FGLM and coprime polynomial pairs

Pasqualina Fragneto (pasqualina.fragneto@st.com)
STMicroelectronics, AST Agrate - Milano, Italy.

Anna Rimoldi (rimoldi@science.unitn.it)
Department of Mathematics, University of Trento, Italy.

Luigi Sportiello (luigi.sportiello@st.com)
STMicroelectronics, AST Agrate - Milano, Italy.

Abstract
To obtain coprime polynomial pairs, it is often used an approach that consists of taking two random polynomials of the required degrees and testing whether they are relatively prime. If they are not, they are discarded and another pair is tried. The test can obviously be carried out very efficiently. Although in many cases the probability of success for the test is close to 1, this test approach is not deterministic.

In [4], a deterministic method to generate coprime polynomial pairs has been proposed. Starting from such a method, we have implemented an algorithm that generates, in a finite field of characteristic 2, at most $2^d\lambda$ distinct polynomials $\tilde{a}$ such that $\gcd(\tilde{a}, \tilde{b}) = 1$ and $\deg \tilde{a} = \deg \tilde{b} + d$, where $d \in \mathbb{N}$ and λ is a parameter that depends on our setting. This is accomplished by an application of the FGLM algorithm.

A congruence module

Let $\mathbb{K}$ be an arbitrary field, we denote with $\mathbb{K}[x]^r$ the product ring $\mathbb{K}[x]^r = \mathbb{K}[x] \times \cdots \times \mathbb{K}[x]$ that is a module over $\mathbb{K}[x]$.
Let f and g be polynomials in $\mathbb{K}[x]$ such that $\deg(f) = n$ and $\deg(g) \leq n-1$, where $n \in \mathbb{N}$, and $n \geq 2$.

Using simple generalizations of results from [2], we are interested in finding the minimal element $(\tilde{a}, \tilde{b})$ of the following submodule of $\mathbb{K}[x]^2$

$$M = \{(a, b) \in \mathbb{K}[x]^2 \mid a \equiv bg \mod f\} \tag{1}$$

such that $\deg \tilde{a} \leq \alpha$ and $\deg \tilde{b} \leq \beta$, where $\alpha, \beta \in \mathbb{N}$.

It is easy to show that the subset $B = \{(g, 1), (f, 0)\}$ of M is a reduced Gröbner basis relative to the term order $<_{\deg(g)}$.
We apply the FGLM algorithm [1] to determine another Gröbner basis B', relative to the particular term order $<_{\alpha-\beta}$ that is defined in this way:

$$\begin{array}{ll} (x^i, 0) <_{\alpha-\beta} (x^{i'}, 0) & \text{if } i < i' \\ (0, x^j) <_{\alpha-\beta} (0, x^{j'}) & \text{if } j < j' \\ (x^i, 0) <_{\alpha-\beta} (0, x^j) & \text{if } i \leq j + (\alpha - \beta) \end{array}$$

Let $\boldsymbol{t}_1 <_{\alpha-\beta} \boldsymbol{t}_2 <_{\alpha-\beta} \cdots$ be consecutive terms in $\mathbb{K}[x]^2$.
Let j be the smallest positive integer such that

$$\mathrm{Nf}_B(\boldsymbol{t}_j) = \sum_{i<j} c_i \mathrm{Nf}_B(\boldsymbol{t}_i)\,, \tag{2}$$

where the c_i's are in $\mathbb{K}$.
Then the first element of B' will be $(\tilde{a}, \tilde{b}) = \boldsymbol{t}_j - \sum_{i<j} c_i \boldsymbol{t}_i$.

Construction of coprime polynomial pairs

If polynomials g and f are arbitrary, then the minimal element $(\tilde{a}, \tilde{b})$ of M always satisfies the required degree conditions, but it is possible that $\gcd(\tilde{a}, \tilde{b}) \neq 1$.

