Lifting Techniques for Triangular Decompositions

X. Dahan[⋆], M. Moreno Maza[†], É. Schost[⋆], W. Wu[†] & Y. Xie[†]

⋆: LIX, École polytechnique, Palaiseau, France.

†: ORCCA, University of Western Ontario, London, Canada.

ISSAC-05, July 24-27, 2005.

Framework: Polynomial systems solving

$\rightarrow$ by use of *triangular decomposition*,

$\rightarrow$ over the field $\mathbb{Q}$ of rational numbers,

$\rightarrow$ using a modular method (Hensel lifting).

Framework: Polynomial systems solving

→ by use of *triangular decomposition*

→ over the field $\mathbb{Q}$ of rational numbers.

→ using a modular method (Hensel lifting).

• Why triangular decomposition?

1) Gröbner basis: loss of geometric information during the classical algorithm

⇒ makes a sharp modular method hard to design.

2) primitive element representation: lack of canonicity.

• Irreducible decomposition problem: irreducibility may not hold anymore modulo any prime.

• Among all possible triangular decompositions, we introduce a *canonical* one adapted to sharp modular computations:

The equiprojectable decomposition

Related work

- Modular methods for Gröbner bases: (Trinks 1985), (Winkler 1988), (Arnold 2003); and, for primitive element representation: (TERA group, 1997 - now), (Rouillier 1999, Noro and Yokoyama 1999) ...

- Non modular methods for triangular decomposition algorithms: (Wu, 1987), (Chou & Gao 1990), (Lazard 1991), (Kalkbrener 1993), (Wang 1993), (Moreno Maza 2000), (Boulier, Lemaire & Moreno Maza 2001), (Hubert, 2003), ...

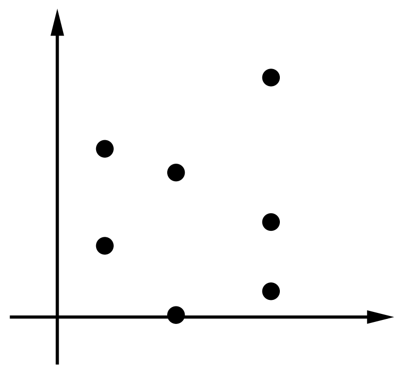
- Modular method for only *one* triangular set (Schost 2003)

Specialization problem

The following example illustrates the difficulties of designing a modular algorithm for triangular decompositions.

Let V be the zero-dimensional variety defined over $\mathbb{Q}$ by

$$\{326x - 10y^6 + 51y^5 + 17y^4 + 306y^2 + 102y + 34,\ y^7 + 6y^4 + 2y^3 + 12\}.$$



Specialization problem

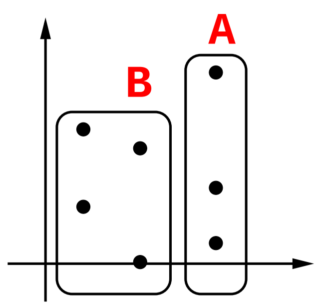
The following example illustrates the difficulties of designing a modular algorithm for triangular decompositions.

Let V be the zero-dimensional variety defined over $\mathbb{Q}$ by

$$\{326x - 10y^6 + 51y^5 + 17y^4 + 306y^2 + 102y + 34,\ y^7 + 6y^4 + 2y^3 + 12\}.$$

The unique decomposition for $x < y$ is A and B.

$$A \left| \begin{array}{l} y^3 + 6 \\ x - 1 \end{array} \right. , \quad B \left| \begin{array}{l} y^2 + x \\ x^2 + 2 \end{array} \right.$$



Specialization problem

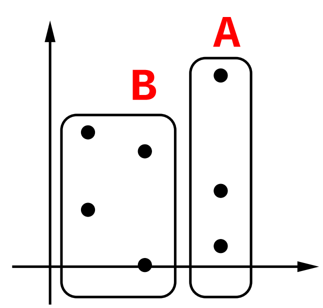
The following example illustrates the difficulties of designing a modular algorithm for triangular decompositions.

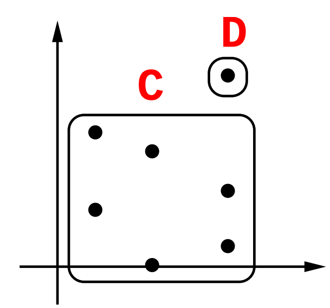
Let V be the zero-dimensional variety defined over $\mathbb{Q}$ by

$$\{326x - 10y^6 + 51y^5 + 17y^4 + 306y^2 + 102y + 34,\ y^7 + 6y^4 + 2y^3 + 12\}.$$

The unique decomposition for $x < y$ is A and B. Modulo $p = 7$, the zeros can be described by C and D.

$$A \left| \begin{array}{l} y^3 + 6 \\ x - 1 \end{array} \right. , \quad B \left| \begin{array}{l} y^2 + x \\ x^2 + 2 \end{array} \right. \qquad \Bigg\| \qquad C \left| \begin{array}{l} y^2 + 6yx^2 + 2y + x \\ x^3 + 6x^2 + 5x + 2 \end{array} \right. , \quad D \left| \begin{array}{l} y + 6 \\ x + 6 \end{array} \right.$$

