Polynomials over Power Series and their Applications to Limit Computations (tutorial version)

Marc Moreno Maza
University of Western Ontario
IBM Center for Advanced Studies

CASC 2018 Tutorial
Université de Lille
Bâtiment M^3
June 11, 2021

Plan

1. Polynomials over Power Series
   - The Hensel-Sasaki Construction: Bivariate Case

Plan

1. Polynomials over Power Series
   - The Hensel-Sasaki Construction: Bivariate Case

Plan

1. Polynomials over Power Series
   - The Hensel-Sasaki Construction: Bivariate Case

The extended Hensel construction (EHC)

Goal

- Factorize $F(X,Y) \in \mathbb{C}[X,Y]$ into linear factors in X over $\mathbb{C}(\langle Y^* \rangle)$:
$$F(X,Y) = (X - \chi_1(Y))(X - \chi_2(Y)) \cdots (X - \chi_d(Y))$$
where each $\chi_i(Y)$ is a *Puiseux series*.
- Thus offers an alternative algorithm to that of Newton-Puiseux.

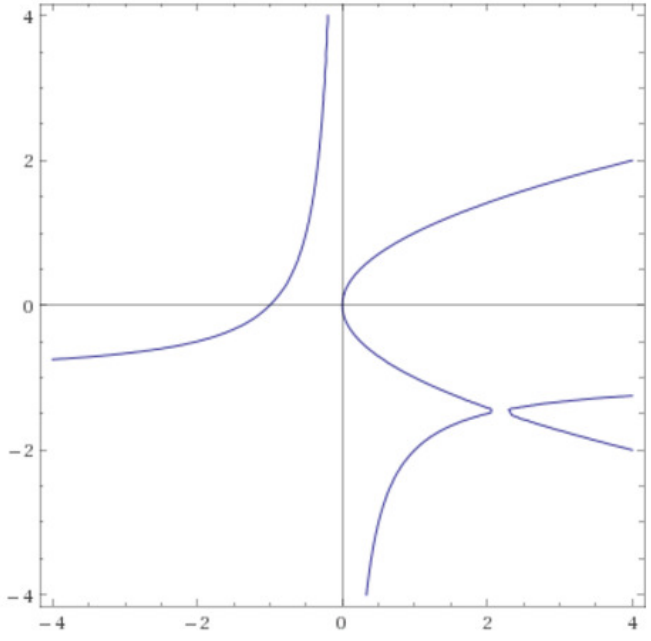
Remarks

- The EHC generalizes to factorize polynomials over multivariate power series rings
- Hence, the EHC has similar goal to Abhyankar-Jung theorem
- However, it is a weaker form:
  - less demanding hypotheses, and
  - weaker output format, making it easier to compute.

An example with the PowerSeries library

```
> P := PowerSeries([y]):
> U := UnivariatePolynomialOverPowerSeries([y], x):
> poly := y^2 *x + y^2 - y*x^3 - y*x^2 + y -x^2;
                                3      2        2    2    2
                    poly := -x  y - x  y + x y  - x  + y  + y

U:-ExtendedHenselConstruction(poly,[0],3);
                         -T - 1          2        2          2       2
          [[y = T, x = ------], [y = T , x = -T ], [y = T , x = T ]]
                           T
```



Another example

```
> P := PowerSeries([y, z]):
  U := UnivariatePolynomialOverPowerSeries([y, z], x):
  poly := y·x^3 + (-2·y + z + 1)·x + y:
  U:-ExtendedHenselConstruction(poly, [0, 0], 3);
```

$$\left[\left[x = \frac{-\mathit{RootOf}(\_Z^2 + y) + \mathit{RootOf}(\_Z^2 + y)\, y - \frac{1}{2}\,\mathit{RootOf}(\_Z^2 + y)\, z + \frac{1}{2}\, y^2}{y}\right],\right.$$

$$\left[x = \frac{\mathit{RootOf}(\_Z^2 + y) - \mathit{RootOf}(\_Z^2 + y)\, y + \frac{1}{2}\,\mathit{RootOf}(\_Z^2 + y)\, z + \frac{1}{2}\, y^2}{y}\right],$$

$$\left.[x = -y]\right]$$

Related works (1/2)

1. Extended Hensel Construction (EHC):
   - Introduction: F. Kako and T. Sasaki, 1999
   - Extensions:
     - M. Iwami, 2003,
     - D. Inaba, 2005,
     - D. Inaba and T. Sasaki 2007,
     - D. Inaba and T. Sasaki 2016.
2. Newton-Puiseux:
   - H. T. Kung and J. F. Traub, 1978,
   - D. V. Chudnovsky and G. V. Chudnovsky, 1986
   - A. Poteaux and M. Rybowicz, 2015.

Related works (2/2)

- The Extended Hensel Construction (EHC) compute all branches concurrently
- while approaches based on Newton-Puiseux computes one branch after another.

For $F(X,Y) := -X^3 + Y\,X + Y$:

1. the EHC produces
   1. $\chi_1(Y) := Y^{\frac{1}{3}} + \frac{1}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   2. $\chi_2(Y) := \frac{-1+\sqrt{-3}}{2}\,Y^{\frac{1}{3}} + \frac{1}{3}\,(\frac{-1-\sqrt{-3}}{2})\,Y^{\frac{2}{3}} + O(Y)$,
   3. $\chi_3(Y) := (\frac{-1-\sqrt{-3}}{2})\,Y^{\frac{1}{3}} + \frac{1}{3}\,(\frac{-1+\sqrt{-3}}{2})\,Y^{\frac{2}{3}} + O(Y)$.
2. Whereas Kung-Traub's method (based on Newton-Puiseux) computes
   1. $\chi_1(Y) := Y^{\frac{1}{3}} + \frac{1}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   2. $\chi_2(Y) := \theta\,Y^{\frac{1}{3}} + \frac{\theta^2}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   3. $\chi_3(Y) := \theta^2\,Y^{\frac{1}{3}} + \frac{\theta}{3}\,Y^{\frac{2}{3}} + O(Y)$,

   for $\theta \in \mathbb{C}$ such that $\theta^3 = 1, \theta^2 \neq 1, \theta \neq 1$, since $F(X,Y)$ is a Weierstrass polynomial.

Related works (2/2)

- The Extended Hensel Construction (EHC) compute all branches concurrently
- while approaches based on Newton-Puiseux computes one branch after another.

