Intervals, Syzygies, Numerical Gröbner Bases: A Mixed Study

Marco BODRATO, Alberto ZANONI

Dipartimento di Matematica "Leonida Tonelli"
Università di Pisa
Largo B. Pontecorvo 5, 56127 Pisa, Italy

{bodrato,zanoni}@posso.dm.unipi.it

CASC 2006, Chisinau, Moldova - September 11, 2006

The scene

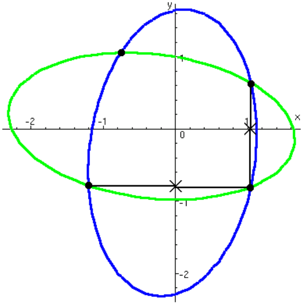
- Let $\mathbb{K}$ be a field and $\mathcal{F} = \{f_1, \ldots, f_s\} \subset \mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]$ a list of polynomials representing the initial system. In this paper we consider $\mathbb{K} = \mathbb{R}$.
- We want to compute $\overline{\mathcal{G}}$, the Gröbner basis of $\mathcal{F}$, with Buchberger algorithm, but...
- ...we do not know **exactly** all the coefficients of $\mathcal{F}$: some of them are known only with a limited precision.
- "Interval" coefficients: not a single one, but many different $\mathcal{F}$ should be considered at the same time.
- Which is the "best" $\mathcal{F}$ and relative Gröbner basis $\mathcal{G}$ we are interested in ? Can it be computed ?
- We consider the best system to be the "most degenerate" one.

☺ The scene with picture

Example : Windsteiger's system, lexicographic order.

There are two solutions with almost equal x coordinate.

If $y < x$ the system becomes Gröbner-unstable.

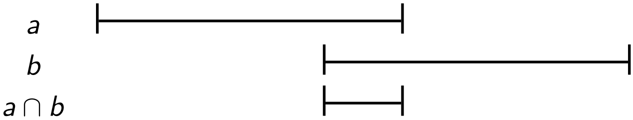


☺ The scene with picture

Example : degree lexicographic order.

$$\begin{cases} f_1 = x^2y + ax + 1 & = 0 \\ f_2 = xy^2 + by & = 0 \end{cases} \quad \rightarrow \quad S(f_1, f_2) = (a-b)xy + y$$

"Most degenerate" means here $\boxed{a - b = 0}$



We can shrink both intervals !

♫ Note and take note of notation

- $\alpha, \beta, \delta, \dots \in \mathbb{N}^n$ multindexes
- $\{\mathbb{T}, <\} = \{X^\delta \mid |\delta| = 0, 1, \dots\}$ the ordered term monoid
- $lt(f)$ = the leading term of f
- $lc(f)$ = the leading coefficient of f
- $f_i = \sum_{\beta \in B_i} F_i^\beta X^\beta \quad , \quad k_i = \sum_{\alpha \in A_i} K_i^\alpha X^{\alpha_i}$
- Abusing notation, they will also be considered as variables

$$
\begin{aligned}
F =& \{F_i^\beta \mid \beta \in B_i, i = 1, \dots, s\} \\
K =& \{K_i^\alpha \mid \alpha \in A_i, i = 1, \dots, s\}
\end{aligned}
$$

Behind the scene : syzygies

Could you please tell me the way to $\overline{\mathcal{G}}$? (I)

Definition

A *syzygy* for $\mathcal{F}$ is a s–tuple $\mathcal{H} = (h_1, \ldots, h_s) \subset \mathbb{K}[X]^s$ such that

$$\mathcal{H} \cdot \mathcal{F} = \sum_{i=1}^{s} h_i(X) \cdot f_i(X) = 0$$

Let $\mathcal{G} = \{g_1, \ldots, g_t\} \subset \mathbb{K}[X]$ be a system obtained from $\mathcal{F}$ during a Buchberger algorithm application. We want also to keep track of the steps to derive $\mathcal{G}$ from $\mathcal{F}$, (mimicing extended Euclid).
In other words, we look for $\{k_{ij}(X)\} \in \mathbb{K}[X]$ with

$$g_j(X) = \sum_{i=1}^{s} k_{ij}(X) \cdot f_i(X) \qquad j = 1, \ldots, t$$

Behind the scene : extended syzygies

Could you please tell me the way to $\overline{\mathcal{G}}$? (II)