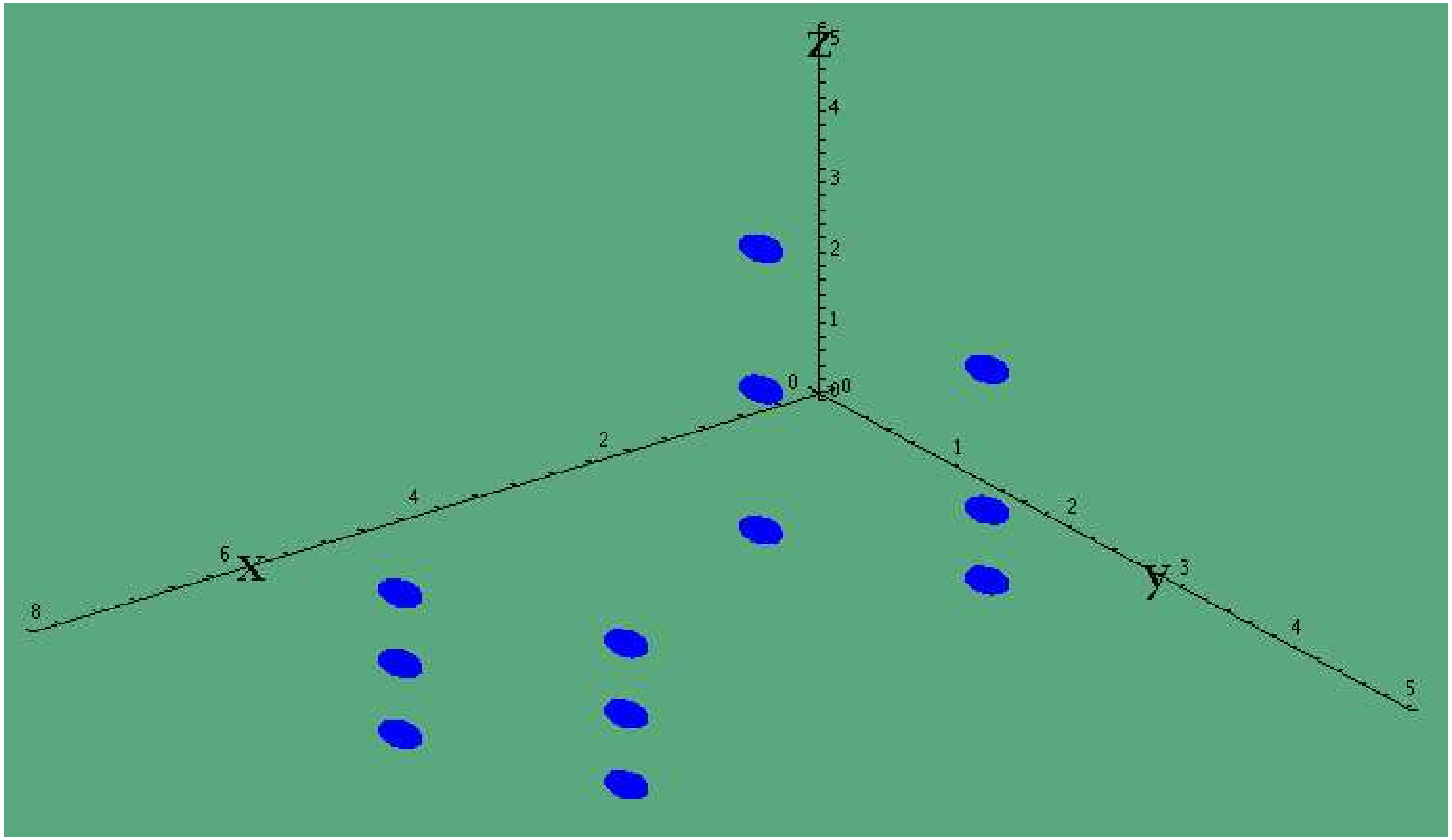




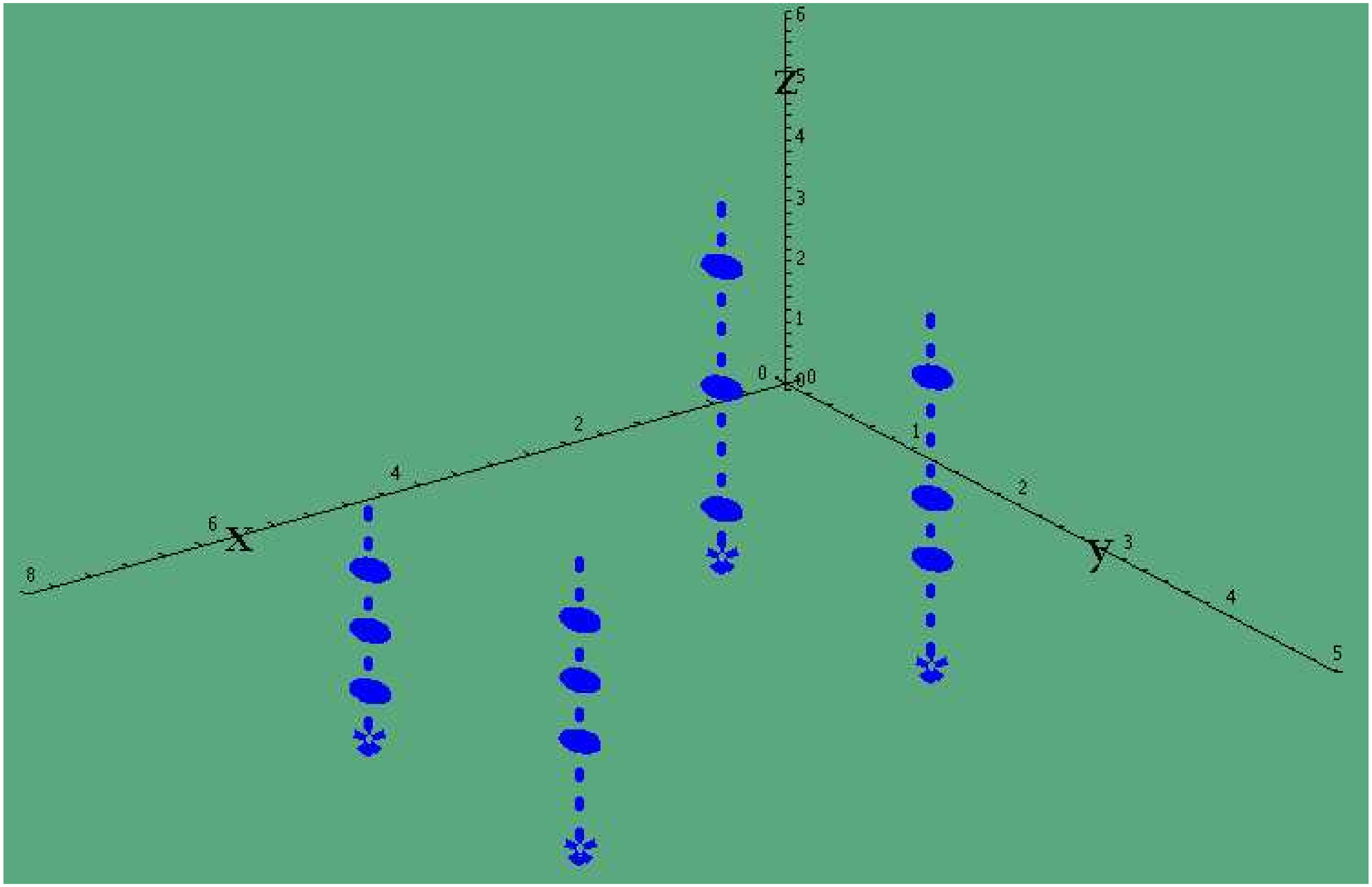
Equiprojectable decomposition: what it improves

- We introduce a canonical way of decomposing a zero-dimensional variety V into a union of equiprojectable ones: the equiprojectable decomposition of V.
- The notion of equiprojectable variety is motivated by:
  A zero-dimensional variety over a perfect field k is equiprojectable iff its defining ideal is generated by a triangular set (Aubry and Valibouze, 2000).
- The equiprojectable decomposition of V has good specialization properties modulo a prime number p.
- From any triangular decomposition of V we show how to compute the equiprojectable decomposition of V.
- Using Hensel lifting techniques, we deduce a modular algorithm for computing the equiprojectable decomposition of V.

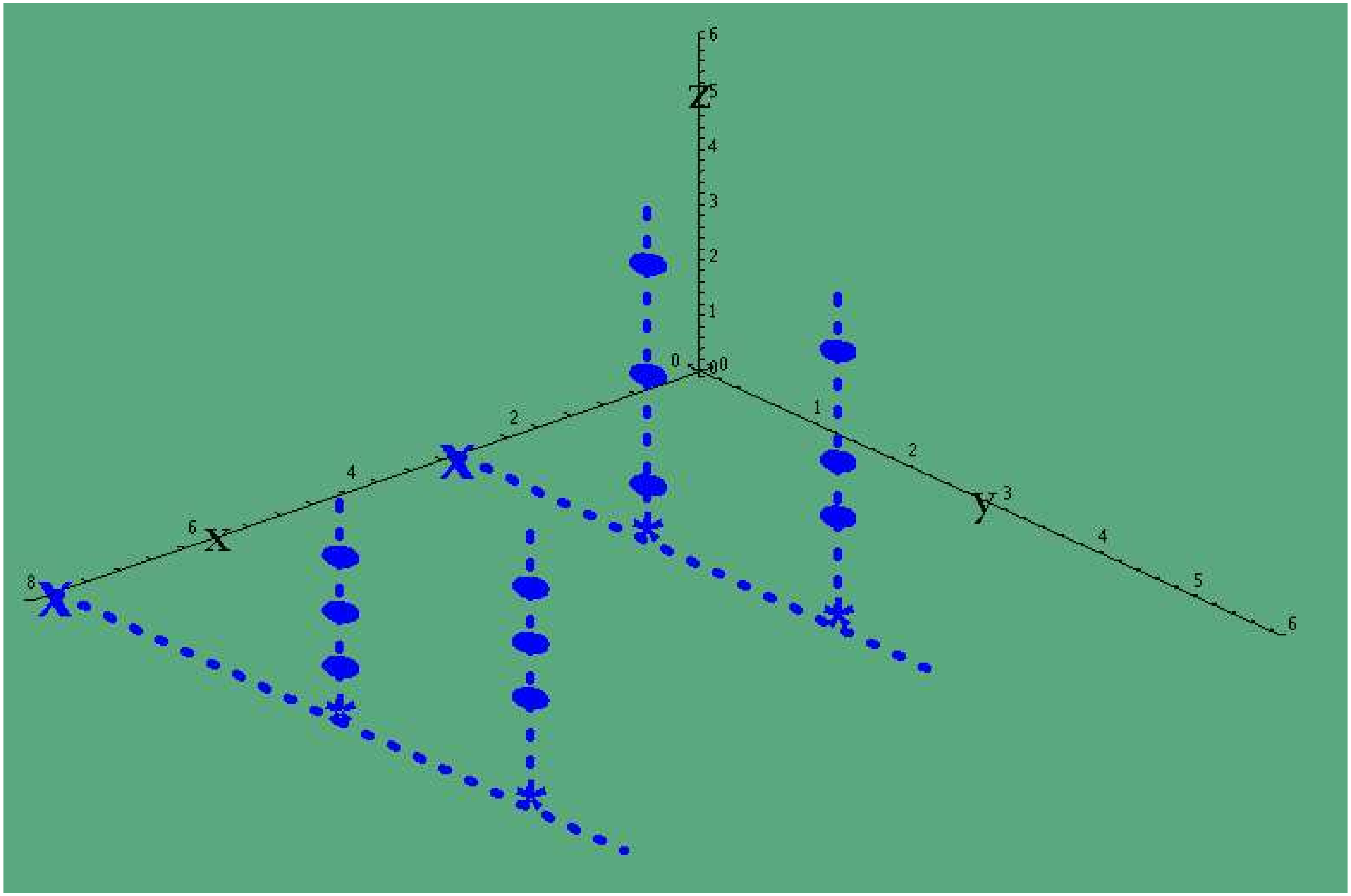
Equiprojectable variety definition (1/3)