For $F(X,Y) := -X^3 + Y\,X + Y$:

1. the EHC produces
   1. $\chi_1(Y) := Y^{\frac{1}{3}} + \frac{1}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   2. $\chi_2(Y) := \frac{-1+\sqrt{-3}}{2}\,Y^{\frac{1}{3}} + \frac{1}{3}\,(\frac{-1-\sqrt{-3}}{2})\,Y^{\frac{2}{3}} + O(Y)$,
   3. $\chi_3(Y) := (\frac{-1-\sqrt{-3}}{2})\,Y^{\frac{1}{3}} + \frac{1}{3}\,(\frac{-1+\sqrt{-3}}{2})\,Y^{\frac{2}{3}} + O(Y)$.
2. Whereas Kung-Traub's method (based on Newton-Puiseux) computes
   1. $\chi_1(Y) := Y^{\frac{1}{3}} + \frac{1}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   2. $\chi_2(Y) := \theta\,Y^{\frac{1}{3}} + \frac{\theta^2}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   3. $\chi_3(Y) := \theta^2\,Y^{\frac{1}{3}} + \frac{\theta}{3}\,Y^{\frac{2}{3}} + O(Y)$,

   for $\theta \in \mathbb{C}$ such that $\theta^3 = 1, \theta^2 \neq 1, \theta \neq 1$, since $F(X,Y)$ is a Weierstrass polynomial.

Related works (2/2)

- The Extended Hensel Construction (EHC) compute all branches concurrently
- while approaches based on Newton-Puiseux computes one branch after another.

For $F(X,Y) := -X^3 + Y\,X + Y$:

1. the EHC produces
   1. $\chi_1(Y) := Y^{\frac{1}{3}} + \frac{1}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   2. $\chi_2(Y) := \frac{-1+\sqrt{-3}}{2}\,Y^{\frac{1}{3}} + \frac{1}{3}\,(\frac{-1-\sqrt{-3}}{2})\,Y^{\frac{2}{3}} + O(Y)$,
   3. $\chi_3(Y) := (\frac{-1-\sqrt{-3}}{2})\,Y^{\frac{1}{3}} + \frac{1}{3}\,(\frac{-1+\sqrt{-3}}{2})\,Y^{\frac{2}{3}} + O(Y)$.
2. Whereas Kung-Traub's method (based on Newton-Puiseux) computes
   1. $\chi_1(Y) := Y^{\frac{1}{3}} + \frac{1}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   2. $\chi_2(Y) := \theta\,Y^{\frac{1}{3}} + \frac{\theta^2}{3}\,Y^{\frac{2}{3}} + O(Y)$,
   3. $\chi_3(Y) := \theta^2\,Y^{\frac{1}{3}} + \frac{\theta}{3}\,Y^{\frac{2}{3}} + O(Y)$,

   for $\theta \in \mathbb{C}$ such that $\theta^3 = 1, \theta^2 \neq 1, \theta \neq 1$, since $F(X,Y)$ is a Weierstrass polynomial.

Overview

Notations

- Let $F(x, y) \in \mathbb{C}[x, y]$ be square-free, monic in x and let $d := \deg_x(F)$.
- Note that assuming $F(x, y)$ is general in x of order $d = \deg_x(F)$ (thus meaning $F(x, 0) = x^d$ and $F(x, y)$ is a Weierstrass polynomial) is a stronger condition, which is not required here.
- On can easily reduce to the case where F is monic in x as long as the leading coefficient of F in x can be seen an invertible power series in $\mathbb{C}\langle y \rangle$.

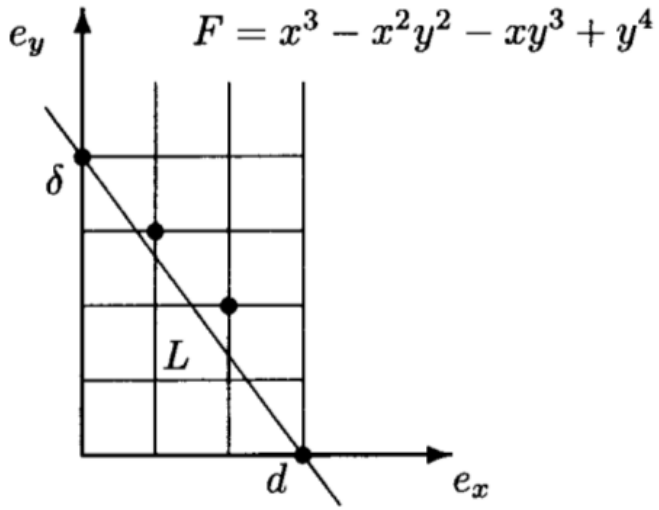
Objectives

- The final goal is to to factorize F over the field $\mathbb{C}(\langle y^* \rangle)$ of convergent Puiseux series over $\mathbb{C}$.
- This follows the ideas of Hensel lemma: lifting the factors of an initial factorization.
- If the initial factorization has no multiple roots, then we are able to generate the homogeneous parts (one degree after another) of the coefficients of the factors predicted by Puiseux's theorem.

Newton line (1/2)

Definition

- We consider a 2D grid G where the Cartesian coordinates (e_x, e_y) of a point are integers.
- Each nonzero term $c\,x^{e_x}y^{e_y}$ of $F(x, y)$, with $c \in \mathbb{C}$ is mapped to the point of coordinates (e_x, e_y) on the grid.
- Let L be the straight line passing through the point $(d, 0)$ as well as another point of the plot of F such that no points in the plot of F lye below L; The line L is called the *Newton line* of F.



Newton line (2/2)

```
> F := x^3  - x^2 * y^2  -x*y^3 + y^4;
                                    2  2      3    4    3
                          F := -x  y  - x y  + y  + x
> U := UnivariatePolynomialOverPowerSeries([y], x):
> U:-ExtendedHenselConstruction(F,[0],2);
                                          5      6
       3       4            5       T      T
[[y = T , x = T  %1 - 1/3 T  %1 + ---- + ----],
                                    3      3
          3        4        5        6
    [y = T , x = -T  - 1/3 T  + 1/3 T ],
                                              6
          3        4       4        5       T
    [y = T , x = -T  %1 + T  + 1/3 T  %1 + ----]]
                                             3
                 2
%1 := RootOf(_Z  - _Z + 1)
```

Newton polynomial

Definition

The sum of all the terms of $F(x, y)$, which are plotted on the Newton line of F is called the *Newton polynomial* of F and is denoted by $F^{(0)}(x, y)$.

Remarks

- The Newton polynomial is uniquely determined and has at least two terms.
- Let $\delta \in \mathbb{Q}$ such that the equating of the Newton line is $e_x/d + e_y/\delta = 1$.
- Observe that $F^{(0)}(x, y)$ is homogeneous in $(x, y^{\delta/d})$ of degree d.
- That is, $F^{(0)}(x, y)$ consists of monomials included in the set $\{x^d, x^{d-1}y^{\delta/d}, x^{d-2}y^{2\delta/d}, \ldots, y^{d\delta/d}\}$.