We can obtain both

- ⋆ syzygies h_{ij} : $i = 1, \dots s$; $j = 1, \dots$
- ⋆ extended syzygies k_{ij} : $i = 1, \dots s$; $j = 1, \dots, t$

by using a variant of Buchberger algorithm itself (Caboara, Traverso, 1998). Just two new added variables needed.

$$\mathcal{F} \xrightarrow{\mathcal{H}^{(1)}} \mathcal{G}^{(1)} \xrightarrow{\mathcal{H}^{(2)}} \mathcal{G}^{(2)} \xrightarrow{\mathcal{H}^{(3)}} \dots \xrightarrow{\mathcal{H}^{(k)}} \mathcal{G}^{(k)}$$

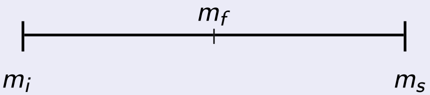
The $\mathcal{H}$'s will be used to find a way to the "right" $\overline{\mathcal{G}}$.

☹ Representing not exact coefficients

The idea is to take benefit from the combined use of floating point and interval arithmetics.

Definition

A `multiCoeff` m is an "enriched" representation of a real number, consisting of an interval $m_I = [m_i, m_s]$ and a floating point value $m_f \in m_I$.



(We do not discuss implementation details.)

Using `multiCoefficients`

Interval and (whatever) floating point arithmetic are used independently for m_I and m_f, respectively.

Definition

An interval $I = [a, b] \subset \mathbb{R}$ is *dangerous* when $0 \in I$. A `multiCoeff` m is dangerous when m_I is dangerous.

Dangerousness means that the coefficient *may* be zero, but, because of interval arithmetic overestimation, the final decision should be made case by case.

Many zero test for approximate coefficients were proposed, but they all suffer in not being flexible.

Some Zero Tests

- Threshold : $|m_f| < \varepsilon$
- Bracket coefficients : (Shirayanagi 1996)
- HCoeff : (Migheli 1999)
- F2Coeff : (Traverso, Zanoni 2002)
- ε-perturbation & monomials movement (Stetter, Traverso 2002)
- ...

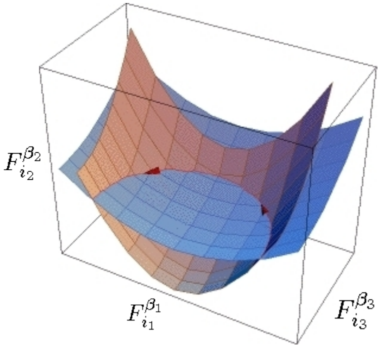
Some of these are "local" methods (they only watch a single coefficient), some are "neighbor" method (watch a polynomial), and depend on some tunable parameters, whose values are constant during the algorithm ("rigidity").

We try to propose a *global* test.

A geometric perspective

The general idea is to let the algorithm flow until some interval becomes dangerous, decide if we can really obtain 0 or not – "biforcation" – and (in case) continue imposing the corresponding coefficient *is* 0.

This means adding more and more restrictions on $\mathcal{F}$ coefficients, that is, equations in F variables… as well as moving on hypersurfaces intersection, becoming more and more restrictive.



What a zero test!

Definition

A `multiCoefficients`-polynomial p involved in Buchberger algorithm is *dangerous* when $lc(p)$ is and p is no more head–reducible with respect to the current basis.

Let r be the first encountered dangerous polynomial

$$r(X) = \sum_{\gamma} r_\gamma X^\gamma = \sum_{i=1}^{s} k_i(X) \cdot f_i(X) \qquad ; \qquad lt(r) = X^\rho$$

Equating coefficients on both sides and considering initial intervals we obtain

This is what happens...

$$S_\rho = \left\{ \begin{array}{ll} 0 = \displaystyle\sum_{\substack{i=1 \\ \alpha+\beta=\gamma}}^{s} K_i^\alpha F_i^\beta & \gamma > \rho \\ r_\gamma = \displaystyle\sum_{\substack{i=1 \\ \alpha+\beta=\gamma}}^{s} K_i^\alpha F_i^\beta & \gamma \leqslant \rho \\ \underline{F}_i^\beta \leqslant F_i^\beta \leqslant \overline{F}_i^\beta & \\ \underline{K}_i^\alpha \leqslant K_i^\alpha \leqslant \overline{K}_i^\alpha & \end{array} \right\}$$