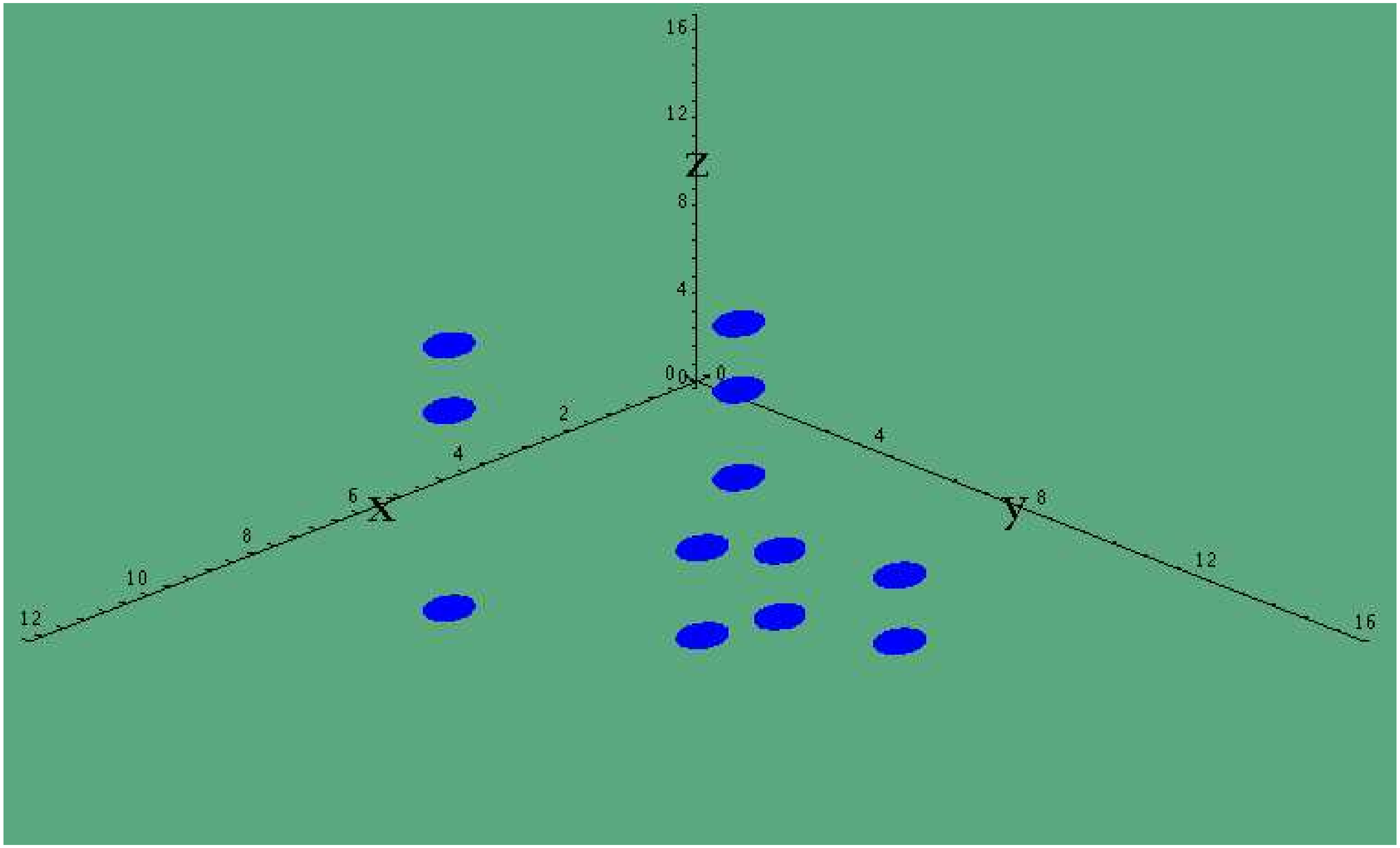
Equiprojectable variety definition (2/3)



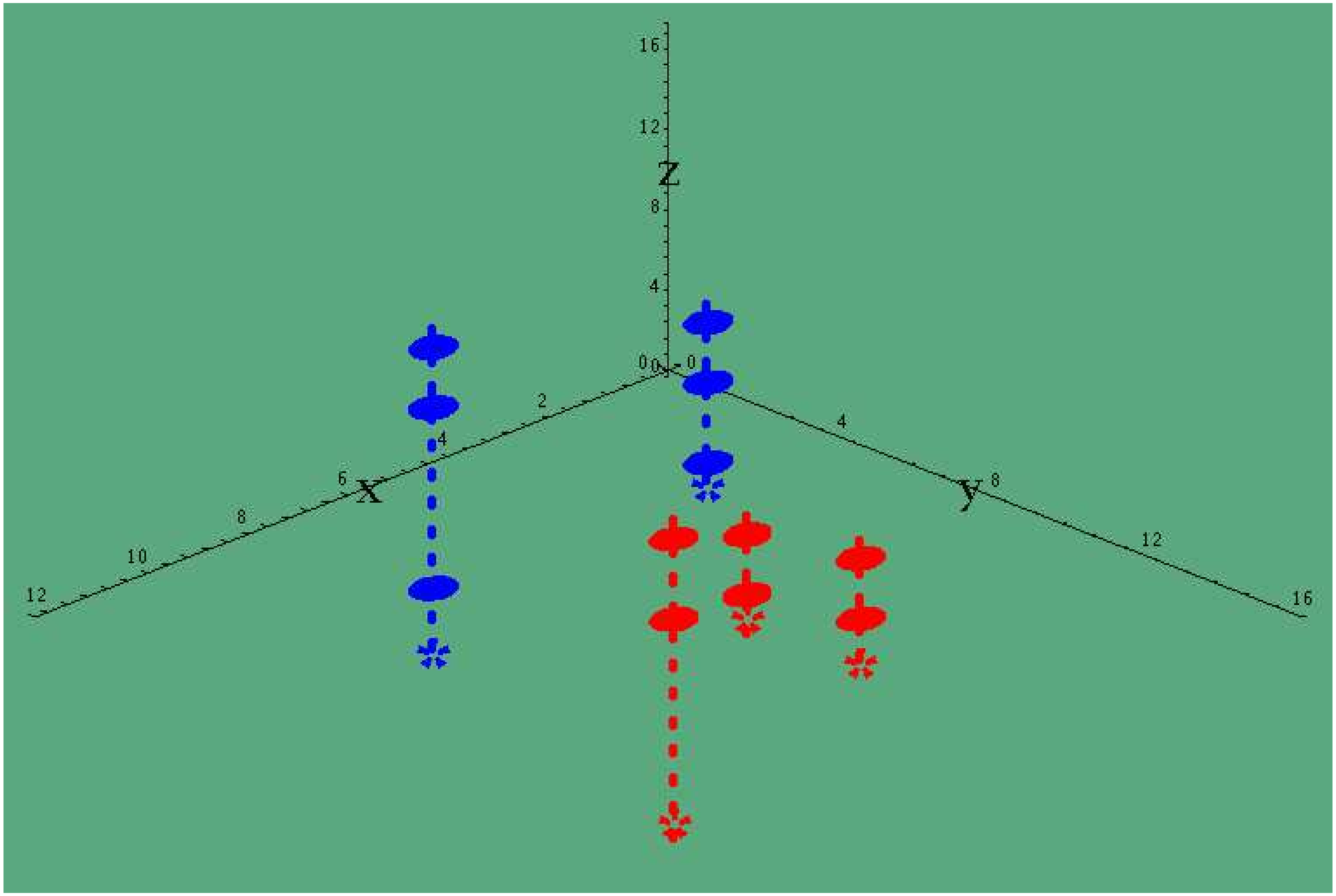
Equiprojectable variety definition (3/3)



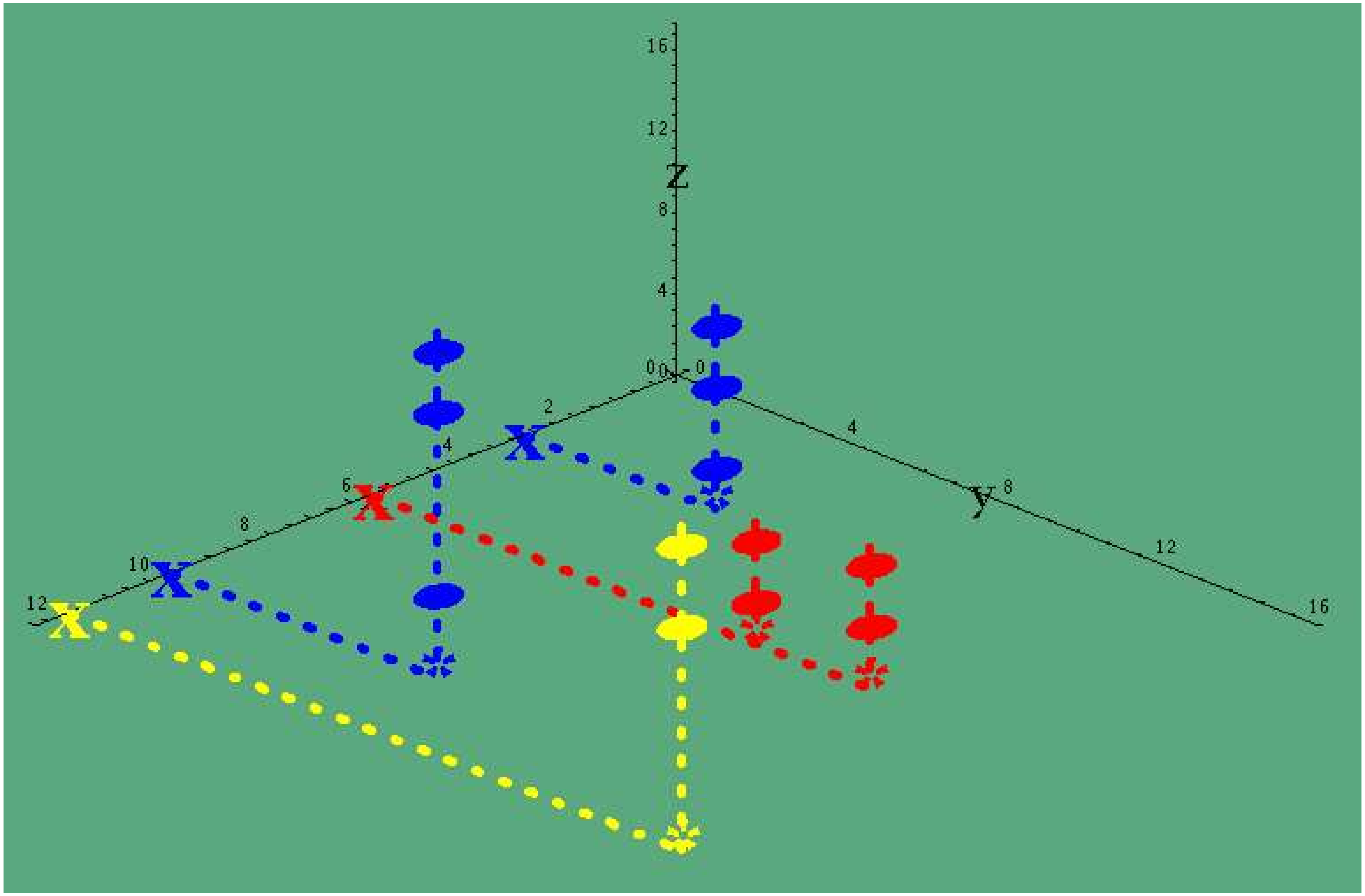
Equiprojectable decomposition definition (1/3)



Equiprojectable decomposition definition (2/3)



Equiprojectable decomposition definition (3/3)

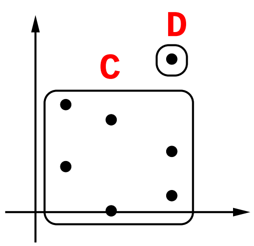


From triangular to equiprojectable decomposition

- Let Δ be a triangular decomposition of V over a field k.
- We compute from Δ another triangular decomposition $\{T^1, \ldots, T^d\}$ of V such that $V(T^1), \ldots, V(T^d)$ is the equiprojectable decomposition of V.
- We proceed into two steps:
  - split: reducing what we call *critical pairs* by means of GCD computations modulo triangular sets,
  - merge: reducing what we call *solvable pairs* by means of CRT computations modulo triangular sets.
- Complexity is work in progress (see the poster for a preliminary work).