It is proved in [4] the following theorem

Theorem. *Let $(\tilde{a}, \tilde{b})$ be the minimal element of M. Then*

$$\gcd(\tilde{a}, \tilde{b}) | f$$

From the previous result we have the starting point:

Corollary. *Let $(\tilde{a}, \tilde{b})$ be the minimal element of M. If f is an irreducible polynomial, then*

$$\gcd(\tilde{a}, \tilde{b}) = 1\,.$$

A first method to get a pair $(\tilde{a}, \tilde{b})$ of polynomials in $\mathbb{K}[x]$ such that $\gcd(\tilde{a}, \tilde{b}) = 1$ and $\deg(\tilde{a}) \leq \alpha$, $\deg(\tilde{b}) \leq \beta$ is the following:

Choose two integers $\alpha, \beta \geq 1$ and a field $\mathbb{K}$.
Fix the term order $<_{\alpha-\beta}$.
Take any n such that $n > \alpha$ and $n > \beta$.
Take any irreducible polynomial $f \in \mathbb{K}[x]$ s.t. $\deg(f) = n$.
Take any $g \in \mathbb{K}[x]$ s.t. $\deg(g) < n$.
Compute the minimal element $(\tilde{a}, \tilde{b})$ of M using FGLM.

Coprime polynomial pairs of fixed degree

The effectiveness of the previous method is strongly limited by the lack of control on the polynomial degrees. Moreover, the choice of f and g influences the outcome in a very unpredictable way.

Since we only need the first linear combination that occurs in the FGLM algorithm, it is possible to estimate how many terms are needed to get it. We exploit the following proposition [4] to fix conditions on g and f . This ensures we get a pair $(\tilde{a}, \tilde{b})$ of polynomials in $\mathbb{K}[x]$ s.t. $\gcd(\tilde{a}, \tilde{b}) = 1$ and $\deg \tilde{a} < z$, $\deg \tilde{b} = z$, for a fixed z.

Proposition. *Let $A_{f,g}$ be the solution matrix corresponding to a module M. Assume $A_{f,g}$ be a β-circulant matrix of rank z. Suppose $n = \beta + 1 + z$ and fix the term order $<_{-1}$. Let ϕ be the circulant polynomial of $A_{f,g}$. We have:*

1 $g = \phi^* x^z + \psi$ *where* ϕ^* *and* ψ *are polynomials with* $\deg(\phi^*) \leq \beta$ *and* $\deg(\psi) < z$,

2 $\deg(\phi) = \beta + 1 - z$, $\phi = \gcd(\phi^*, x^{\beta+1} - 1)$,

3 $\phi\tilde{b} = x^{\beta+1} - 1$, ϕ *is monic.*

We have adapted previous proposition to the case f irreducible. Moreover, this solution has been improved in the following way:

1. we have also a control on the degree of $\tilde{a}$ (see [4]).
2. over finite fields of characteristic p we can exactly obtain p^d distinct polynomials $\tilde{a}$ such that $\deg \tilde{a} = d + z$, for any fixed $\tilde{b}$ with $\deg \tilde{b} = z$ and $d \geq 0$. (As proved in [4])

3. let $p = 2$, starting from such a method, we have implemented an algorithm that generates

   - at most λ distinct polynomials $\tilde{a}$ such that $\deg \tilde{a} < \tilde{b}$
   - at most $2^d\lambda$ distinct polynomials $\tilde{a}$ s.t. $\deg \tilde{a} = d + z$, for any fixed $\tilde{b}$ with $\deg \tilde{b} = z$ and $d \geq 0$

Time performance in $\mathbb{F}_{2^n}$

The tables below summarize runtimes for generating coprime polynomial pairs over a finite field of characteristic 2 with our technique (Tech). As compare, we have generated the same number of distinct pairs in a random way: for any fixed $\tilde{b}$, we generated a random polynomial $\tilde{a}$ and checked that $\gcd(\tilde{a}, \tilde{b}) = 1$ and that such polynomial was not already considered.

First case: $\deg \tilde{a} \leq \deg \tilde{b}$; we obtain at most λ pairs.

$\deg \tilde{b}$	50		100		200	
	Tech.	*Rand*	*Tech.*	*Rand*	*Tech.*	*Rand*
Time	0.005	0.001	0.023	0.004	0.083	0.019
Pairs	96		192		384	

$\deg \tilde{b}$	300		400		500	
	Tech.	*Rand*	*Tech.*	*Rand*	*Tech.*	*Rand*
Time	0.355	0.031	0.363	0.089	1.621	0.116
Pairs	384		768		768	

We observe that the random method is more efficient than our ones due to the high probability (very close to 1) that two random polynomials are coprime. In this way, it is not necessary to try many random $\tilde{a}$ to obtain the required number of pairs.