Since we want to detect if the dangerous leading coefficient r_ρ can be zero or not, this leads us to solve the following optimization problem:

... in dangerous situations

$$
\mathcal{P}_\rho : \begin{cases}
\textbf{min} \quad c = \left| \sum_{\substack{i=1 \\ \alpha+\beta=\rho}}^{s} K_i^\alpha F_i^\beta \right| & (O) \\
0 = \sum_{\substack{i=1 \\ \alpha+\beta=\gamma}}^{s} K_i^\alpha F_i^\beta \qquad \gamma > \rho & (V) \\
\left. \begin{array}{l} \underline{F}_i^\beta \leqslant F_i^\beta \leqslant \overline{F}_i^\beta \\ \underline{K}_i^\alpha \leqslant K_i^\alpha \leqslant \overline{K}_i^\alpha \end{array} \right\} \forall\, i, \alpha, \beta & (B)
\end{cases}
$$

We call c the *objective function* (o.f.)

♂ A point of view

A quadratic optimization problem with quadratic restrictions.

- **Symbolic** (S) : Find explicitly equations in F such that the algorithm trace remains valid and the new relation $c = 0$ is valid (Bodrato, Zanoni 2004).
- **Numeric** (N) : Since (S) is often computationally hard, find numerically only some particular values for K_i^α, F_i^β satisfying above equations, and manage the whole analysis based on these obtained values.

Another point of view

We consider the quadratic system composed by (V) equations as living in $\mathbb{K}[F][K]$ instead than $\mathbb{K}[K,F]$, that is, with F variables considered as parameters.
Now it looks like a sparse **linear parametric** system.

$$\mathcal{M}_{\mathcal{F}} \cdot K = \begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & F_{ij} & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix} \begin{pmatrix} \cdot \\ K_{ij} \\ \cdot \end{pmatrix} = 0$$

$\mathcal{M}_{\mathcal{F}}$ entries are monic F-monomials.

Some initial symbolic management may help in reducing the system size.

⚤ How to manage the ménage (I)

Definition

A polynomial p (an equation $p = 0$) is *mute* if p is a linear binomial with its two coefficients equal to 1.

$$K_i + K_j = 0 \quad \longrightarrow \quad K_i = -K_j$$

$$(F_1)K_1 + (F_2)K_2 = 0 \quad \longrightarrow \quad K_1 = -\frac{F_2}{F_1}K_2 \quad ; \quad K_2 = -\frac{F_1}{F_2}K_1$$

An easy way to eliminate variables, with possible repercussions on interval shrinkings.

⚥ How to manage the ménage (II)

Definition

A variable v is *single* for a linear system S (S-single, or simply *single* if S is clear from the context) if it appears only once in S (in polynomial p_v).

If K_1 is V-single, we may consider a block term ordering (possibly changing the one we're currently using) such that it is the greatest variable. Then $lt(p_{K_1}) = K_1$, and it will not be used at all, for there is nothing to reduce by it.

We can then consider it as virtually discarded from V, and look now at $V_1' = V \setminus \{p_{K_1}\}$. And so on...

A function for iterative numerical methods

In order to apply whatever iterative numerical method to find a solution for $\mathcal{P}_\rho$, a function to be evaluated pointwise is needed.

- Specialize $\mathcal{M}_\mathcal{F}$ entries with π ($F_{ij} = \pi_{ij}$), obtaining $\mathcal{M}_\pi$.
- Solve the system $\mathcal{M}_\pi \cdot K = 0$, that is, find $\mathcal{K} = \ker(\mathcal{M}_\pi)$ in the form $K_v = N(\pi) \cdot K_p$, where K_p is the set of remaining "free parameters".
- Eliminate K_v variables in the o.f. by means of the found expressions in terms of K_p ones.
- Now the o.f. depends only on K_p variables: instantiate them with corresponding $\sigma = \{\sigma_{ij}\}$ values.

We note that, given $\mathcal{F}$, we always use the same σ values for K_p, for every point π.

