$.
  - The map P or equivalently its n quadratic components: $(p_1(x_1, \ldots, x_n), \ldots, p_n(x_1, \ldots, x_n))$ with $p_i(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$.
- **Secret Key:**it includes the following information:
  - The central polynomial F,
  - The maps S, T.

The HFE Cryptosystem is a *Bipolar system*.

HFE Cryptosystem - Encryption

Given a plaintext message $(M_1, \ldots, M_n) \in \mathbb{F}^n$, the corresponding ciphertext is:

$$(C_1, \ldots, C_n) = P((M_1, \ldots, M_n))$$

or equivalently

$$C_i = p_i((M_1, \ldots, M_n))$$

for all $i = 1, \ldots, n$.

HFE Cryptosystem - Decryption I

Recall that $P = S \circ F' \circ T = S \circ \phi \circ F \circ \phi^{-1} \circ T$.
Given the ciphertext $(C_1, \ldots, C_n)$, decryption works as follows:

- compute $(\bar{C}_1, \ldots, \bar{C}_n) = S^{-1}((C_1, \ldots, C_n))$,
- let $\bar{c} = \phi^{-1}(\bar{C}_1, \ldots, \bar{C}_n)$, compute (Berlekamp's algorithm)

$$\mathcal{Z} = \{z \in \mathbb{E} \mid F(z) = \bar{c}\}.$$

If $D = \deg F(X)$, then the complexity of this step will be $\mathcal{O}(nD^2 \log D + D^3)$. From this we see that D cannot be too large, since otherwise the decryption process is inefficient. Equivalently, we must not choose r_1, r_2 to be too large.

HFE Cryptosystem - Decryption II

- compute $\forall z \in \mathcal{Z}$:

$$T^{-1} \circ \phi(z) = (M_{i,1}, \ldots M_{i,n})$$

Although we would like that F to be a one-to-one map, it is possible that $\mid \mathcal{Z} \mid > 1$. In this case we can use one of several techniques (hash functions, Plus method, etc.) to detect the plaintext among the solutions.

Table of Contents

Monomial order

A monomial ordering $>$ on $K[x_1, \ldots, x_n]$ is a relation on the set of monomials x^α with $\alpha \in \mathbb{Z}^n_{\geq 0}$, satisfying:

1. $>$ is a total ordering on $\mathbb{Z}^n_{\geq 0}$
2. If $\alpha > \beta$ and $\gamma \in \mathbb{Z}^n_{\geq 0}$, then $\alpha + \gamma > \beta + \gamma$
3. $>$ is a well ordering on $\mathbb{Z}^n_{\geq 0}$.

The most used one is the *d*egrevlex order, that we use from now, on. Let $|\alpha| = \sum_{i=1}^n \alpha_i$ then $\alpha > \beta$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and the rightmost nonzero entry of $\alpha - \beta$ is negative.

Leading term ideal

Definition

Let $I = (f_1, \ldots, f_r)$ be any ideal in $K[x_1, \ldots, x_n]$ and $<$ a monomial order, then

$$LT(I) = (LT(f) : f \in I).$$

Note that this is a monomial ideal coming from a "degeneration" of the starting ideal, that maintains most important invariants of the ideal I.

Macaulay's Lemma

The dimension of vector spaces of degree d does not change under LT deformation. Namely,

$$\dim_K(R/I)_d = dim_K(R/LT(I))_d.$$

At that time there was no clear way to compute it.

Gröbner basis definition

B. Buchberger (1965) in his PhD thesis defined the following

Definition

Let $I = (f_1, \ldots, f_r)$ be any ideal in $K[x_1, \ldots, x_n]$ and $<$ a monomial order, then $G := \{g_1, \ldots, g_s\}$ is a Gröbner basis if

$$LT(I) = (LT(g_1), \ldots, LT(g_s)).$$

Moreover, provided a way to compute $G = \{g_1, \ldots, g_s\}$. The basis depends on $<$.

Computation by example

Let $I = (f_1, f_2) = (x^3 - 2xy, x^2y - 2y^2 + x)$. We start with $G = \{f_1, f_2\}$ and we want to find the hidden leading terms of $f \in I$. So we mutually cancel the leading terms of f_1 and f_2 taking the least common multiple of $LT(f_1)$ and $LT(f_2)$, namely x^3y and consider the polynomial in I

$$S(f_1, f_2) = \frac{x^3y}{LT(f_1)} f_1 - \frac{x^3y}{LT(f_2)} f_2 = -x^2.$$

We observe that $-x^2 \notin (LT(f_1), LT(f_2))$, hence we add it, $G = \{f_1, f_2, f_3\}$. Another, hidden polynomial cames from $S(f_1, f_3) = -2xy = f_4$. The last new polynomial arises from $S(f_2, f_3) = -2y^2 + x = f_5$. Now, $S(f_i, f_j)$ for all $i, j \in \{1, 2, 3, 4, 5\}$ (after the reduction step) goes to zero. In particular

$$LT(I) = (x^2, y^2, xy).$$

Reduction step

In general $S(f_i, f_j)$ need to be reduced in the sense that there exist a polynomial $f \in G$ such that the $LT(f)$ divides $LT(S(f_i, f_j))$. Hence we need to perform the division algorithm in many variables with many possible divisors in G, to check if the remainder is nonzero hence a new element of G. This is the most most expensive part of the algorithm! Moreover, it is very often useless, since we have a "reduction to zero".

