

In the following, we run a small example of an iterative version of our algorithm Algorithm 3 GuessingBivar(u). It consists in replacing the call to Half-Gcd-Seq by a call to Gcd-Seq, which would be an iterative version thereof. While the iterative version is not available in the paper, it is easier to follow. It mainly consists in calling QuoBivar on the successive remainders, as in the univariate Euclidean algorithm. The Maple code is available at https://github.com/ktran11/CrecbiseqGuessing/blob/main/maple/bivariate_iterative.mpl.

Context

Let $\mathbb{K} = \mathbb{F}_{97}$. We consider the ideal of relation I_u generated by the following reduced Gröbner basis G_u

$$\begin{aligned} &x^5 + 60x^4 + 45x^3 + 77x^2 + 10x + 28, \\ &yx^3 + yx^2 + 84yx + 69y + 30x^4 + 59x^3 + 27x^2 + 44x + 61, \\ &y^2x^2 + 34y^2x + 42y^2 + 12yx^2 + 20yx + 19y + 28x^4 + 4x^3 + 18x^2 + 43x + 70, \\ &y^3 + 88y^2x + 86y^2 + 84yx^2 + 33yx + 31y + 88x^4 + 65x^3 + 96x^2 + 67x + 45 \end{aligned}$$

We have the parameter $d_x = 5, d_y = 3$ and set $D_x = 10, D_y = 6$.

We build a sequence $\mathbf{u} = (u_{i,j})_{(i,j) \in \mathbb{N}^2}$ with random initial terms that we extend using the relations given by G_u .

	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
	\vdots	77	17	3	8	13	86	20	70	49	70	50
	\vdots	11	9	61	23	24	93	19	7	89	10	16
	\vdots	3	20	67	78	50	75	79	26	6	34	73
	\vdots	38	80	91	65	0	38	41	4	56	4	17
	\vdots	22	40	1	35	47	41	39	63	43	41	80
$j = 1$	79	95	10	45	66	74	42	75	57	90	64	
$j = 0$	29	5	31	39	23	18	58	53	38	36	83	
$u_{i,j}$	$i = 0$	$i = 1$	\dots	\dots	\dots	\dots	\dots	\dots	\dots	\dots	\dots	

Input of the pseudo-Euclidean algorithm

$$r_{-1} := (29x^{10} + 5x^9 + 31x^8 + 39x^7 + 23x^6 + 18x^5 + 58x^4 + 53x^3 + 38x^2 + 36x + 83)y^7$$

and

$$\begin{aligned} r_0 := & (29x^{10} + 5x^9 + 31x^8 + 39x^7 + 23x^6 + 18x^5 + 58x^4 + 53x^3 + 38x^2 + 36x + 83)y^6 \\ & + (79x^{10} + 95x^9 + 10x^8 + 45x^7 + 66x^6 + 74x^5 + 42x^4 + 75x^3 + 57x^2 + 90x + 64)y^5 \\ & + (22x^{10} + 40x^9 + x^8 + 35x^7 + 47x^6 + 41x^5 + 39x^4 + 63x^3 + 43x^2 + 41x + 80)y^4 \\ & + (38x^{10} + 80x^9 + 91x^8 + 65x^7 + 38x^5 + 41x^4 + 4x^3 + 56x^2 + 4x + 17)y^3 \\ & + (3x^{10} + 20x^9 + 67x^8 + 78x^7 + 50x^6 + 75x^5 + 79x^4 + 26x^3 + 6x^2 + 34x + 73)y^2 \\ & + (11x^{10} + 9x^9 + 61x^8 + 23x^7 + 24x^6 + 93x^5 + 19x^4 + 7x^3 + 89x^2 + 10x + 16)y \\ & + (77x^{10} + 17x^9 + 3x^8 + 8x^7 + 13x^6 + 86x^5 + 20x^4 + 70x^3 + 49x^2 + 70x + 50)1 \end{aligned}$$

Computation of the quotient matrix Q_0 and the relation of $v_{*,0}$

First we compute the C-relation on the first slice,

$$\left| \begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c} j=0 & 29 & 5 & 31 & 39 & 23 & 18 & 58 & 53 & 38 & 36 & 83 \\ \hline u_{i,j} & i=0 & i=1 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{array} \right|$$

which can be read off from the polynomial $lc(r_0)$.

$$f_0 = \text{GuessingUnivar}(lc(r_0)) = x^5 + 60x^4 + 45x^3 + 77x^2 + 10x + 28$$