Special cases

When there is only one free parameter $K_p = \{\overline{K}\}$ we have

$$c_\pi = D(\pi) \cdot \overline{K}$$

D is a rational function, indicating explicitly that and how c depends on initial coefficients. In this case it is more evident that what really counts is essentially working on $D(\pi)$.

$$sign(c_{\pi_1}) \neq sign(c_{\pi_0}) \longrightarrow \exists\ \bar{\pi} = \pi_0 + t \cdot (\pi_1 - \pi_0) \in F\text{-}box$$

$\bar{\pi}$ solving the problem, with $t \in (0, 1)$. Approximable e.g. by successive bisections.

Numerical Buchberger Algorithm (NBA)

1. Construct the $\overline{\mathcal{F}}$ system with `multiCoefficients`, start Buchberger algorithm.
2. If there is a remaining S-polynomial, compute r, its complete reduction with respect to the current basis, otherwise go to 5.
3. If $r = 0$ or its head coefficient c is not dangerous, update the data structures as usual and go to step 2, otherwise to 4.
4. Decide if c can really be or is surely different from 0. Update data structures and in the first case modify $\mathcal{F}$ and go to 1, otherwise continue from 2.
5. Extract the final polynomials g_i from the obtained basis, and output them.

The working tools

- S_i : the i^{th} reduced S-polynomial
- $\mathcal{A} = \{a_j\} = \{(i_j, c_j, t_j)\}$ (the *agenda*)
  - $i_j \in \mathbb{N}$ are labels $(j < \ell \rightarrow i_j < i_\ell)$, $c_j = lc(S_{i_j})$, $t_j = lt(S_{i_j})$
- $\mathcal{O} = \{(o_j, \mathcal{V}_j, \sigma_j)\}$ (the *restrictions*)
  - $o_j = \sum_{i,\alpha+\beta=\rho_j} K_i^\alpha F_i^\beta$ are o.f. expressions,
  - $\mathcal{V}_j$ are the corresponding (V) equations
  - σ_j the found values for K variables.

The Procedure

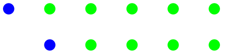
- We may have obtained from precedent computations that, for a specific critical point, $lc(r)$ could effectively be (set to) 0.
- Numerical errors $\longrightarrow$ cancellations not exact, we obtain again the leading dangerous coefficient.
- We know it *must* be 0, (the actual F values were set such that it should). Idem for other monomials beyond the leading one.
- "Actual" head : the first monomial m, starting from the leading one, such that the answer to the corresponding $\mathcal{P}_\rho$ was not "$c_j = 0$" (either $c_j \neq 0$ or $\mathcal{P}_\rho$ was still not solved).
- Record in the corresponding entry of $\mathcal{A}$coefficient and term of the actual head. If all r coefficients can be set to 0 at the same time, use the default $(c_j, t_j) = (0, \mathbf{1})$.

Data updating (I)

At the beginning, $\mathcal{A}$, $\mathcal{O}$ are both empty.

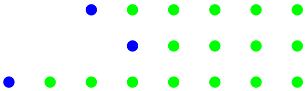
Data updating (I)

At the beginning, $\mathcal{A}$, $\mathcal{O}$ are both empty.



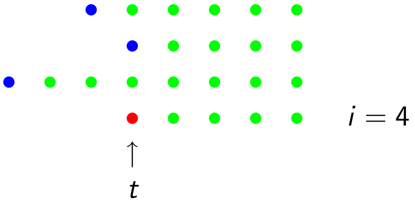
Data updating (I)

At the beginning, $\mathcal{A}$, $\mathcal{O}$ are both empty.



Data updating (I)

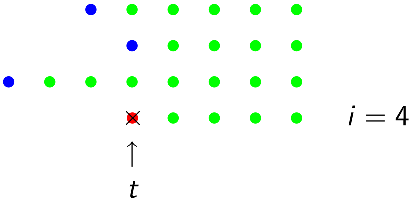
At the beginning, $\mathcal{A}$, $\mathcal{O}$ are both empty.



When a dangerous polynomial $r = S_i$ appears $(lc(r) = c)$ ...

Data updating (I)

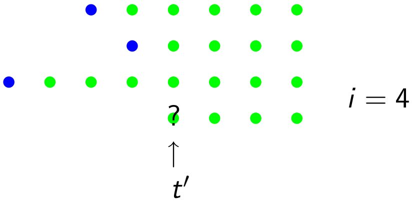
At the beginning, $\mathcal{A}$, $\mathcal{O}$ are both empty.