The homogeneous case

Let I be a homogeneous ideal then

$$I = \oplus_{d \geq 0} I_d$$

We observe that for any monomial order the (reduced) S-pairs are homogeneous, too, with a non-decreasing total degree. That is we can define an algorithm computing each I_d in an "ordered way".
Moreover each I_d is computed in an efficient way using linear algebra and Gauss-elimination.
We show an example. Let $f_1 = (x^2 - 2y^2 - 2yz - z^2)$,
$f_2 = (-xy + 2yz + z^2)$, and $f_3 = (-x^2 + xy + xz + z^2)$.
Fix the degree revlex ordering with $x > y > z$ in $K[x, y, z]$

The matrix M_2

Consider the matrix representing the $K-$vector space I_2 with columns associated to the ordered monomials $x^2 > xy > y^2 > xz > yz > z^2$ and rows representing the coefficients of f_1, f_2, and f_3. We have

$$M_2 = \begin{pmatrix} 1 & 0 & -2 & 0 & -2 & -1 \\ 0 & -1 & 0 & 0 & 2 & 1 \\ -1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

and after Gaussian reduction we obtain

$$M_2' = \begin{pmatrix} 1 & 0 & 0 & -1 & -2 & -2 \\ 0 & 1 & 0 & 0 & -2 & -1 \\ 0 & 0 & 1 & -\frac{1}{2} & 0 & -\frac{1}{2} \end{pmatrix}$$

The matrix M_3

In a similar way we define the matrix representing the $K-$vector space I_3 with columns associated to the ordered monomials $x^3 > x^2y > xy^2 > y^3 > xyz > y^2z > xz^2 > yz^2 > z^3$ and rows representing the coefficients of xf_1, yf_1, $zf_1, \ldots, zf_3$. The matrix obtained is much bigger but can use the reduced one M_2'. After Gaussian reduction we obtain M_3'.
We observe that in each step we are computing the Gröbner basis of I_d (e.g. $d = 2, 3$).
To stop the algorithm we need to know the Hilbert-Poincarè series of I and compare with the leading term ideal of the matrices M_d.

F_4 algorithms

The F_4 algorithm was introduced by Faugère (1999). There is a family of algorithms with many variants and alternatives. The common properties are:

1. In F_4 they use linear algebra as in the homogeneous case. That is S-polynomials are "substituted" by Gaussian reduction.
2. F_4 algorithms do not necessarily proceed strictly degree by degree, as in the homogeneous case.
3. F_4 algorithms use a termination derived by Buchberger's criterion.