Example: *split* + *merge* modulo 7

$$C \left| \begin{array}{l} C_2 = y^2 + 6yx^2 + 2y + x \\ C_1 = x^3 + 6x^2 + 5x + 2 \end{array} \right. \quad , \quad D \left| \begin{array}{l} D_2 = y + 6 \\ D_1 = x + 6 \end{array} \right.$$

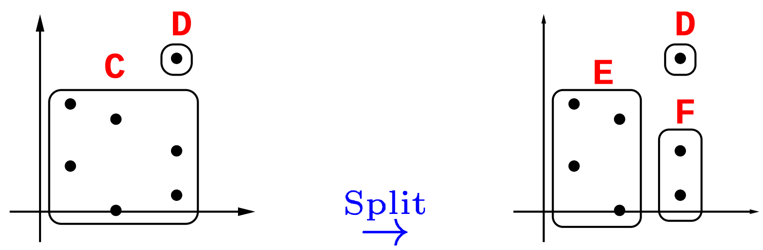


Example: *split+merge* modulo 7

$$C \left| \begin{array}{l} C_2 = y^2 + 6yx^2 + 2y + x \\ C_1 = x^3 + 6x^2 + 5x + 2 \end{array} \right. , \quad D \left| \begin{array}{l} D_2 = y + 6 \\ D_1 = x + 6 \end{array} \right.$$

$\downarrow$ Split C : GCD $\downarrow$

$$E \left| \begin{array}{l} {C_2}' = y^2 + x \\ {C_1}' = x^2 + 5 \end{array} \right. , \quad F \left| \begin{array}{l} C_2'' = y^2 + y + 1 \\ C_1'' = x + 6 \end{array} \right. , \quad D \left| \begin{array}{l} D_2 = y + 6 \\ D_1 = x + 6 \end{array} \right.$$



Example: *split+merge* modulo 7

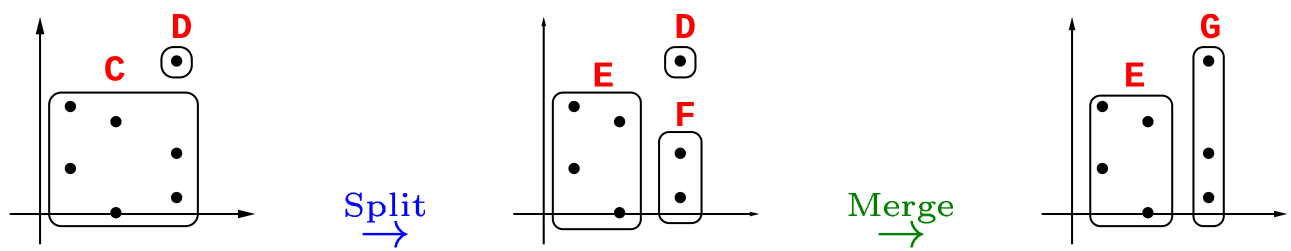
$$C \left| \begin{array}{l} C_2 = y^2 + 6yx^2 + 2y + x \\ C_1 = x^3 + 6x^2 + 5x + 2 \end{array} \right. , \quad D \left| \begin{array}{l} D_2 = y + 6 \\ D_1 = x + 6 \end{array} \right.$$

$\downarrow$ Split C : GCD $\downarrow$

$$E \left| \begin{array}{l} {C_2}' = y^2 + x \\ {C_1}' = x^2 + 5 \end{array} \right. , \quad F \left| \begin{array}{l} C_2'' = y^2 + y + 1 \\ C_1'' = x + 6 \end{array} \right. , \quad D \left| \begin{array}{l} D_2 = y + 6 \\ D_1 = x + 6 \end{array} \right.$$

$\downarrow$ Merge F and D : CRT $\downarrow$

$$E \left| \begin{array}{l} C_2' = y^2 + x \\ C_1' = x^2 + 5 \end{array} \right. , \quad G \left| \begin{array}{l} G_2 = y^3 + 6 \\ G_1 = x + 6 \end{array} \right.$$



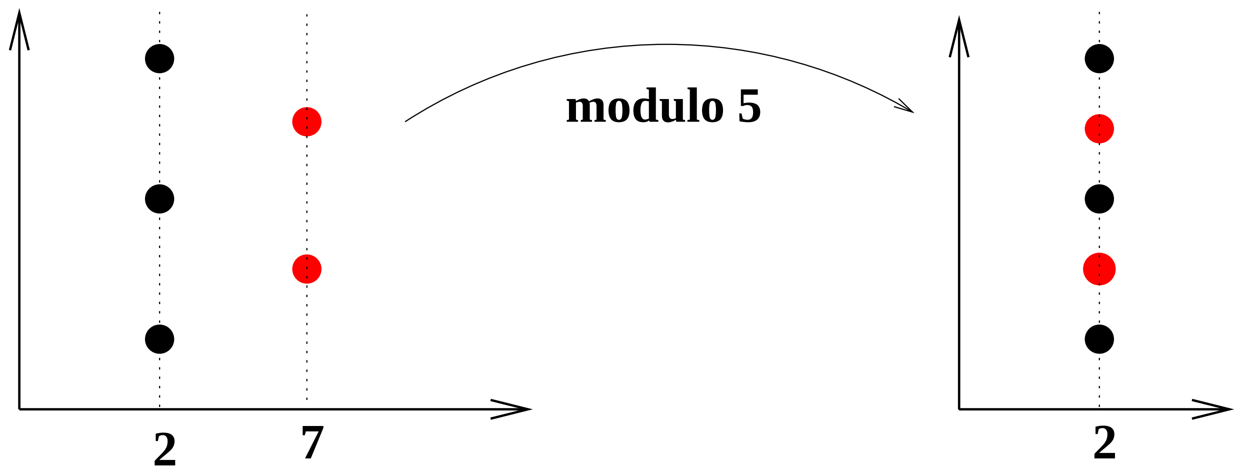
Specialization properties

Oversimplified case: all points in V are in $\mathbb{Q}^n$.

Theorem 1 *If:*

1. *p divides no denominator of the coordinates;*
2. *the cardinality of none of the projections of V decreases mod p;*

then the equiprojectable decomposition specializes mod p.



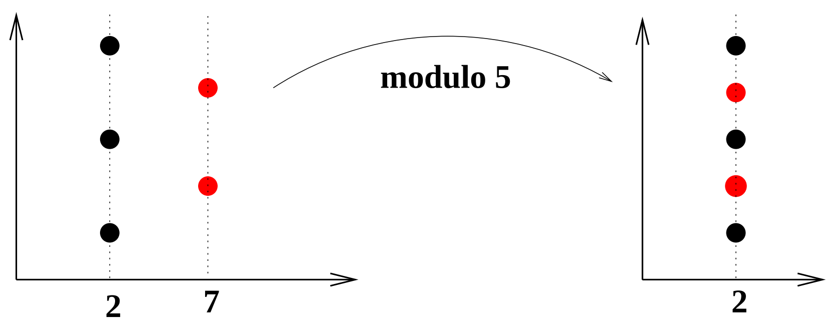
Specialization properties

Oversimplified case: all points in V are in $\mathbb{Q}^n$.

Theorem 2 *If:*

1. *p divides no denominator of the coordinates;*
2. *the cardinality of none of the projections of V decreases mod p;*

then the equiprojectable decomposition specializes mod p.



General case: Under *similar* assumptions, every coordinate of every point of V lies in a direct sum $\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ where $\mathbb{Z}_p$ is the ring of p-adic integers. This implies that $V \mod p$ is well defined.

Estimates for prime of good reduction

Let F a polynomial system with $V = V(F)$. Let h the maximum number of digits of all the coefficients, and d the maximum degree.

Corollary 1 *There exists $A \in \mathbb{N} - \{0\}$ such that:*

- $h(A) \leq 2n^2 d^{2n+1}(3h + 7\log(n+1) + 5n\log d + 10)$.
- *If p is a prime and does not divide A, then the equiprojectable decomposition specializes well mod p.*

Estimates for prime of good reduction

Let F a polynomial system with $V = V(F)$. Let h the maximum number of digits of all the coefficients, and d the maximum degree.

Corollary 2 *There exists* $A \in \mathbb{N} - \{0\}$ *such that:*

• $h(A) \leq 2n^2 d^{2n+1}(3h + 7\log(n+1) + 5n\log d + 10)$.

• *If* p *is a prime and does not divide* A*, then the equiprojectable decomposition specializes well mod* p*.*

Sketch of proof:

- Height bounds of the coefficients of the polynomials in a primitive element representation.