…we solve the corresponding $\mathcal{P}_\rho$ problem.

Data updating (I)

At the beginning, $\mathcal{A}$, $\mathcal{O}$ are both empty.

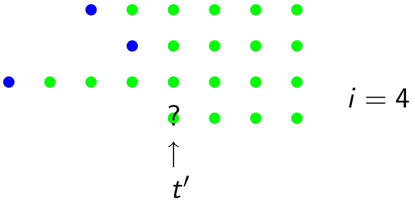


In this case, 0 can be obtained, and we remember the next coefficient to be analyzed next time.

$$\mathcal{A} = \{a = (4, c', t')\} \quad ; \quad \mathcal{O} = \{(o, \mathcal{V}_4, \sigma)\}$$

Data updating (I)

At the beginning, $\mathcal{A}$, $\mathcal{O}$ are both empty.



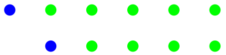
We then begin again with the new values for F.

Data updating (II)

$$\mathcal{A} = \{a = (4,\ c',\ t')\} \quad ; \quad \mathcal{O} = \{(o, \mathcal{V}_4, \sigma)\}$$

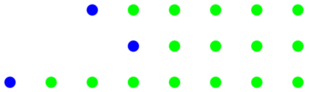
Data updating (II)

$$\mathcal{A} = \{a = (4,\ c',\ t')\} \quad ; \quad \mathcal{O} = \{(o, \mathcal{V}_4, \sigma)\}$$



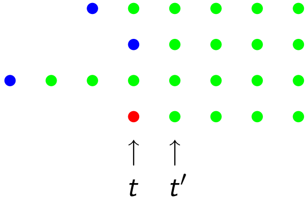
Data updating (II)

$$\mathcal{A} = \{a = (4,\ c'\ ,\ t')\} \quad ; \quad \mathcal{O} = \{(o, \mathcal{V}_4, \sigma)\}$$



Data updating (II)

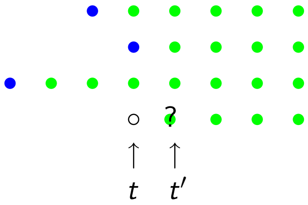
$$\mathcal{A} = \{a = (4,\ c',\ t')\} \quad ; \quad \mathcal{O} = \{(o, \mathcal{V}_4, \sigma)\}$$



Because of machine approximation we obtain again the same dangerous coefficient, but . . .

Data updating (II)

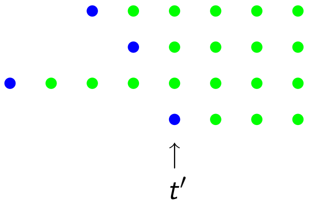
$$\mathcal{A} = \{a = (4,\ c',\ t')\} \quad ; \quad \mathcal{O} = \{(o, \mathcal{V}_4, \sigma)\}$$



...after a look to the agenda, we detect it's 0 ($t \neq t'$), and simply go on, setting up and solving another $\mathcal{P}_{\rho'}$ problem.

Data updating (II)

$$\mathcal{A} = \{a = (4,\ c'',\ t')\} \quad ; \quad \mathcal{O} = \{(o, \mathcal{V}_4, \sigma)\}$$



In this case the solution tells us this is a not dangerous coefficient. . . . . . we update the agenda again. . . and continue the computation with the following S-polynomial.

✂ Stricter and stricter restrictions

As we proceed, new restrictions (dangerous coefficients $c = 0$) are added one by one, and the new values for F must be such that the old ones are always satisfied while trying to set to 0 the latest one (look for particular point on a variety).

How to obtain this ?