Since $lc(r_0) = lc(r_{-1})$ we deduce that $a_0 = -1$ and

$$\begin{aligned} r_1^{tmp} &:= yr_0 + a_0 r_{-1} \\ &= (79x^{10} + 95x^9 + 10x^8 + 45x^7 + 66x^6 + 74x^5 + 42x^4 + 75x^3 + 57x^2 + 90x + 64)y^6 \\ &\quad + (22x^{10} + 40x^9 + x^8 + 35x^7 + 47x^6 + 41x^5 + 39x^4 + 63x^3 + 43x^2 + 41x + 80)y^5 \\ &\quad + (38x^{10} + 80x^9 + 91x^8 + 65x^7 + 38x^5 + 41x^4 + 4x^3 + 56x^2 + 4x + 17)y^4 \\ &\quad + (3x^{10} + 20x^9 + 67x^8 + 78x^7 + 50x^6 + 75x^5 + 79x^4 + 26x^3 + 6x^2 + 34x + 73)y^3 \\ &\quad + (11x^{10} + 9x^9 + 61x^8 + 23x^7 + 24x^6 + 93x^5 + 19x^4 + 7x^3 + 89x^2 + 10x + 16)y^2 \\ &\quad + (77x^{10} + 17x^9 + 3x^8 + 8x^7 + 13x^6 + 86x^5 + 20x^4 + 70x^3 + 49x^2 + 70x + 50)y \end{aligned}$$

Now, we need to write the sequence read off from $lc(r_1^{tmp})$ as $b_0 \star u_{*,0}$:

$$b_0 := \text{HankelSolver}(lc(r_0), lc(r_1^{tmp}), f_0):$$

We can then compute the quotient matrix

$$Q_0 = \begin{bmatrix} 0 & 1 \\ a_0 & y - b_0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 96 & y + 4x^4 + 53x^3 + 33x^2 + 92x + 59 \end{bmatrix}$$

also obtain the next remainder

$$\begin{aligned} r_1 &:= a_0 r_{-1} + (y - b_0) r_0 \\ &= (9x^{10} + 10x^9 + 38x^8 + 53x^7 + 42x^6 + 62x^5 + 28x^4 + 14x^3 + 49x^2 + 44x + 15)y^5 + \\ &\quad (11x^{10} + 37x^9 + 72x^8 + 38x^7 + 91x^6 + 91x^5 + 22x^4 + 23x^3 + 95x^2 + 44x + 89)y^4 + \\ &\quad (48x^{10} + 83x^9 + 14x^8 + 81x^7 + 87x^5 + 47x^4 + 17x^3 + 23x^2 + 59x + 37)y^3 + \\ &\quad (37x^{10} + 73x^9 + 59x^8 + 83x^7 + 12x^6 + 3x^5 + 52x^4 + 32x^3 + 49x^2 + 77x + 1)y^2 + \\ &\quad (32x^{10} + 27x^9 + 69x^8 + 14x^7 + 87x^6 + 87x^5 + 78x^4 + 94x^3 + 58x^2 + 50x + 38)y + \\ &\quad 86x^{10} + 54x^9 + 63x^8 + 26x^7 + 53x^6 + 73x^5 + 52x^4 + 3x^3 + 10x^2 + 31x + 36 \end{aligned}$$

Computation of Q_1 , f_1 and r_2

With the same method, we can compute

$$Q_1 = \begin{bmatrix} 0 & 1 \\ 16x^4 + 31x^3 + 64x^2 + 52x + 82 & y + 25x^2 + 90x + 78 \end{bmatrix}, \quad f_1 = x^3 + x^2 + 84x + 69$$

and the remainder r_2 , whose coefficient in y^5 has been eliminated by construction,

$$\begin{aligned}
r_2 &:= a_1 r_0 + (y - b_1) r_1 \\
&= (84x^{10} + 42x^9 + 88x^8 + 94x^7 + 92x^6 + 5x^5 + 40x^4 + 79x^3 + 96x^2 + 14x + 51)y^4 \\
&\quad + (41x^{10} + 90x^9 + 68x^8 + 19x^7 + 87x^6 + 27x^5 + 84x^4 + 84x^3 + 18x^2 + 31x + 33)y^3 \\
&\quad + (64x^{10} + 73x^9 + 68x^8 + 54x^7 + 61x^6 + 23x^5 + 51x^4 + 16x^3 + 30x^2 + 54x + 8)y^2 \\
&\quad + (13x^{10} + 38x^9 + 13x^8 + 55x^7 + 90x^6 + 80x^5 + 77x^4 + 38x^3 + 11x^2 + 21x + 69)y \\
&\quad + 37x^{10} + 17x^9 + 61x^8 + 30x^7 + 48x^6 + 52x^5 + 54x^4 + 65x^3 + 83x^2 + 41x + 93
\end{aligned}$$

Note that the two products must be understood as \cdot_{f_0} as in Theorem 4.1.3. This is the reason why no terms in y^5 appears.