Estimates for prime of good reduction

Let F a polynomial system with $V = V(F)$. Let h the maximum number of digits of all the coefficients, and d the maximum degree.

Corollary 3 *There exists* $A \in \mathbb{N} - \{0\}$ *such that:*

• $h(A) \leq 2n^2 d^{2n+1}(3h + 7\log(n+1) + 5n \log d + 10)$.

• *If* p *is a prime and does not divide* A, *then the equiprojectable decomposition specializes well mod* p.

Sketch of proof:

- Height bounds of the coefficients of the polynomials in a primitive element representation.
- Arithmetic Bézout theorem (Philippon, Krick-Pardo-Sombra).

Estimates for prime of good reduction

Let F a polynomial system with $V = V(F)$. Let h the maximum number of digits of all the coefficients, and d the maximum degree.

Corollary 4 *There exists* $A \in \mathbb{N} - \{0\}$ *such that:*

• $h(A) \leq 2n^2 d^{2n+1}(3h + 7\log(n+1) + 5n\log d + 10)$.

• *If p is a prime and does not divide A, then the equiprojectable decomposition specializes well mod p.*

Sketch of proof:

- Height bounds of the coefficients of the polynomials in a primitive element representation.
- Arithmetic Bézout theorem (Philippon, Krick-Pardo-Sombra).
- Classical height bounds (Hadamard's bound, . . .)

A modular algorithm for triangular decomposition

Choice of primes:

• For a *deterministic* algorithm the prime p of reduction must be larger than A. However, A is *too large* for an efficient modular method.

• So, we present a *probabilistic* algorithm:

- involving smaller primes.
- the probability of success is explicitly quantified and can be made arbitrarily close to 1.
- the choice of $p \simeq \log A$ leads to more than 99% of success.

A modular algorithm for triangular decomposition

Choice of primes:

• For a *deterministic* algorithm the prime p of reduction must be larger than A. However, A is *too large* for an efficient modular method.

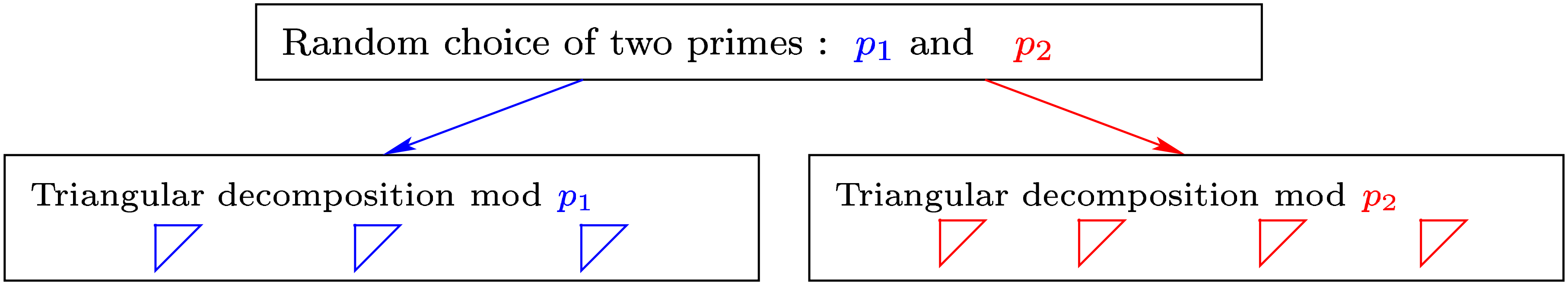
• So, we present a *probabilistic* algorithm:

- involving smaller primes.

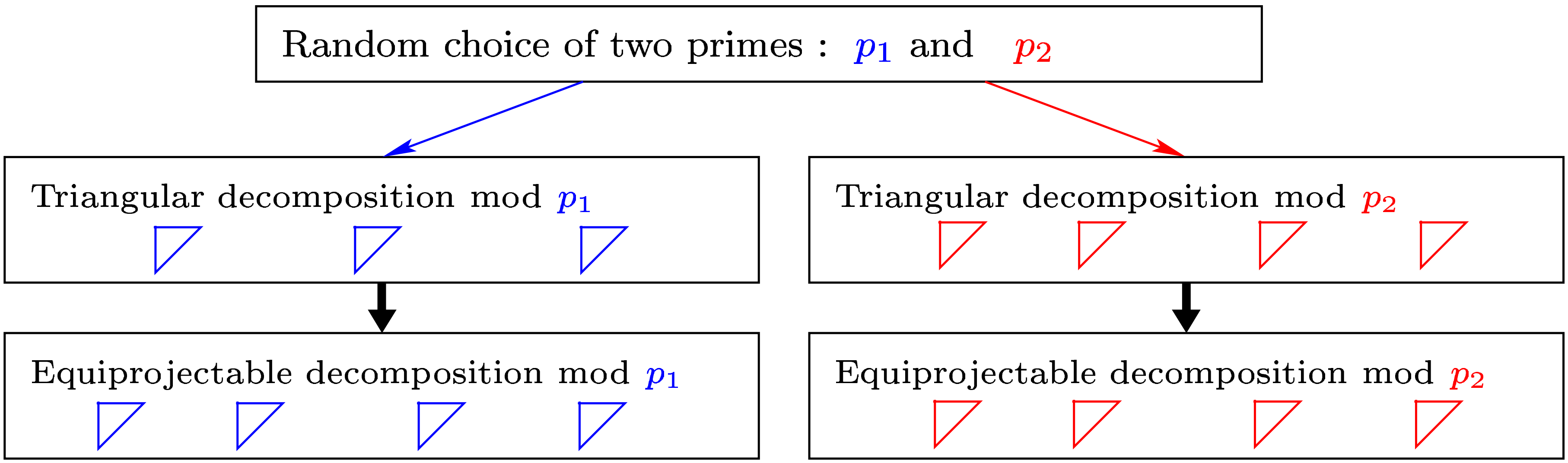
- the probability of success is explicitly quantified and can be made arbitrarily close to 1.

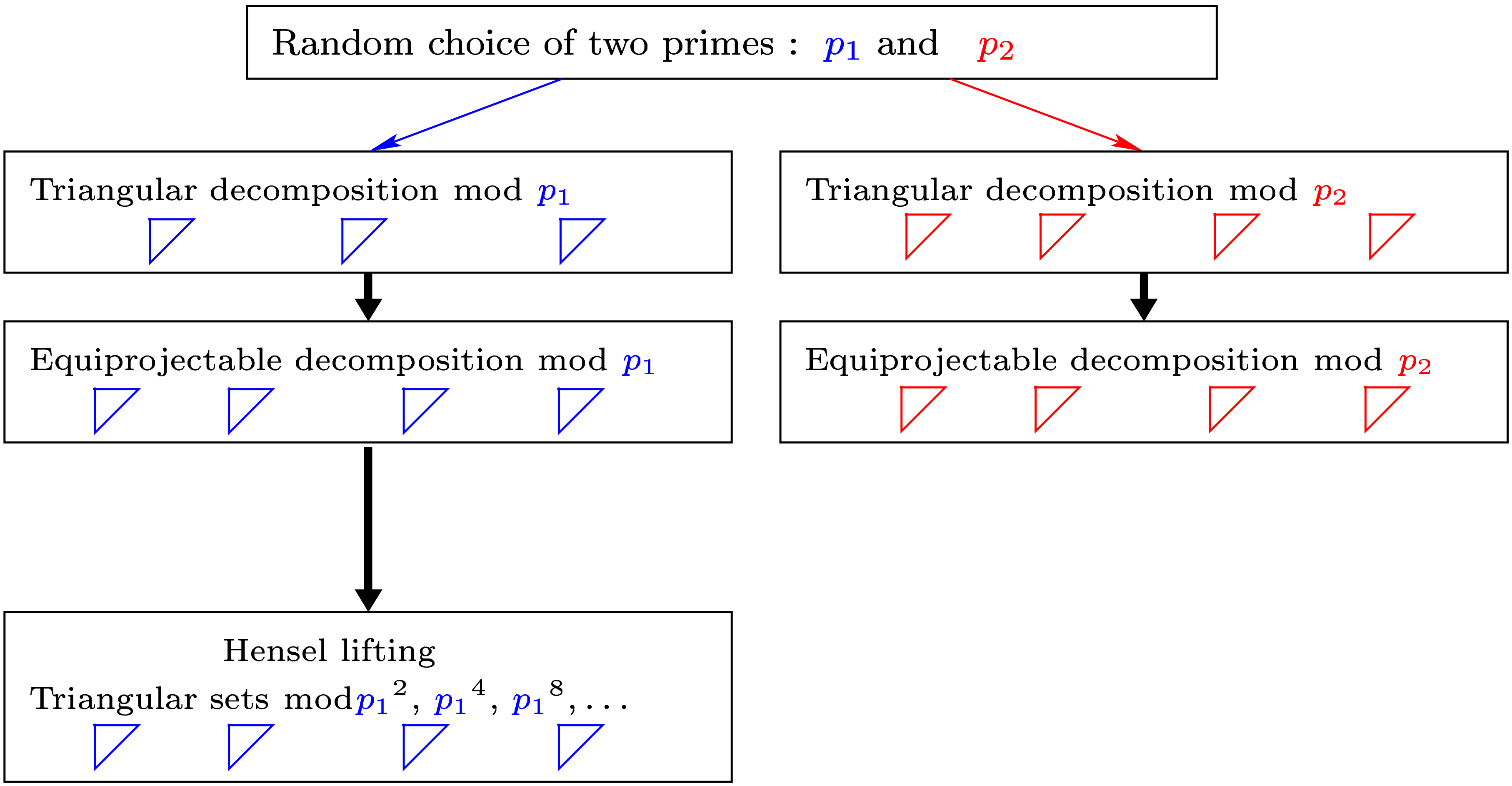
- the choice of $p \simeq \log A$ leads to more than 99% of success.