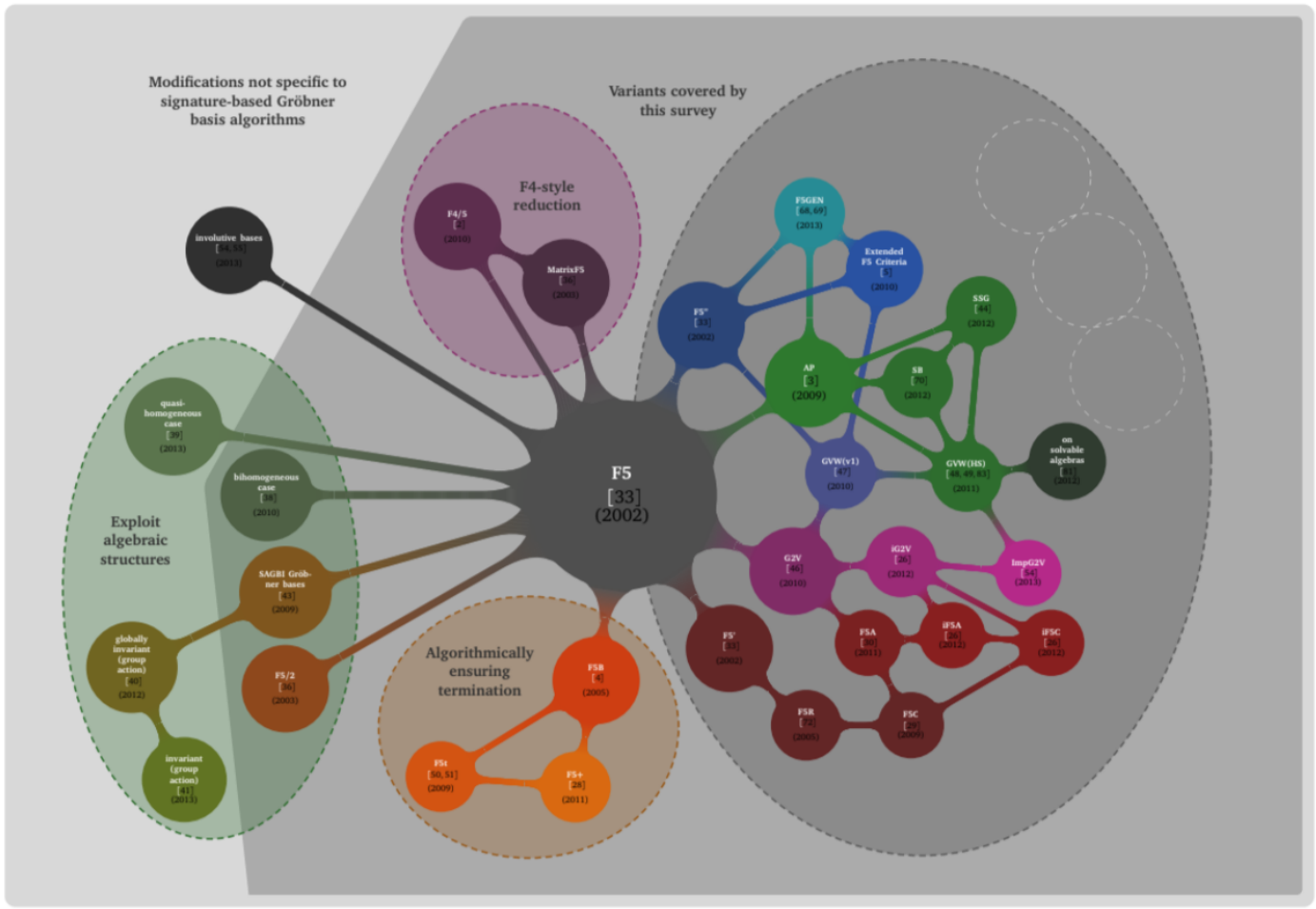
F_5: The signature based algorithms

The F_5 algorithm was introduced by Faugère (2002). There is a family of with many variants and alternatives. In a recent survey Eder and Faugère (2014) clarify the picture (including also the F_4 algorithms).

1. F_5 algorithms have been successful in solving previous intractable problems (e.g. cryptographic applications, e.g. HFE)
2. In (2002) Faugère did not provide a complete termination and correcteness. Now we have complete proofs and a termination of the algorithms (e.g. Survey (2014)).

Here is the picture taken from the survey

A big family


Modifications not specific to signature-based Gröbner basis algorithms
Variants covered by this survey
F4-style reduction
Exploit algebraic structures
Algorithmically ensuring termination
F5 [33] (2002)
F4/5 [2] (2010)
MatrixF5 [24] (2003)
involutive bases [54, 55] (2013)
quasi-homogeneous case [39] (2013)
bihomogeneous case [38] (2010)
SAGBI Gröbner bases [43] (2009)
globally invariant (group action) [42] (2012)
invariant (group action) [41] (2013)
F5/2 [36] (2003)
F5R [4] (2005)
F5t [50, 51] (2009)
F5+ [28] (2011)
F5GEN [68, 69] (2013)
Extended F5 Criteria [5] (2010)
F5' [33] (2002)
SSG [44] (2012)
AP [3] (2009)
SB [70] (2012)
GVW(v1) [47] (2010)
GVW(HS) [48, 49, 83] (2011)
on solvable algebras [3] (2012)
G2V [46] (2010)
iG2V [26] (2012)
impG2V [44] (2013)
F5' [33] (2002)
F5A [30] (2011)
iF5A [26] (2012)
iF5C [26] (2012)
F5R [74] (2005)
F5C [29] (2009)

Syzygies

Let $R = K[x_1, \ldots, x_n]$ a polynomial ring over a field K, $I = (f_1, \ldots, f_s) \subset R$. We have the following natural surjection

$$\phi : R^s \to I$$

with $\phi(\mathbf{a}) = \sum_{i=1}^{s} a_i f_i$ and $\mathbf{a} = (a_1, \ldots, a_s)$, $a \in R^s$ is a syzygy, namely an element of $\ker \phi$, if

$$\phi(\mathbf{a}) = \sum_{i=1}^{s} a_i f_i = 0$$

A very well known examples are the Koszul sygygies

$$f_i \mathbf{e_j} - f_j \mathbf{e_i}.$$

POT (position over term) order and signatures

The POT order on R^s is defined by

$$x^\alpha \mathbf{e}_i > x^\beta \mathbf{e}_j \iff i > j, \text{ or } i = j \text{ and } x^\alpha > x^\beta$$