- Simply adding the new o.f. as new equations in (V) does not always make sense.
- (Suggestion) Modify o.f. shape for $\mathcal{P}_\rho$ problems successive to the first one.

$$O = \sum_{i=1}^{\omega} o_i^2 + |o|$$

Something here and there...

$$\begin{cases} z - 10 & = 0 \\ z^5 + 20x^2y + 21xy & = 0 \\ z^5 + 21xy^2 + 20y^2 & = 0 \end{cases}$$

6^{th} critical pair: dangerous situation with $O = (F_{2,2})K_{2,1}$

$$V = \begin{cases} K_{0,0} + K_{2,0} = 0 & (1) \\ K_{0,1} + K_{1,0} = 0 & (2) \\ (F_{0,1})K_{0,0} + K_{0,2} = 0 & (3) \\ (F_{0,1})K_{0,1} + K_{0,3} = 0 & (4) \\ K_{0,4} + K_{2,1} = 0 & (5) \\ (F_{1,1})K_{1,0} + (F_{2,1})K_{2,0} = 0 & (6) \\ (F_{0,1})K_{0,2} + K_{0,5} = 0 & (7) \\ (F_{0,1})K_{0,3} + K_{0,6} = 0 & (8) \\ (F_{0,1})K_{0,4} + K_{0,7} = 0 & (9) \\ (F_{0,1})K_{0,5} + K_{0,8} = 0 & (10) \\ (F_{0,1})K_{0,6} + K_{0,9} = 0 & (11) \\ (F_{0,1})K_{0,7} + K_{0,10} = 0 & (12) \\ (F_{1,2})K_{1,0} + (F_{2,2})K_{2,0} + (F_{2,1})K_{2,1} = 0 & (13) \end{cases}$$

Equations (1), (2), (5) are mute. $K_{0,8}$ is single: remove (10). $K_{0,5}$ is single, so (7) is removed, too. . . and so on.

Something up and down...

The variables (and equations) we can avoid to consider are

$$\{\ K_{0,8},\ K_{0,5},\ K_{0,2},\ K_{0,9},\ K_{0,6},\ K_{0,3},\ K_{0,10},\ K_{0,7}\ \}$$

$$V = \begin{cases} (F_{1,1})K_{1,0} + (F_{2,1})K_{2,0} & = 0 \\ (F_{1,2})K_{1,0} + (F_{2,2})K_{2,0} + (F_{2,1})K_{2,1} & = 0 \end{cases}$$

$K_{2,1}$ is dangerous, $K_{1,0}, K_{2,0}$ not $\rightarrow$ change ordering: $K_{2,1}$ is the greatest variable.

$$\overline{\mathcal{M}}_{\mathcal{F}} \cdot K = \left(\begin{array}{cc|c} F_{1,1}F_{2,1} & 0 & F_{1,1}F_{2,2} - F_{1,2}F_{2,1} \\ 0 & F_{1,1} & F_{2,1} \end{array}\right) \begin{pmatrix} K_{2,1} \\ K_{1,0} \\ K_{2,0} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$O = \frac{N(F)}{D(F)}\ K_{2,0} = \frac{F_{1,1}F_{2,2} - F_{1,2}F_{2,1}}{F_{1,1}F_{2,1}}\ K_{2,0}$$

Something near and far...

Windsteiger's system:

Exact version:

$$\begin{cases} -4+3\left(\frac{172966043}{174178537}x-\frac{42176556}{358072327}y\right)^2+\left(\frac{1}{3}+\frac{42176556}{358072327}x+\frac{172966043}{174178537}y\right)^2 & =0 \\ -4+\left(\frac{1}{3}-\frac{42176556}{358072327}y+\frac{172966043}{174178537}x\right)^2+4\left(\frac{172966043}{174178537}y+\frac{42176556}{358072327}x\right)^2 & =0 \end{cases}$$

Approximated version

$$\begin{cases} 10277480y^2-4678710xy+29722520x^2+6620260y+785252x-38888890=0 \\ 39583780y^2+7018070xy+10416220x^2-785252y+6620260x-38888890=0 \end{cases}$$

Something found, at last !

We report the obtained condition (partially factorized) and its values after substitution of the exact values for $F_{i,j}$

$$\begin{aligned} O &= (F_{1,5}-F_{0,5})(F_{0,1}-F_{1,1})^2 \\ &+ (F_{0,4}-F_{1,4})(F_{0,1}-F_{1,1})(F_{0,2}-F_{1,2})+ \\ &+ (F_{1,3}-F_{0,3})(F_{0,2}-F_{1,2})^2 \simeq 3.41251314801457080845 \cdot 10^{-16} \end{aligned}$$

Modifying the initial values for F such that this relation is satisfied exactly is a step towards a/the “most instable” system near Windsteiger's.