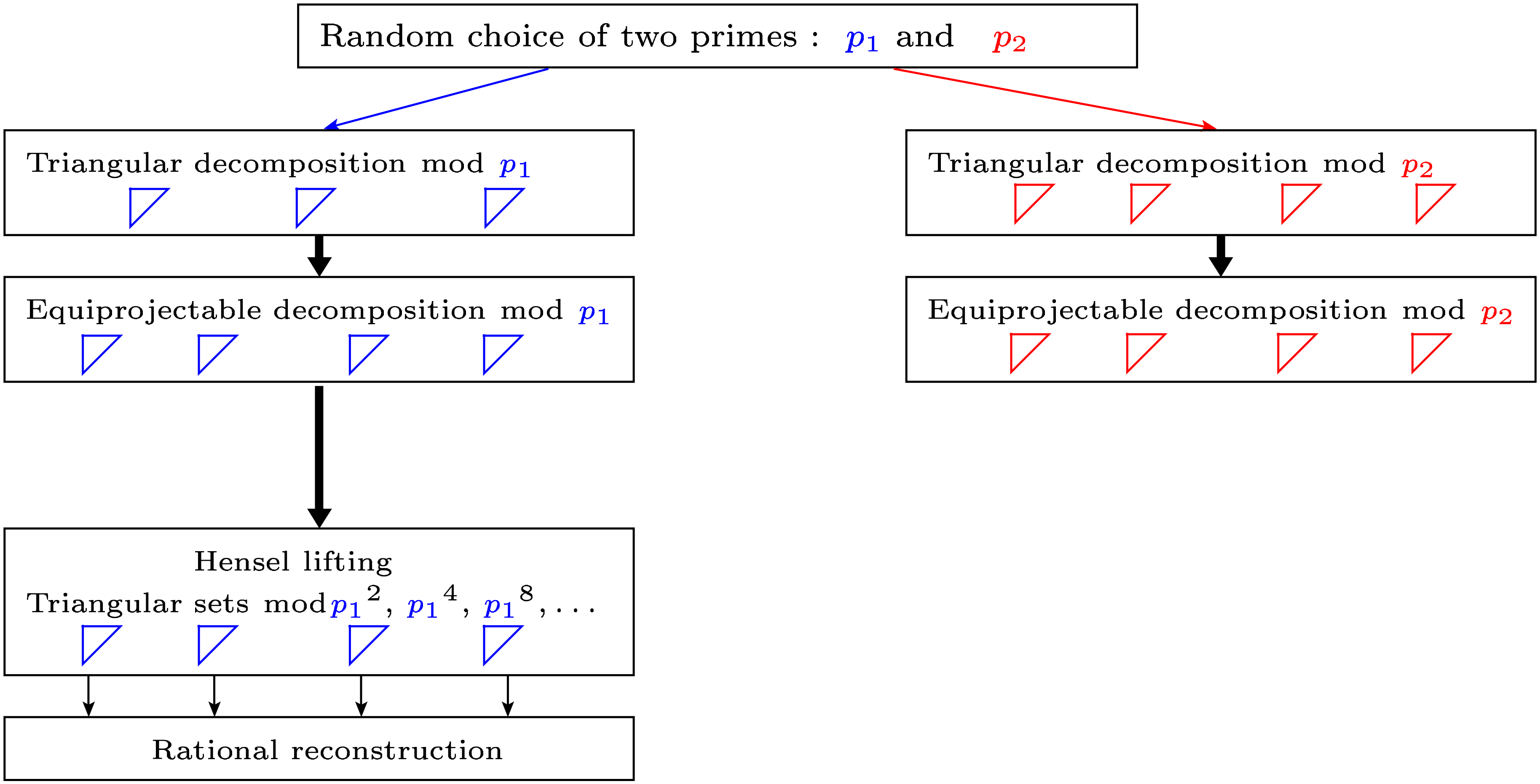
Hensel lifting for a triangular set: Already pointed out by (Schost 2003) ("Jacobian lifting").