The *signature* of $\mathbf{g} \in R^n$, $\mathfrak{s}(g)$, is the leading term of g w.r.t. POT, with $\mathfrak{s}(g) \in R^n$.
Let $g, h \in R^s$. An $\mathfrak{s}$-*reduction* of g by h is $f = g - cx^\alpha h$, where $c \in K$ and

1. there is a term in the polynomial $\phi(g)$ that is equal to $LT(cx^\alpha \phi(h))$
2. $\mathfrak{s}(g) \geq \mathfrak{s}(x^\alpha h)$

The $\mathfrak{s}$-reduction is analogous to one-step in a division algorithm.

Signatures as a pair

Since the signature is a vector of zero entries, but in position ℓ where we have a monomial, we can write it as a pair

$$\mathfrak{s}(f) = (LM(f), \ell).$$

Consider the ideal $I = (f_1, f_2)$ with $f_1 = x^2 + z$, $f_2 = xy - z$. Then $\mathfrak{s}(f_1) = (1, 1)$, $\mathfrak{s}(f_2) = (1, 2)$. Moreover,

$$f_3 = S(f_1, f_2) = yf_1 - xf_2.$$

And $\mathfrak{s}(f_3) = x\mathfrak{s}(f_2) = (x, 2)$.
We observe that $xz + yz = f_3$, and it is reduced (and in particular $\mathfrak{s}$-reduced). So f_3 is a new element of the Gröbner basis.

A useless S-pair

But,

$$f_4 = S(f_1, f_3) = zf_1 - xf_3,$$

and $\mathfrak{s}(f_4) = x\mathfrak{s}(f_3) = (x^2, 2)$, Using this fact it is sufficient to see that f_4 reduces to zero. (*)
In fact, by doing the computation, we have that

$$f_4 = z^2 - xyz = -zf_2$$

that reduces to zero. To have a glimpse of (*), we observe that

$$S(f_1, f_3) = zf_1 - x(yf_1 - xf_2) = (-f_2, f_1 - z)(f_1, f_2),$$

that is similar to a Koszul syzygy $(-f_2, f_1)(f_1, f_2)$. Moreover $f_1\mathbf{e_2} - f_2\mathbf{e_1}$ has signature $(x^2, 2)(= \mathfrak{s}(f_4))$.
Hence we know "a-priori" that $S(f_1, f_3)$ reduces to 0.

F_5 criterion

For the sake of simplicity we assume that the polynomials are monic.

Theorem

$S(p, q) = u_p p - u_q q$ reduces to zero, if $\mathfrak{s}(p) = (t, \ell)$ and there exists an element $g \in G_{\ell-1}$ such that

$$LT(g) | u_p t.$$

In the previous example $g \in G_1 = \{x^2 + z\}$ and $u_p t = x^2$ in $S(p, q)$, with $p = f_3$.
We observe that F_5 computes a Gröbner basis incrementally with respect to ℓ.

Table of Contents

Cyclic n ideals: Computation with Sage

Sagemath is a "wrapper" of two nice libraries for Gröbner basis computation: Singular (standard algorithms) and giac (Faugere's algorithms).
In my laptop with Intel i5 and 8 Gigabytes, I computed the Gröbner bases of Cyclic ideals n with $n \in \{3, 4, 5, 6, 7\}$ on the field $\mathbb{Q}$. These ideals has been used as a test in Faugere's papers (considering also the cases within 9 elements).
These are "nice" ideals: e.g. Cyclic 3 is

$$(x + y + z, xy + xz + yz, xyz - 1),$$

Cyclic 4 is

$$(x + y + z + t, xy + yz + xt + zt, xyz + xyt + xzt + yzt, xyzt - 1),$$

and so on.

Gröbner basis of Cyclic 5, 7 and 10

Let G be the Gröbner basis of our cyclic ideal. If $n = 5$, the first element of G is:

$$t^2u^6 + 28yzt + 14z^2t - 21yt^2 - 12zt^2 - 12t^3 - 11yzu + 3z^2u + 9ytu +$$

$$+17ztu - 30t^2u - 5yu^2 + 29zu^2 - 28tu^2 + 18u^3,$$

and there are other 20 polynomials in G!
Doing the same computation for cyclic 7 using standard strategies needs, surely more than 30 minutes, on my laptop. But computing using giac needs only 7 seconds.
Recently, in [Pb] the author of giac, computed the Groebner basis of Cyclic 10 for the first time, obtaining a 25 Gigabytes as output and using parallel computation.