Factorizing Newton polynomial (1/2)

Notations

Let $r \geq 1$ be an integer, let $\zeta_1, \ldots, \zeta_r \in \mathbb{C}$, with $\zeta_i \neq \zeta_j$ for any $i \neq j$ and let $m_1, \ldots, m_r \in \mathbb{N}$ be positive such that we have

$$F^{(0)}(x, 1) = (x - \zeta_1)^{m_1} \cdots (x - \zeta_r)^{m_r}.$$

Recall that $F^{(0)}(x, y)$ is homogeneous in $(x, y^{\delta/d})$ of degree d.

Lemma

We have:

$$F^{(0)}(x, y) = (x - \zeta_1 y^{\delta/d})^{m_1} \cdots (x - \zeta_r y^{\delta/d})^{m_r}.$$

Proof of the lemma

- It is enough to show that $(\zeta_i y^{\delta/d}, y)$ vanishes $F^{(0)}(x, y)$ for all y.
- Define $\hat{y} = y^{\delta/d}$ such that $F^{(0)}(x, \hat{y})$ is homogeneous of degree d in $(x, \hat{y})$.
- Since each monomial of $F^{(0)}(x, \hat{y})$ is of the form $x^{e_x} y^{e_y}$ where $e_x + e_y = d$, we have

$$F^{(0)}(\zeta_i \hat{y}, \hat{y}) = \hat{y}^d \underbrace{(\cdots)}_{\text{some constant terms}} = 0.$$

- The last equality is valid since $F^{(0)}(\zeta_i, 1) = 0$ clearly holds.

Factorizing Newton polynomial (2/2)

```
> F := x^3  - x^2 * y^2  -x*y^3 + y^4;
                                  2  2      3    4    3
                          F := -x  y  - x y  + y  + x

>  L := x^3 - y^4;
                                        4    3
                                  L := -y  + x

> PolynomialTools:-Split(eval(L,[y=1]), x);
                           2                                  2
  (x - 1) (x - RootOf(_Z  + _Z + 1)) (x + 1 + RootOf(_Z  + _Z + 1))

> U:-ExtendedHenselConstruction(F,[0],1);
                                      5      6
       3       4           5       T      T
[[y = T , x = T  %1 - 1/3 T  %1 + ---- + ----],
                                      3      3
          3        4        5        6
    [y = T , x = -T  - 1/3 T  + 1/3 T ],
                                             6
          3        4       4        5       T
    [y = T , x = -T  %1 + T  + 1/3 T  %1 + ----]]
                                             3
                 2
%1 := RootOf(_Z  - _Z + 1)
```

The moduli of the Hensel-Sasaki construction (1/2)

Notations

Let $\hat{\delta}, \hat{d} \in \mathbb{Z}^{>0}$ such that:

$$\hat{\delta}/\hat{d} = \delta/d, \quad \gcd \hat{\delta}, \hat{d} = 1$$

Choosing such integers $\hat{\delta}, \hat{d}$ is possible since $\delta \in \mathbb{Q}$ and $d \in \mathbb{N}^{>0}$.

Lemma

Each non-constant monomial of $F(x, y)$ is contained in the set

$$\{x^d y^{(k+0)/\hat{d}}, x^{d-1} y^{(k+\hat{\delta})/\hat{d}}, x^{d-2} y^{(k+2\hat{\delta})/\hat{d}}, \ldots, x^0 y^{(k+d\hat{\delta})/\hat{d}} \mid k = 0, 1, 2, \ldots\}.$$

Proof of the lemma

- It is enough to show that for each exponent vector (e_x, e_y) which is not below the Newton's line, there exists i, k such that we have $x^{e_x} y^{e_y} = x^{d-i} y^{(k+i\hat{\delta})/\hat{d}}$.
- Given such an exponent vector (e_x, e_y), let us choose $i = d - e_x$ and $k = e_y \hat{d} - i\hat{\delta}$.
- One should check, of course, that $k \geq 0$ holds, which follows easily from $e_x/d + e_y/\delta \geq 1$.

The moduli of the Hensel-Sasaki construction (2/2)

Notations

The previous lemma leads us to define the following monomial ideals

$$\begin{aligned} S_k &= <x, y^{\hat{\delta}/\hat{d}}>^d \times <y^{1/\hat{d}}>^k \\ &= <x^d, x^{d-1}y^{\hat{\delta}/\hat{d}}, x^{d-2}y^{2\hat{\delta}/\hat{d}}, \ldots, x^0 y^{d\hat{\delta}/\hat{d}}> \times <y^{1/\hat{d}}>^k \\ &= <x^d y^{(k+0)/\hat{d}}, x^{d-1}y^{(k+\hat{\delta})/\hat{d}}, x^{d-2}y^{(k+2\hat{\delta})/\hat{d}}, \ldots, x^0 y^{(k+d\hat{\delta})/\hat{d}}> \end{aligned}$$

Remark

- The generators of $<x, y^{\hat{\delta}/\hat{d}}>^d$ are homogeneous monomials in $(x, y^{\hat{\delta}/\hat{d}})$ of degree d.
- We can view S_k as a polynomial ideal in the variables x and $y^{1/\hat{d}}$; note that the monomials generating S_k regarded in this way do not all have the same total degree.
- We shall use the ideals S_k, for $k = 1, 2, \ldots$, as moduli of the Hensel-Sasaki construction to be described hereafter.
- We have $F(x, y) \equiv F^{(0)}(x, y) \mod S^{(1)}$.

A weak but algrithmic version of Puiseux theorem (1/2)

As before, for $F \in \mathbb{C}[x, y]$ (and in fact, even for $F(x, y) \in \mathbb{C}\langle y \rangle[x]$) our ultimate goal is to factorize $F(x, y)$ as

$$F(x, y) = G_1(x, y) \cdots G_r(x, y)$$

where

1. this factorization holds in $\mathbb{C}((y^*))$, and
2. $\deg_x(G_i) = 1$ holds for all $i = 1, \ldots, r$.

In our first step, we will allow $\deg_x(G_i) \geq 1$ for all $i = 1, \ldots, r$. Moreover, in practice,

1. we compute a truncated factorization, that is, $G_1(x, y), \ldots, G_r(x, y)$ are polynomials in $\mathbb{C}]x, y]$ (in fact homomogeneous polynomials) and,
2. the relation $F(x, y) = G_1(x, y) \cdots G_r(x, y)$ holds modulo an ideal S_k.

A weak but algrithmic version of Puiseux theorem (2/2)

Hypothesis

We assume that $F^{(0)}(x,y)$ has been factorized as

$$F^{(0)}(x,y) = G_1^{(0)}(x,y) \cdots G_r^{(0)}(x,y)$$

where the polynomials $G_i^{(0)}(x,y)$ are homomogeneous and coprime w.r.t. x (that is, once y is specialized to 1). Of course, a special case is

$$G_i^{(0)}(x,y) = (x - \zeta_i y^{\delta/d})^{m_i}$$

For simplicity, we write $\hat{y} = y^{\hat{\delta}/\hat{d}}$.