Second case: $\deg \tilde{a} = \deg \tilde{b} + d$; we obtain at most $p^d \lambda$ pairs.

The considered values for $\deg \tilde{b}$, d and the number of generated pairs by the technique are

$\deg \tilde{b}$	50	100	200	300	400	500
d						
2	364	768	1536	1536	3072	3072
3	768	1536	3072	3072	6144	6144
4	1536	3072	6144	6144	12288	12288
5	3072	6144	12288	12288	24576	24576
6	6144	12288	24576	24576	49152	49152
7	12288	24576	49152	49152	98304	98304

With our technique we generate $2^d \delta$ pairs, where $\delta \leq \lambda$ and determinated by the choice of $\deg \tilde{b}$. To compute such pairs, δ needed sets of values are first precomputed and then for each of them 2^d polynomial are generated.

The running times of our technique are the following:

$d \backslash \deg \tilde{b}$	50	100	200	300	400	500
2	0.019	0.078	0.314	0.727	1.368	2.934
3	0.038	0.158	0.618	1.220	2.718	4.703
4	0.079	0.311	1.251	2.218	5.375	8.296
5	0.160	0.620	2.484	4.203	10.796	15.359
6	0.329	1.227	4.921	8.171	21.64	29.593
7	0.653	2.453	9.843	16.125	43.578	58.453

It is easy to observe that, for any fixed $\deg \tilde{b}$, since the number of required precomputation does not change, the running times increase almost with factor 2. For any fixed d, for growing values of $\deg \tilde{b}$, δ increases and more time is spent for the precomputations.

The running times of the random method are the following:

$d \setminus \deg \tilde{b}$	50	100	200	300	400	500
2	0.006	0.021	0.085	0.136	0.398	0.519
3	0.014	0.052	0.207	0.301	1.026	1.284
4	0.035	0.140	0.551	0.738	4.734	4.954
5	0.107	0.416	2.344	3.797	20.204	20.453
6	0.359	1.433	12	15.938	77.938	79.422
7	1.334	8.172	49.297	63.390	303.765	308.734

We observe that, for any fixed $\deg \tilde{b}$, the required times increase almost with factor 4. This is due to the check needed to have distinct pairs, which costs almost as $(2^d\delta)^2$ and represents the main part of the required time.
We note that the execution latency of our technique is better than the random approach ones, for $d > 5$.

Our experiments were carried out on a Pentium IV (2,4 GHz) with 512 Mb of RAM, running Windows XP Professional SP1. All code was developed in C++, based on Victor Shoup' s NTL library and compiled with MS Visual C++ in release mode.

Acknowledgements

This paper comes from the second author Master's Thesis: *"Coppersmith's algorithm with Fitzpatrick's techniques"*, supervised by Prof. M.Sala, University College Cork, Prof. F.Dalla Volta, Università di Milano- Bicocca and Dott. P. Fragneto, STMicroelectronics.

The authors heartily thank, for their useful suggestions and comments, G.Bertoni, P. Fitzpatrick, T. Mora, M. Orsini, I. Simonetti and C. Traverso.

References

[1] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, J. Symbolic Comput. **16** (1993), no. 4, 329344. MR MR1263871 (94k:68095)

[2] Patrick Fitzpatrick, *On the key equation*, IEEE Trans. on Inf. Th. **41** (1995), no. 5, 12901302. MR MR1366325 (96i:94033)

[3] Teo Mora, *Solving polynomial equation systems.* I, Encyclopedia of Mathematics and its Applications, vol. 88, Cambridge University Press, Cambridge, 2003, The Kronecker-Duval philosophy. MR MR1966700 (2004d:12001)

[4] P.Fragneto, A.Rimoldi, M.Sala *An approach to create coprime polynomial pairs*, submitted paper (available http://www.bcri.ucc.ie)