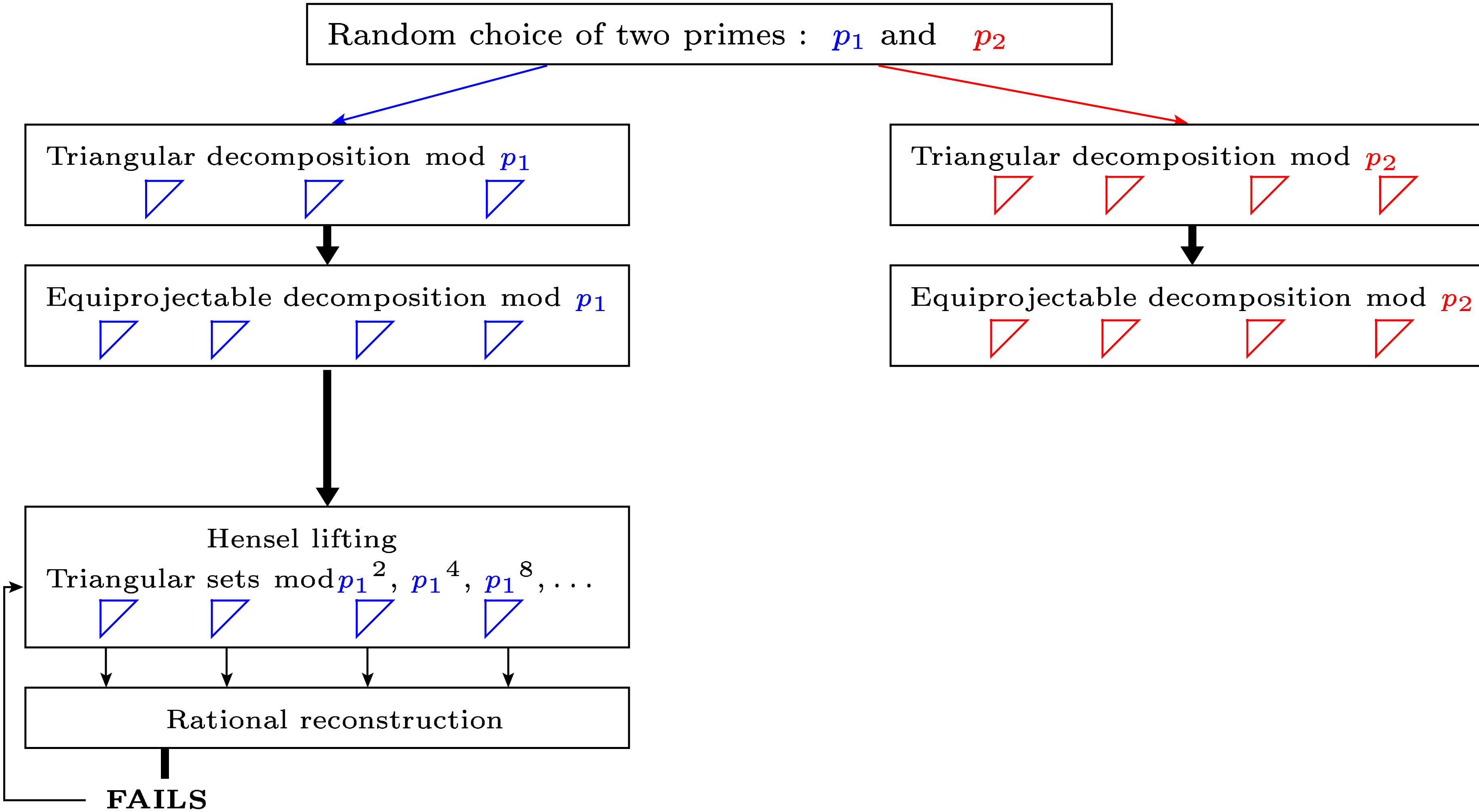


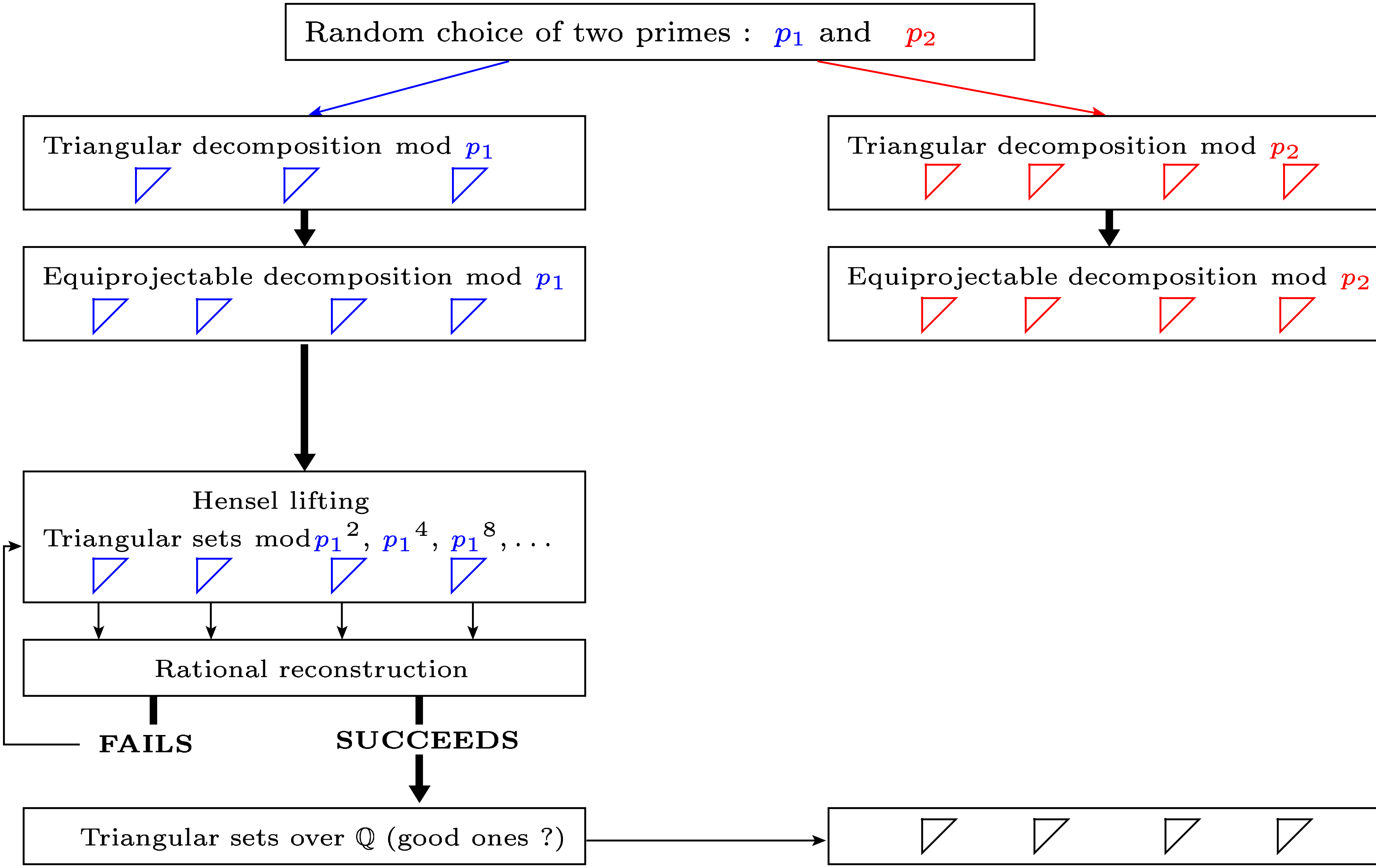
Random choice of two primes : p_1 and p_2
Triangular decomposition mod p_1
Triangular decomposition mod p_2


Random choice of two primes : p_1 and p_2
Triangular decomposition mod p_1
Triangular decomposition mod p_2
Equiprojectable decomposition mod p_1
Equiprojectable decomposition mod p_2

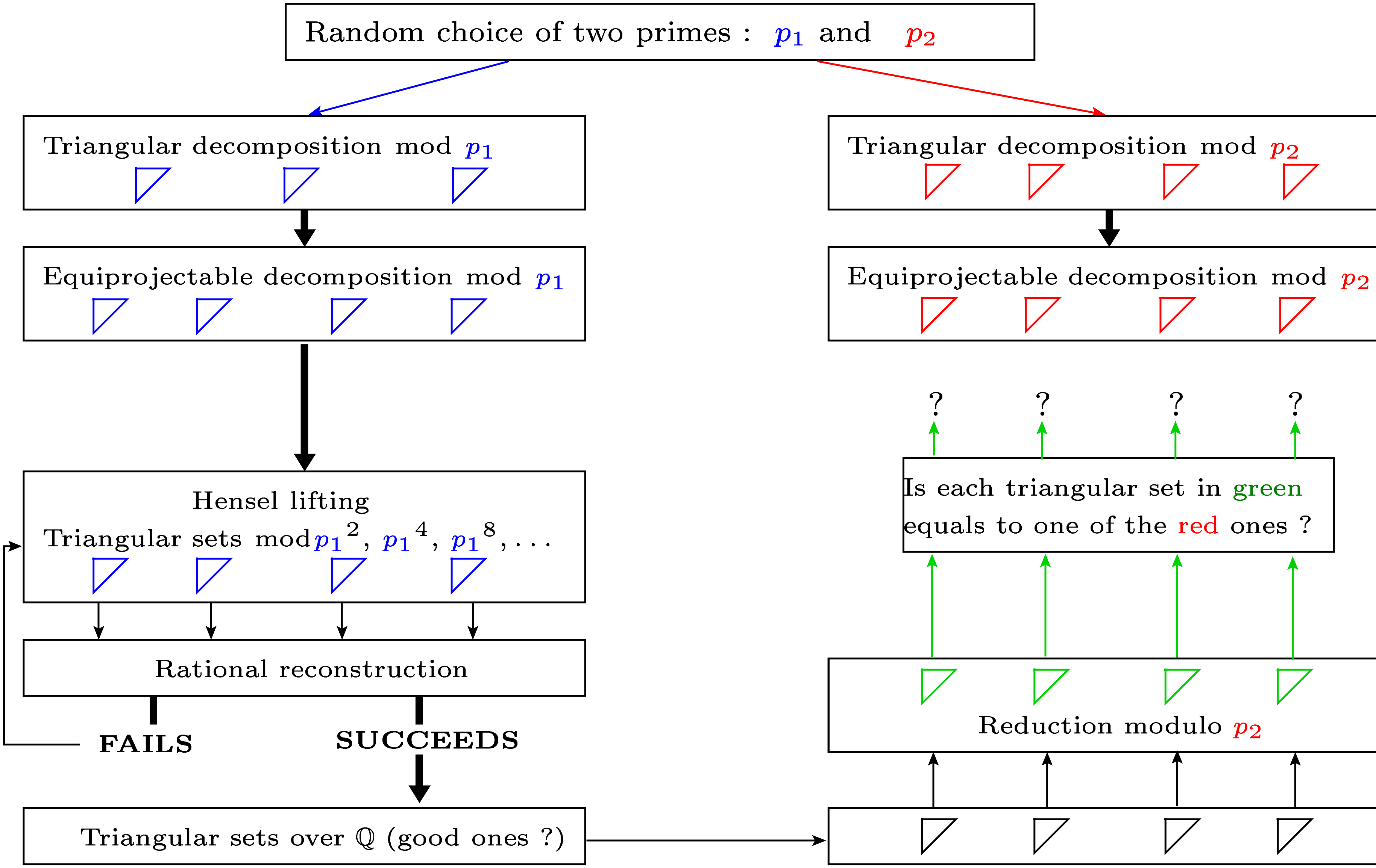

Random choice of two primes : p_1 and p_2
Triangular decomposition mod p_1
Triangular decomposition mod p_2
Equiprojectable decomposition mod p_1
Equiprojectable decomposition mod p_2
Hensel lifting
Triangular sets mod ${p_1}^2$, ${p_1}^4$, ${p_1}^8$, . . .


Random choice of two primes : p_1 and p_2
Triangular decomposition mod p_1
Triangular decomposition mod p_2
Equiprojectable decomposition mod p_1
Equiprojectable decomposition mod p_2
Hensel lifting
Triangular sets mod $p_1{}^2$, $p_1{}^4$, $p_1{}^8$, ...
Rational reconstruction