Lagrange's Interpolation polynomials (1/4)

Lemma

Let $\hat{G}_i(x, \hat{y}) \in \mathbb{C}[x, \hat{y}]$, for $i = 1, \ldots, r$, be homogeneous polynomials in $(x, \hat{y})$, that we regard in $\mathbb{C}\langle\hat{y}\rangle[x]$, such that

- $r \geq 2$ and $d = \deg_x \left(\hat{G}_1 \cdots \hat{G}_r\right)$,
- $\deg_x \hat{G}_i = m_i$ for $i = 1, \ldots, r$, and
- $\gcd_x(\hat{G}_i, \hat{G}_j) = 1$ for any $i \neq j$.

Then, for each $\ell \in \{0, \ldots, d-1\}$, there exists only one set of polynomials $\{W_i^{(\ell)}(x, \hat{y}) \in \mathbb{C}\langle\hat{y}\rangle[x] \mid i = 1, \ldots, r\}$ satisfying

1. $W_1^{(\ell)}\left(\left(\hat{G}_1 \cdots \hat{G}_r\right)/\hat{G}_1\right) + \cdots + W_r^{(\ell)}\left(\left(\hat{G}_1 \cdots \hat{G}_r\right)/\hat{G}_r\right) = x^\ell \hat{y}^{d-\ell}$,
2. $\deg_x\left(W_i^{(\ell)}(x, \hat{y})\right) < \deg_x\left(\hat{G}_i(x, \hat{y})\right)$, for $i = 1, \ldots, r$.

Moreover, the polynomials $W_i^{(0)}, \ldots, W_i^{(d-1)}$, for $i = 1, \ldots, r$ are homogeneous in $(x, \hat{y})$ of degree m_i. We call them the *Lagrange's interpolation polynomials*.

Lagrange's Interpolation polynomials (2/4)

Proof of the lemma (1/3)

- We shall first prove that there exists only one set of polynomials
$$\{W_i^{(\ell)}(x,1) \mid i = 1,\ldots,r\}$$
satisfying (1) and (2) in the above lemma statement, when $\hat{y} = 1$.
- Using the extended Euclidean algorithm, one can compute $A_1,\ldots,A_s \in \mathbb{C}[x]$ such that
$$A_1\frac{\hat{G}_1\cdots\hat{G}_s}{\hat{G}_1} + \cdots + A_s\frac{\hat{G}_1\cdots\hat{G}_s}{\hat{G}_s} = 1.$$
- If we multiply both sides of the above equality by x^ℓ, then we have
$$A_1x^\ell\frac{\hat{G}_1\cdots\hat{G}_s}{\hat{G}_1} + \cdots + A_sx^\ell\frac{\hat{G}_1\cdots\hat{G}_s}{\hat{G}_s} = x^\ell \quad (\bigstar).$$

Lagrange's Interpolation polynomials (3/4)

Proof of the lemma (2/3)

- For each $i = 1, \ldots, r-1$, let $Q_i, R_i \in \mathbb{C}[x]$ such that
  - $A_i x^\ell = Q_i \hat{G}_i + R_i$ and
  - $\deg_x(R_i) < \deg_x(\hat{G}_i)$
- Thus the equality $(\bigstar)$ can be re-written as:

$$R_1 \frac{\hat{G}_1 \cdots \hat{G}_r}{\hat{G}_1} + \cdots + R_{r-1} \frac{\hat{G}_1 \cdots \hat{G}_r}{\hat{G}_{r-1}} + (A_r x^\ell + \sum_{i=1}^{r-1} Q_i \hat{G}_r) \frac{\hat{G}_1 \cdots \hat{G}_r}{\hat{G}_r} = x^\ell.$$

- Observe that we have
  - $\deg_x(R_i \frac{\hat{G}_1 \cdots \hat{G}_r}{\hat{G}_i}) < d$ for $i = 1, \ldots, r-1$,
  - $\deg_x(\frac{\hat{G}_1 \cdots \hat{G}_r}{\hat{G}_r}) = d - m_r$, and also
  - $\ell < d$.
- Combined with relation $(\bigstar)$, we obtain

$$\deg_x(A_r x^\ell + \sum_{i=1}^{r-1} Q_i \hat{G}_r) < m_r = \deg_x(\hat{G}_r).$$

Lagrange's Interpolation polynomials (4/4)

Proof of the lemma (3/3)

- Hence, we set
  - $W_i^{(\ell)}(x,1) = R_i$, for $i = 1, \ldots, r-1$
  - $W_r^{(\ell)}(x,1) = A_r x^\ell + \sum_{i=1}^{r-1} Q_i \hat{G}_r$
- The proof of the unicity will be added later ...
- Note that we have $\deg(x^\ell \hat{y}^{d-\ell}) = d$.
- Since $\deg_x \left(W_i^{(\ell)}(x,1) \left(\hat{G}_1 \cdots \hat{G}_r \right) / \hat{G}_i \right) < d$, we can homogenize in degree d both $W_i^{(\ell)}(x,1)$ and $\hat{G}_i(x,1)$, for $i = 1, \ldots, r$, using $\hat{y}$ as homogeization variable.
- This homogeization process defines each $W_i^{(\ell)}(x,\hat{y})$ uniquely.
- Moreover we have,

$$\deg_x(W_i^{(\ell)}(x,\hat{y})) < \deg_x(\hat{G}_i),$$

since the homogenization has no effect on degrees in x.

Hensel-Sasaki construction: bivariate case

Theorem

Let $F(x,y) \in \mathbb{C}\langle y \rangle [x]$ be a square-free polynomial, monic in x of degree $d > 0$. Let $F^{(0)}(x,y)$ be the Newton polynomial of $F(x,y)$. Let $G_1^{(0)}(x,y), \ldots, G_r^{(0)}(x,y) \in \mathbb{C}[x,y]$ be homogeneous polynomials in $(x,\hat{y})$, pairwise coprime when $\hat{y} = 1$, such that we have:

$$F^{(0)}(x,y) = G_1^{(0)}(x,y) \cdots G_r^{(0)}(x,y).$$

Recall $S_k = <x^d y^{(k+0)/\hat{d}}, x^{d-1} y^{(k+\hat{\delta})/\hat{d}}, x^{d-2} y^{(k+2\hat{\delta})/\hat{d}}, \ldots, x^0 y^{(k+d\hat{\delta})/\hat{d}}>$ for $k = 1, 2, \ldots$. Then, for any positive integer k, we can construct $G_i^{(k)}(x,y) \in \mathbb{C}\langle y^{1/\hat{d}} \rangle [x]$, for $i = 1, \ldots, r$, satisfying

1. $F(x,y) = G_1^{(k)}(x,y) \cdots G_r^{(k)}(x,y) \mod S_{k+1}$,
2. $G_i^{(k)}(x,y) = G_i^{(0)}(x,y) \mod S_1, \quad i = 1, \ldots, r.$

The proof is by induction on k and constructive.