Computation of Q_2 , f_2 and r_3

We continue with the computation of the remainder r_3 , which requires the quotient matrix Q_2 and the C-relation f_2

$$Q_2 = \begin{bmatrix} 0 & 1 \\ 72x^2 + 46x + 2 & y + 72 + 67x \end{bmatrix}, \quad f_2 = x^2 + 34x + 42$$

and the remainder r_3 , whose coefficient in y^4 has been eliminated by construction,

$$\begin{aligned}
r_3 &:= a_2 r_1 + (y - b_2) r_2 \\
&= (23x^{10} + 62x^9 + 38x^8 + 40x^7 + 35x^6 + 58x^5 + 31x^4 + 4x^3 + 92x^2 + 53x + 41)y^2 \\
&\quad + (93x^{10} + 3x^9 + 88x^8 + 41x^7 + 49x^6 + 64x^5 + 19x^4 + 3x^3 + 62x^2 + 42x + 43)y \\
&\quad + 34x^{10} + 4x^9 + 94x^8 + 27x^7 + 83x^6 + 28x^5 + 87x^4 + 38x^3 + 54x^2 + 6x + 2
\end{aligned}$$

Again, the products must be understood as \cdot_{f_0} .

The degree sequence is no longer normal

At this step, we have $2 = \deg(r_3) \neq \deg(r_2) - 1 = 3$.

We can stop the computation of the remainders, we have enough informations to reconstruct a Gröbner basis of the ideal of relation. This is similar to the univariate case. Alternatively, this remainder can be seen as a byproduct of the lack of precision in the sequence terms: i.e. we would need further sequence terms to make them vanish.

GuessingBivar

`GuessingBivar` initialization sets f_0 as the first element g_0 of the Grobner basis.

The next computations correspond to the `for` loop on line 6 of Algorithm 3 `GuessingBivar(u)`.

First loop

The matrix product $Q_1 Q_0$ is

$$\begin{bmatrix} 96 & y + 4x^4 + 53x^3 + 33x^2 + 92x + 59 \\ 96y + 72x^2 + 7x + 19 & y^2 + (4x^4 + 53x^3 + 58x^2 + 85x + 40)y + 72x^4 + 67x^3 + 74x^2 + 23x + 83 \end{bmatrix}$$

whose entry on the first line, second column is $t_1 = y + 4x^4 + 53x^3 + 33x^2 + 92x + 59$. Its modular product $g_1 := t_1 f_1 \bmod f_0$ is the second element of the Grobner basis.

$$g_1 = (x^3 + x^2 + 84x + 69)y + 30x^4 + 59x^3 + 27x^2 + 44x + 61$$

Second loop

The matrix product

$$Q_2 Q_1 Q_0 = \begin{bmatrix} s_2 & t_2 \\ s_3 & t_3 \end{bmatrix}$$

where

$$\begin{aligned} s_2 &= 96y + 72x^2 + 7x + 19 \\ t_2 &= y^2 + (4x^4 + 53x^3 + 58x^2 + 85x + 40)y + 72x^4 + 67x^3 + 74x^2 + 23x + 83 \\ s_3 &= 96y^2 + (72x^2 + 37x + 44)y + 71x^3 + 52x^2 + 82x + 8 \\ t_3 &= y^3 + (4x^4 + 53x^3 + 58x^2 + 55x + 15)y^2 + (53x^4 + 74x^3 + 51x^2 + 78x + 20)y \\ &\quad + 33x^4 + 14x^3 + 70x^2 + 87x + 71 \end{aligned}$$

Its modular product $g_2 := t_2 f_2 \bmod f_0$ is the third element of the Grobner basis.

$$g_2 = (x^2 + 34x + 42)y^2 + (58x^4 + 62x^3 + 38x^2 + 90x + 4)y + 50x^4 + 39x^3 + 36x^2 + 34x + 94$$

After the loop

The loop stops after its second iteration because the degree sequence is no longer normal. The last step 11 of Algorithm 3 `GuessingBivar(u)` appends $g_3 := t_{d_y} = t_3$ to the Grobner basis.

Output

The minimal Grobner basis on output is $G := \{f_0, g_1, g_2, t_{d_y}\}$, with

$$\begin{aligned} f_0 &= x^5 + 60x^4 + 45x^3 + 77x^2 + 10x + 28 \\ g_1 &= (x^3 + x^2 + 84x + 69)y + 30x^4 + 59x^3 + 27x^2 + 44x + 61, \\ g_2 &= (x^2 + 34x + 42)y^2 + (58x^4 + 62x^3 + 38x^2 + 90x + 4)y + 50x^4 + 39x^3 + 36x^2 + 34x + 94, \\ t_{d_y} &= y^3 + (4x^4 + 53x^3 + 58x^2 + 55x + 15)y^2 + (53x^4 + 74x^3 + 51x^2 + 78x + 20)y \\ &\quad + 33x^4 + 14x^3 + 70x^2 + 87x + 71 \end{aligned}$$

This Grobner basis does not match G_u because G is only minimal whereas G_u is reduced, *i.e.* minimal and the elements in the basis are reduced w.r.t. the other ones.

Note that G has exactly the same leading monomials as all the ones in G_u . Furthermore, the `Maple` command `Groebner:-InterReduce(G,plex(y,x),characteristic=97)` yields the same polynomials as in G_u , hence the output G is a minimal Gröbner of $I(u)$.

Note that the elements in our output Grobner basis have support in the (d_x, d_y) -box, *i.e.* their partial degrees are bounded by d_x and d_y .