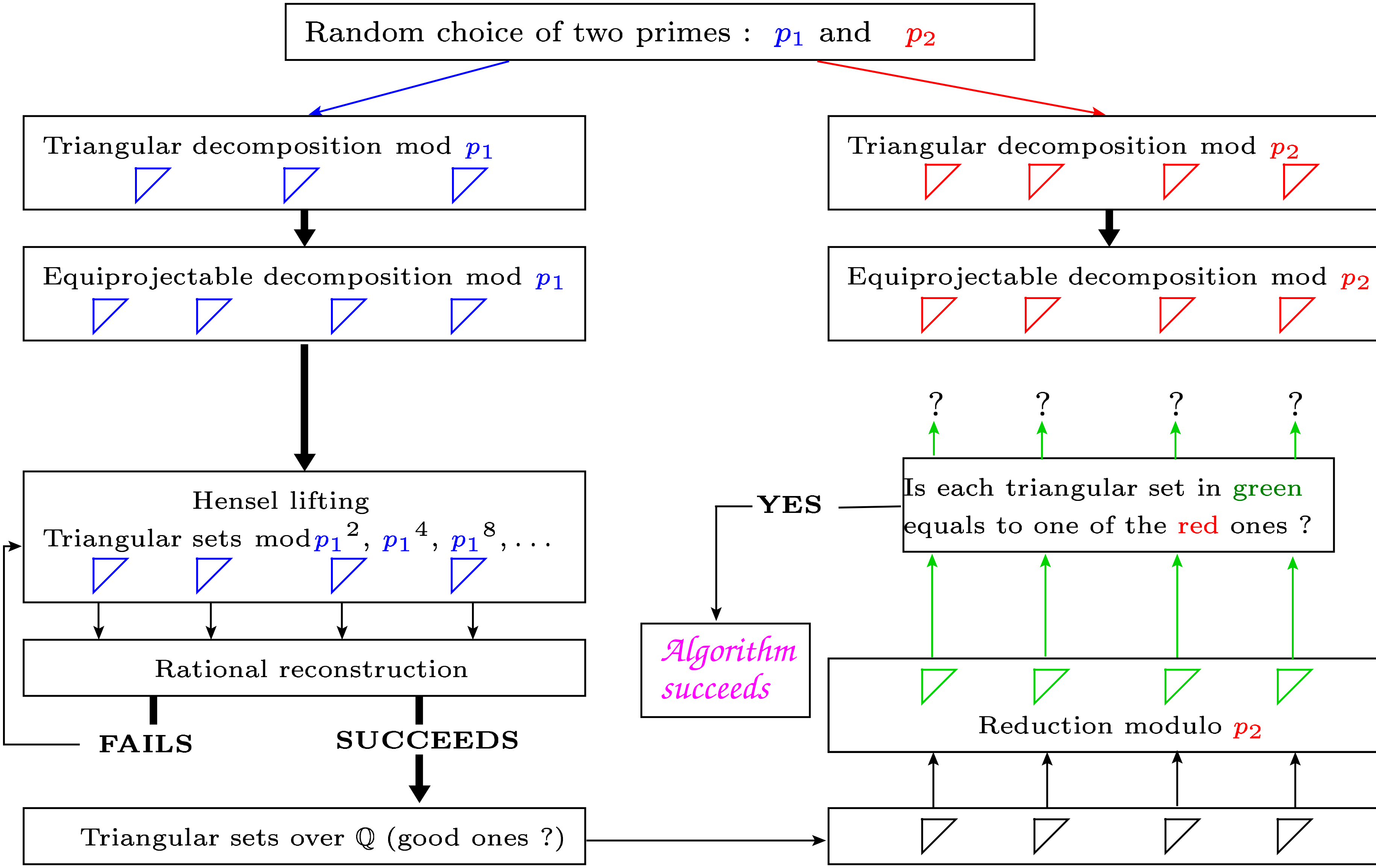

Random choice of two primes : p_1 and p_2
Triangular decomposition mod p_1
Triangular decomposition mod p_2
Equiprojectable decomposition mod p_1
Equiprojectable decomposition mod p_2
Hensel lifting
Triangular sets mod ${p_1}^2$, ${p_1}^4$, ${p_1}^8$, . . .
Rational reconstruction
FAILS



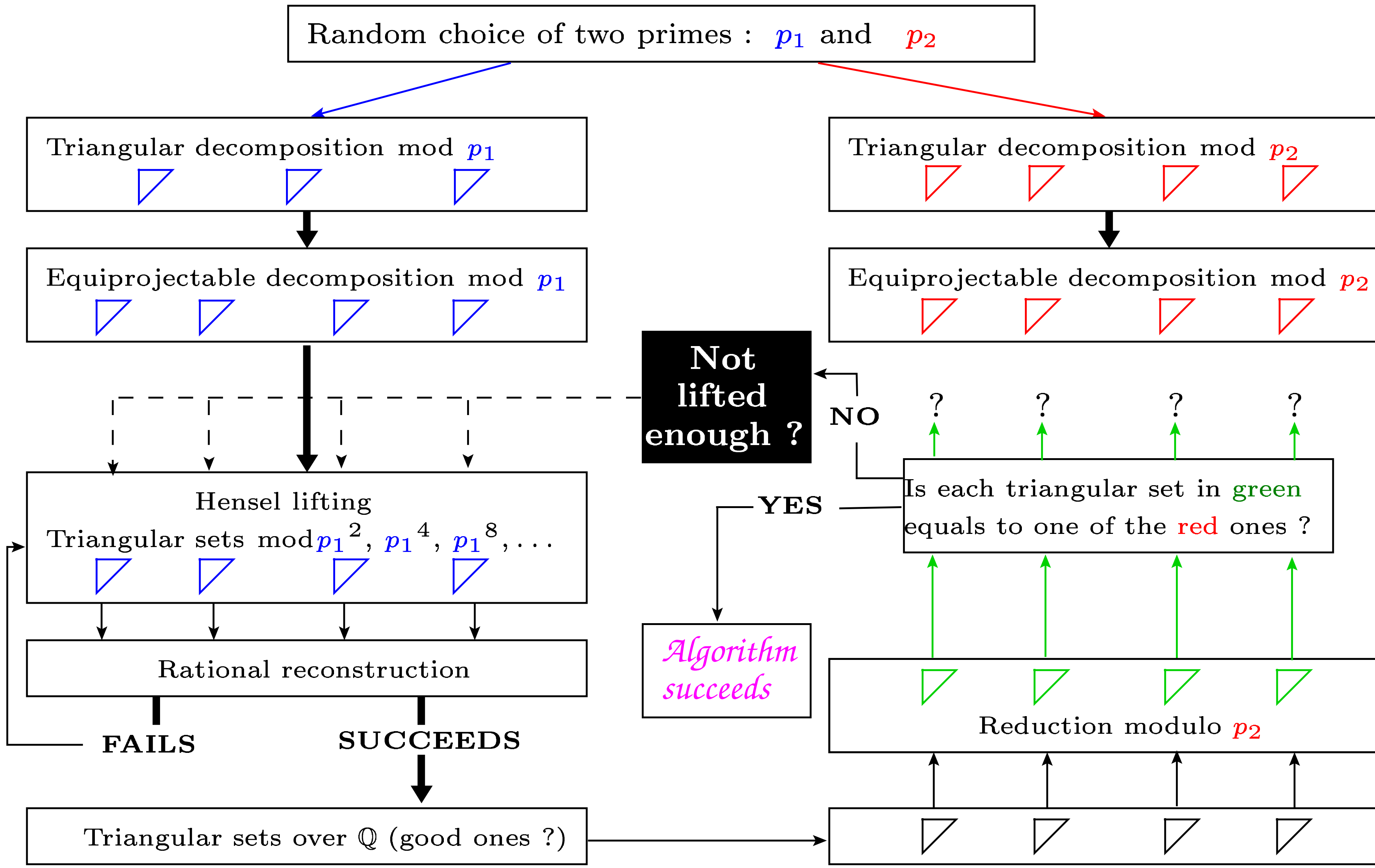
Random choice of two primes : p_1 and p_2
Triangular decomposition mod p_1
Triangular decomposition mod p_2
Equiprojectable decomposition mod p_1
Equiprojectable decomposition mod p_2
Hensel lifting
Triangular sets mod ${p_1}^2$, ${p_1}^4$, ${p_1}^8$, . . .
Rational reconstruction
FAILS
SUCCEEDS
Triangular sets over $\mathbb{Q}$ (good ones ?)



Random choice of two primes : p_1 and p_2
Triangular decomposition mod p_1
Equiprojectable decomposition mod p_1
Hensel lifting
Triangular sets mod $p_1{}^2$, $p_1{}^4$, $p_1{}^8$, ...
Rational reconstruction
FAILS
SUCCEEDS
Triangular sets over $\mathbb{Q}$ (good ones ?)
Triangular decomposition mod p_2
Equiprojectable decomposition mod p_2
?
?
?
?
Is each triangular set in green equals to one of the red ones ?
Reduction modulo p_2



Random choice of two primes : p_1 and p_2
Triangular decomposition mod p_1
Triangular decomposition mod p_2
Equiprojectable decomposition mod p_1
Equiprojectable decomposition mod p_2
?
?
?
?
Hensel lifting
Triangular sets mod $p_1{}^2$, $p_1{}^4$, $p_1{}^8$, . . .
YES
Is each triangular set in green equals to one of the red ones ?
Algorithm succeeds
Rational reconstruction
FAILS
SUCCEEDS
Reduction modulo p_2
Triangular sets over $\mathbb{Q}$ (good ones ?)



Random choice of two primes : p_1 and p_2
Triangular decomposition mod p_1
Triangular decomposition mod p_2
Equiprojectable decomposition mod p_1
Equiprojectable decomposition mod p_2
Not lifted enough ?
NO
? ? ? ?
Hensel lifting
Triangular sets mod $p_1{}^2$, $p_1{}^4$, $p_1{}^8$, ...
YES
Is each triangular set in green equals to one of the red ones ?
Algorithm succeeds
Rational reconstruction
Reduction modulo p_2
FAILS
SUCCEEDS
Triangular sets over $\mathbb{Q}$ (good ones ?)

Table 1: Features of the polynomial systems and prime number for the modular algorithm

Sys	Name	n	d	h	p_1
1	fabfaux	3	3	13	121458749
2	geneig	6	3	2	303179363351
3	eco6	6	3	0	509110405373
4	Weispfenning-94	3	5	0	3441898787
5	Issac97	4	2	2	49956859
6	dessin-2	10	2	7	2011551274283
7	eco7	7	3	0	5433767329489
8	Reimer-4	4	5	1	180771302617
9	Methan61	10	2	16	3557395585699
10	Uteshev-Bikker	4	3	3	2197378999

Table 2: Experimental results from Maple

on top of the RegularChains library in Maple (Lemaire, Moreno Maza, Xie)

Sys	`Trian.Mod` (sec)	`Trian.` (sec)	`gsolve` (sec)		`Trian.Mod` (MB)	`Trian.` (MB)	`gsolve` (MB)
1	27	512	1041		9	275	34
2	18	2.5	-		5	4	fail
3	50	5	9		6	5	5
4	100	3000	4950		12	250	66
5	161	-	1050		20	fail	31
6	524	-	-		14	fail	error
7	3795	1593	-		18	18	fail
8	5575	-	-		38	fail	fail
9	6184	∞	-		12	-	fail
10	8726	-	-		64	fail	fail

Conclusions

- We have introduced a way of encoding the solutions of polynomial systems, **Equiprojectable Decomposition**, which has good computational properties.
- Using Hensel lifting techniques we designed an efficient modular algorithm for solving polynomial systems of dimension zero.
- Our experimentation shows the capacity of this approach to solve problems out of the scope of other comparable solvers.
- Work is in progress on the complexity analysis of *split + merge*: see poster *On the complexity of the D5 principle*.
- We aim at extending this work to variable specialization
  - to speed up modular triangular decompositions.
  - to treat systems of positive dimension.
- An optimized implementation for our algorithm is in progress.