Proof (1/5)

- **base case:** Since $F(x,y) \equiv F^{(0)}(x,y) \mod S_1$, the theorem is valid for $k = 0$.
- **inductive step:** Let the theorem be valid up to the $(k-1)$-st construction. We write

$$G_i^{(k-1)} = G_i^{(0)}(x,y) + \Delta G_i^{(1)}(x,y) + \cdots + \Delta G_i^{(k-1)}(x,y),$$

such that

  - $G_i^{(k')}(x,y) \in S_{k'}$ for $k' = 1, \ldots, k-1$,
  - $\deg_x(\Delta G_i^{(k')}(x,y)) < \deg_x(G_i^{(0)}(x,y)) = m_i, \quad k' = 1, \ldots, k-1.$

These latter properties are part of the induction hypothesis.

Note: Each $\Delta G_i^{(k')}(x,y)$ is being computed in the k'-th Hensel construction step. So the degree in x does not increase contrary to the degree in y, because of the definition of S_k.

Proof (2/5)

We define:

$$\Delta F^{(k)}(x,y) := F(x,y) - G_1^{(k-1)} \cdots G_r^{(k-1)} \mod S_{k+1}.$$

According to the format of monomials of $F(x,y)$ (Lemma in page 8) and also induction assumptions, we have

$$\Delta F^{(k)}(x,y) = f_{d-1}^{(k)} x^{d-1} y^{\hat{\delta}/\hat{d}} + \cdots + f_0^{(k)} x^0 y^{d\hat{\delta}/\hat{d}}$$
$$f_\ell^{(k)} = c_\ell^{(k)} y^{k/\hat{d}},\ c_\ell^{(k)} \in \mathbb{C} \quad \text{for } \ell = 0, \ldots, d-1$$

Proof (3/5)

We construct $G_i^{(k)}(x,y)$ by observing that we have:

$$G_i^{(k)}(x,y) = G_i^{(k-1)}(x,y) + \Delta G_i^{(k)}(x,y), \quad \Delta G_i^{(k)}(x,y) \equiv 0 \mod S_k$$

Then we have:

$$\begin{aligned}
F(x,y) &\equiv \left(G_1^{(k-1)} + \Delta G_1^{(k)}\right) \cdots \left(G_r^{(k-1)} + \Delta G_r^{(k)}\right) \mod S_{k+1} \\
&\equiv G_1^{(k-1)} \cdots G_r^{(k-1)} + \Delta G_1^{(k)} (G_2 \cdots G_r) + \cdots + \Delta G_r^{(k)} (G_1 \cdots G_{r-1}) + \\
&\qquad \underbrace{\text{other terms}} \qquad \mod S_{k+1} \\
&\qquad \text{containg } \Delta G_i^{(k)}(x,y) \text{ and } \Delta G_j^{(k)}(x,y) \\
&\equiv G_1^{(k-1)} \cdots G_r^{(k-1)} + \Delta G_1^{(k)} (G_2 \cdots G_r) + \cdots + \Delta G_r^{(k)} (G_1 \cdots G_{r-1}) \mod S_{k+1} \\
&\equiv G_1^{(k-1)} \cdots G_r^{(k-1)} + \Delta G_1^{(k)} \left(G_2^{(0)} \cdots G_r^{(0)}\right) + \cdots + \Delta G_r^{(k)} \left(G_1^{(0)} \cdots G_{r-1}^{(0)}\right) \mod S_{k+1}
\end{aligned}$$

Proof (4/5)

The last two equivalence relations are valid, since

$$\Delta G_i^{(k)}(x,y)\Delta G_j^{(k')}(x,y) \equiv 0 \mod S_{k+1} \quad \text{for } k' = 1,\ldots,k.$$

It actually follows from the fact that by assumption,

- $\Delta G_j^{(k)} \equiv 0 \mod S_k$
- $\Delta G_j^{(k')} \equiv 0 \mod S_{k'}$ for $k' = 1,\ldots,k$

Thus,

$$\Delta G_j^{(k)}\Delta G_j^{(k')} \equiv 0 \mod S_k S_{k'}$$

Since, $S_k S_{k'} = S_{k+k'}$ then

$$\Delta G_j^{(k)}\Delta G_j^{(k')} \equiv 0 \mod S_{k+k'} \quad \text{for } k' = 1,\ldots,k$$

Furthermore, since $k' \geq 1$, then

$$\Delta G_j^{(k)}\Delta G_j^{(k')} \equiv 0 \mod S_{k+1} \quad \text{for } k' = 1,\ldots,k$$

Proof (5/5)

Therefore,

$$\Delta F^{(k)} \equiv \Delta G_1^{(k)} \left(G_2^{(0)} \cdots G_r^{(0)} \right) + \cdots + \Delta G_r^{(k)} \left(G_1^{(0)} \cdots G_{r-1}^{(0)} \right) \mod S_{k+1}$$

If in the lemma of Lagrange Interpolation polynomial we let $\hat{G}_i(x, \hat{y}) = G_i^{(0)}(x, \hat{y})$, using the other representation of $\Delta F^{(k)}(x, y)$, it allows us to solve the last equation (the equation above) as

$$\begin{aligned} \sum_{i=1}^{r} \Delta G_i^{(k)}(x, y) \frac{\left(G_1^{(0)} \cdots G_r^{(0)} \right)}{G_i^{(0)}} &= \sum_{\ell=0}^{d-1} f_\ell^{(k)} x^\ell \hat{y}^{d-\ell} \\ &= \sum_{\ell=0}^{d-1} f_\ell^{(k)} \left(\sum_{i=1}^{r} W_i^{(\ell)} \frac{\left(G_1^{(0)} \cdots G_r^{(0)} \right)}{G_i^{(0)}} \right) \\ &= \sum_{i=1}^{r} \left(\sum_{\ell=0}^{d-1} f_\ell^{(k)} W_i^{(\ell)} \right) \frac{\left(G_1^{(0)} \cdots G_r^{(0)} \right)}{G_i^{(0)}} \end{aligned}$$

Since $\deg_x(f_\ell^{(k)} W_i^{(\ell)}) < \deg_x(G_i^{(0)})$ and $\deg_x(\Delta G_i^{(k)}(x, y)) < \deg_x(G_i^{(0)})$ for $i = 1, \ldots, r$, then we have

$$\Delta G_i^{(k)}(x, y) = \sum_{\ell=0}^{d-1} W_i^{(\ell)}(x, y) f_\ell^{(k)}(y) \quad i = 1, \ldots, r$$

About the theorem

Remarks

- The proof of the theorem constructs the $G_i^{(k)}(x, y)$ uniquely.
- The theorem holds in particular for the case where the case where $G_i^{(0)}(x, y) = (x - \zeta_i y^{\hat{\delta}/\hat{d}})^{m_i}$ holds for each $i = 1, \ldots, r$.
- However, the theorem is more generral and only requires that the $G_i^{(0)}(x, y)$ are homogeneous polynomials in $(x, \hat{y})$, pairwise coprime when $\hat{y} = 1$.
- And, in fact each factor $G_i^{(0)}(x, y)$ of the Newton polynomial are necessarily a product of some of the $(x - \zeta_i y^{\hat{\delta}/\hat{d}})$ and thus each factor $G_i^{(0)}(x, y)$ is homogeneous in $(x, \hat{y})$.

Proposition

If the initial factors $G_i^{(0)}(x, y)$ are in fact polynomials in $\mathbb{C}[x, y]$, then, after the k-th lifting step, the computed factors $G_i^{(k)}(x, y)$ are themselves polynomials in $\mathbb{C}[x, y]$.

The proof of this proposition follows by tracking the calculations of the lemma and the theorem.

Algorithm 1: EHC_Lift(F, k)

begin

Compute the Newton polynomial $F^{(0)}$ and $\hat{\delta}, \hat{d}$;

Compute $G_i^{(0)} = (X - \zeta_i Y)^{m_i}$, with $1 \leq i \leq r$;

Compute the Yun-Moses polynomial $W_i^{(\ell)}$ for $i = 1, \cdots, r$ and $\ell = 0, \ldots, d-1$;

for $j = 1, \ldots, k$ **do**

Compute $\Delta F^{(j)}(X, Y) := F(X, Y) - \prod_{i=1}^{r} G_i^{(j-1)} \mod \bar{S}_{j+1}$;

Compute $\Delta G_i^{(j)} = \sum_{\ell=0}^{m-1} W_i^{(\ell)} f_\ell^{(j)}$, for $i = 1, \cdots, r$;

Let $G_i^{(j)} = G_i^{(j-1)} + \Delta G_i^{(j)}$ for $i = 1, \cdots, r$;

return $G_1^{(k)}, \ldots, G_r^{(k)}$;

Algorithm 2: EHC_Lift(F, k)

begin

Compute the Newton polynomial $F^{(0)}$ and $\hat{\delta}, \hat{d}$;

Compute $G_i^{(0)} = (X - \zeta_i Y)^{m_i}$, with $1 \leq i \leq r$;

Compute the Yun-Moses polynomial $W_i^{(\ell)}$ for $i = 1, \cdots, r$ and $\ell = 0, \cdots, d-1$;

for $j = 1, \ldots, k$ **do**

Compute

$\Delta F^{(j)}(X,Y) := F(X,Y) - \prod_{i=1}^{r} G_i^{(j-1)} \mod \bar{S}_{j+1}$;

Compute $\Delta G_i^{(j)} = \sum_{\ell=0}^{m-1} W_i^{(\ell)} f_\ell^{(j)}$, for $i = 1, \cdots, r$;

Let $G_i^{(j)} = G_i^{(j-1)} + \Delta G_i^{(j)}$ for $i = 1, \cdots, r$;

return $G_1^{(k)}, \ldots, G_r^{(k)}$;

Algorithm 3: EHC_LiftF, k

begin

Compute the Newton polynomial $F^{(0)}$ and $\hat{\delta}, \hat{d}$;

Compute $G_i^{(0)} = (X - \zeta_i Y)^{m_i}$, with $1 \leq i \leq r$;

Compute the Yun-Moses polynomial $W_i^{(\ell)}$ for $i = 1, \cdots, r$ and $\ell = 0, \cdots, d-1$;

for $j = 1, \ldots, k$ **do**

Compute $\Delta F^{(j)}(X, Y) := F(X, Y) - \prod_{i=1}^{r} G_i^{(j-1)} \mod \bar{S}_{j+1}$;

Compute $\Delta G_i^{(j)} = \sum_{\ell=0}^{m-1} W_i^{(\ell)} f_\ell^{(j)}$, for $i = 1, \cdots, r$;

Let $G_i^{(j)} = G_i^{(j-1)} + \Delta G_i^{(j)}$ for $i = 1, \cdots, r$;

return $G_1^{(k)}, \ldots, G_r^{(k)}$;

Example of Extended Hensel Construction

Consider

$$F(x,y) = x^5 + x^4\,y - 2\,x^3\,y - 2\,x^2\,y^2 + x\,(y^2 - y^3) + y^3. \qquad (1)$$

Then, we have

- $d = \deg_x(F(x,y)) = 5$,
- Newton line: $e_x/5 + e_y/2.5 = 1$
- $\delta/d = 1/2 = \hat{\delta}/\hat{d}$
- $S_0 = <x^5, x^4\,y^{1/2}, x^3\,y, x^2\,y^{3/2}, x\,y^2, y^{5/2}>$
- $F^{(0)}(x,y) = x^5 - 2\,x^3\,y + x\,y^2 = x\,(x + y^{1/2})^2\,(x - y^{1/2})^2$

Note that

$$F^{(0)}(x,1) = x\,(x+1)^2\,(x-1)^2 \qquad (2)$$

Example of Extended Hensel Construction

Hence, we can put

$$G_1^{(0)} = x, G_2^{(0)} = (x + y^{1/2})^2, G_3^{(0)} = (x - y^{1/2})^2.$$

Yun-Moses polynomials are calculated as,

$$\begin{array}{lll}
W_1^{(0)} = y^{1/2} & W_2^{(0)} = -\frac{1}{2}x\,y^{1/2} - \frac{3}{4}y & W_3^{(0)} = -\frac{1}{2}xy^{1/2} + \frac{3}{4}y \\
W_1^{(1)} = 0 & W_2^{(1)} = \frac{1}{4}x\,y^{1/2} + \frac{1}{2}y & W_3^{(1)} = -\frac{1}{4}x\,y^{1/2} + \frac{1}{2}y \\
W_1^{(2)} = 0 & W_2^{(2)} = -\frac{1}{4}y & W_3^{(2)} = \frac{1}{4}y \\
W_1^{(3)} = 0 & W_2^{(3)} = -\frac{1}{4}x\,y^{1/2} & W_3^{(3)} = \frac{1}{4}x\,y^{1/2} \\
W_1^{(4)} = 0 & W_2^{(4)} = \frac{1}{2}x\,y^{1/2} + \frac{1}{4}y & W_3^{(4)} = \frac{1}{2}x\,y^{1/2} - \frac{1}{4}y
\end{array}$$

Example of Extended Hensel Construction

For

$$S_2 = <x^5\, y, x^4 y^{3/2}, x^3 y^2, x^2 y^{5/2}, x y^3, y^{7/2}>$$

We have,

$$\begin{aligned} \Delta F^{(1)} &\equiv F - G_1^{(0)} G_2^{(0)} G_3^{(0)} \mod S_2 \\ &= x^4 y - 2x^2 y^2 - x y^3 + y^3 \\ &= y^{1/2} \cdot x^4 y^{1/2} - 2 y^{1/2} \cdot x^2 y^{3/2} + y^{1/2} y^{5/2} \end{aligned}$$

The last representation of $\Delta F^{(1)}$ in the last equation is for the purpose of computing $f_\ell^{(1)}$ for $\ell = 0, \ldots, d-1$ in

$$\Delta F^{(k)} = \sum_{\ell=0}^{5-1} f_\ell^{(k)} \hat{y}^{d-\ell} x^\ell \quad \text{when } k = 1$$

Example of Extended Hensel Construction

Therefore,

$$f_4^{(1)} = y^{1/2}, f_2^{(1)} = -2y^{1/2}, f_0^{(1)} = y^{1/2}, f_3^{(1)} = f_1^{(1)} = 0$$

Considering the above polynomials and also the Lagrange's interpolation polynomials, we obtain:

- $G_1^{(1)} = G_1^{(0)} + W_1^{(0)} f_0^{(1)} = x + y$
- $G_2^{(1)} = G_2^{(0)} + W_2^{(4)} f_4^{(1)} + W_2^{(0)} f_0^{(1)} + W_2^{(2)} f_2^{(1)} = (x + y^{1/2})^2$
- $G_3^{(1)} = G_3^{(0)} + W_3^{(4)} f_4^{(1)} + W_3^{(0)} f_0^{(1)} + W_3^{(2)} f_2^{(1)} = (x - y^{1/2})^2$

Example of Extended Hensel Construction

Now for $S_3 = <x^5y^{3/2}, x^4y^2, x^3y^{5/2}, x^2y^3, xy^{7/2}, y^4>$, we have

$$\begin{aligned} \Delta F^{(2)} &\equiv F - G_1^{(1)} G_2^{(1)} G_3^{(1)} \mod S_3 \\ &= -y \cdot xy^2 \end{aligned} .$$

Hence,

$$f_1^{(2)} = -y, f_0^{(2)} = f_2^{(2)} = f_3^{(2)} = f_4^{(2)} = 0.$$

And then we obtain,

- $G_1^{(2)} = G_1^{(1)} + 0 = x + y$
- $G_2^{(2)} = G_2^{(1)} + W_2^{(1)} f_1^{(2)} = (x + y^{1/2})^2 - (\frac{1}{4} x\, y^{3/2} + \frac{1}{2} y^2)$
- $G_3^{(2)} = G_3^{(1)} + W_3^{(1)} f_1^{(2)} = (x - y^{1/2})^2 + (\frac{1}{4} x\, y^{3/2} - \frac{1}{2} y^2)$

Example of Extended Hensel Construction

Continuing two more iterations, we have

- $G_1^{(4)} = x + y + y^2$
- $G_2^{(4)} = (x + y^{\frac{1}{2}})^2 - (\frac{1}{4}x\,y^{\frac{3}{2}} + \frac{1}{2}y^2) - (\frac{1}{2}xy^2 + \frac{3}{4}y^{\frac{5}{2}}) - (\frac{53}{64}xy^{\frac{5}{2}} + \frac{9}{8}y^3)$
- $G_3^{(4)} = (x - y^{\frac{1}{2}})^2 + (\frac{1}{4}x\,y^{\frac{3}{2}} - \frac{1}{2}y^2) - (\frac{1}{2}xy^2 + \frac{3}{4}y^{\frac{5}{2}}) + (\frac{53}{64}xy^{\frac{5}{2}} - \frac{9}{8}y^3)$

We note that $G_2^{(4)}$ and $G_3^{(4)}$ can be written as:

- $G_2^{(4)} = G_P^{(4)} + y^{1/2}G_A^{(4)}$
- $G_3^{(4)} = G_P^{(4)} - y^{1/2}G_A^{(4)}$

where

- $G_P^{(4)} = x^2 + y - \frac{1}{2}y^2 - \frac{1}{2}x\,y^2 - \frac{9}{8}y^3$
- $G_A^{(4)} = 2x - \frac{1}{4}x\,y - \frac{3}{4}y^2 - \frac{53}{64}xy^2$

Note: $G_1^{(\infty)} \in \mathbb{C}[x, y]$, since $F^{(0)}(x, y) = x(x^4 - 2x^2y + y^2)$

Yun-Moses Polynomials (1/3)

Assume $G_1(X,Y),\ldots,G_r(X,Y)$ are homogeneous polynomials. Regarding them as polynomials of $\mathbb{C}\langle Y\rangle[X]$, further assume

$$\gcd\left(\hat{G}_i,\hat{G}_j\right)=1 \text{ for } i\neq j,$$

Let $d:=\deg(G_1(X,Y)\ \ldots\ G_r(X,Y))$. Then, for each $\ell\in\{0,\ldots,d-1\}$, there exists a unique set of polynomials $\{W_i^{(\ell)}(X,Y)\in\mathbb{C}\langle Y\rangle[X]\mid i=1,\ldots,r\}$ satisfying

$$W_1^{(\ell)}\left(\frac{G_1\cdots G_r}{G_1}\right)+\cdots+W_r^{(\ell)}\left(\frac{G_1\cdots G_r}{G_r}\right)=X^\ell Y^{d-\ell},$$

where $\deg_X\left(W_i^{(\ell)}(X,Y)\right)<\deg_X\left(G_i(X,Y)\right),\quad i=1,\ldots,r.$

Yun-Moses Polynomials (2/3)

Key observation

Let us fix $i := \lambda$. Writing $W_\lambda^{(\ell)} = \sum_{j=0}^{m_\lambda - 1} w_{\lambda,j}(\hat{Y}) X^j$, we have

$$\sum_{j=0}^{m_\lambda - 1} \frac{\partial^\mu}{\partial X^\mu} \left(X^j \frac{F^{(0)}}{G_\lambda^{(0)}} \right) \Big|_{X=\zeta_\lambda \hat{Y}} w_{\lambda,j}^{(\ell)} = \frac{\partial^\mu}{\partial X^\mu} (X^\ell \hat{Y}^{d-\ell}) \Big|_{X=\zeta_\lambda \hat{Y}} .$$

where ζ_λ is a root of $F^{(0)}(X, 1)$ and m_λ is its multiplicity

Consequences

- This is a system of linear equations $\mathcal{W}_\lambda \mathcal{X}_\lambda^{(\ell)} = \mathcal{B}_\lambda^{(\ell)}$.
- The matrix $\mathcal{W}_\lambda$ is a Wronskian matrix.

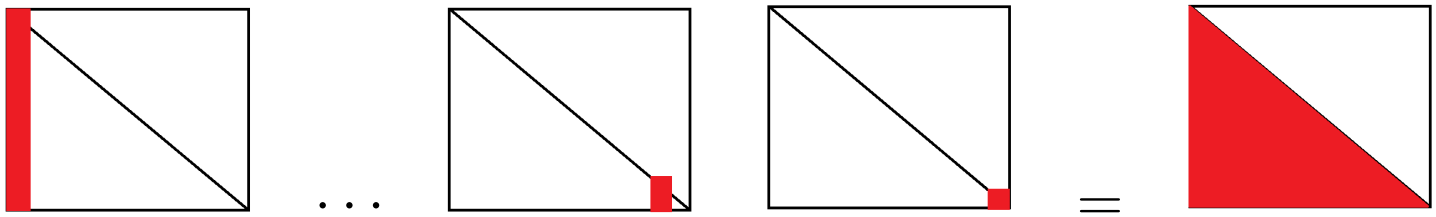
Yun-Moses Polynomials (3/3)

The inverse of $\mathcal{W}_\lambda$ is $\mathcal{W}_\lambda^{-1} = M_2 M_1$ where M_1 and M_2 are square matrices of order m_λ, defined as follows. The matrix M_1 writes $M_1 = M_{1(m_\lambda-1)} \cdots M_{11} M_{10}$ such that, for $j = 0, \cdots, m_\lambda - 1$, we have

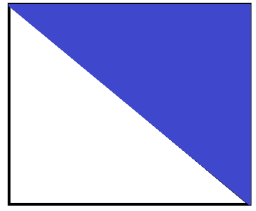
$$M_{1j} = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \frac{1}{j!f} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \binom{j+1}{j}\frac{-f'}{f} & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \binom{m_\lambda-1}{j}\frac{-f^{(m_\lambda-1-j)}}{f} & 0 & \cdots & 1 \end{bmatrix}.$$

Hence, the matrix M_{1j} differs from the identity matrix only in its $(j+1)$-th column. The matrix M_2 is an upper triangular matrix $M_2 = [\gamma_{j,k}]$ with $\gamma_{j,k} = (-1)^{j+k}\binom{k}{k-j}\zeta_\lambda^{k-j}\hat{Y}^{k-j}$ if $j \leq k$ and $\gamma_{j,k} = 0$ if $j > k$, for $j, k \in \{0, 1, \ldots, m_\lambda - 1\}$.

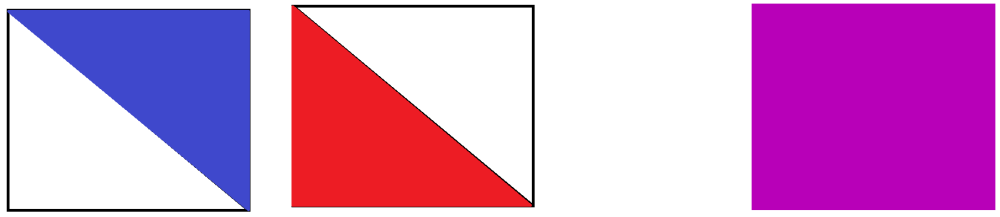
Matrix M_1



Matrix M_2



Matrix $\mathcal{W}_i^{-1} = M_2 M_1$



Complexity Result:

Theorem 1:

One can compute all the Yun-Moses polynomials $W_i^{(\ell)}$ $(0 \leq \ell \leq d-1,$ $1 \leq i \leq r)$, within

- $\mathcal{O}(d^3)$ operations in $\mathbb{C}$, or
- $\mathcal{O}(d^3\,\mathsf{M}(d))$ operations in the field of coefficients of $F(X,Y)$.

Algorithm 4: EHC_LiftF, k

begin

Compute the Newton polynomial $F^{(0)}$ and $\hat{\delta}, \hat{d}$;

Compute $G_i^{(0)} = (X - \zeta_i Y)^{m_i}$, with $1 \leq i \leq r$;

Compute the Yun-Moses polynomial $W_i^{(\ell)}$ for $i = 1, \cdots, r$ and $\ell = 0, \cdots, d-1$;

for $j = 1, \ldots, k$ **do**

Compute

$\Delta F^{(j)}(X,Y) := F(X,Y) - \prod_{i=1}^{r} G_i^{(j-1)} \mod \bar{S}_{j+1}$;

Compute $\Delta G_i^{(j)} = \sum_{\ell=0}^{m-1} W_i^{(\ell)} f_\ell^{(j)}$, for $i = 1, \cdots, r$;

Let $G_i^{(j)} = G_i^{(j-1)} + \Delta G_i^{(j)}$ for $i = 1, \cdots, r$;

return $G_1^{(k)}, \ldots, G_r^{(k)}$;

Computing $\Delta F^{(j)}(X,Y)$

Goal

$$\Delta F^{(j)}(X,Y) := F(X,Y) - \prod_{i=1}^{r} G_i^{(j-1)} \mod \bar{S}_{j+1}$$

Oobservation

- $G_i^{(j-2)} := G_i^{(0)} + \Delta G_i^{(1)} + \cdots + \Delta G_i^{(j-2)}$
- $G_i^{(j-1)} := G_i^{(0)} + \Delta G_i^{(1)} + \cdots + \Delta G_i^{(j-2)} + \Delta G_i^{(j-1)}$

Hence, we aim at recycling terms in the product $\prod_{i=1}^{r} G_i^{(j-1)} \mod \bar{S}_{j+1}$ computed from previous iterations.

Notations

1. $P_2^{k+1} := \prod_{i=1}^{2} G_i^{(k)} \mod \overline{S}_{k+1}$
2. $P_j^{k+1} := \prod_{i=1}^{j} G_i^{(k)} \mod \overline{S}_{k+1}$, for $j = 3, \ldots, r$.

We want

$$P_r^{k+1} = \prod_{i=1}^{r} G_i^{(k)} \mod \overline{S}_{k+2}$$

Computing $\Delta F^{(j)}(X,Y)$

Initially define: $P_j^1 \equiv G_1^{(0)} \cdots G_j^{(0)} \mod S_2$, for $j = 2, \cdots, r$. and recursively compute:

$$P_2^{k+1} = P_2^k + (\Delta_1^0 \Delta_2^k + \Delta_1^k \Delta_2^0)\tilde{Y}^k + (\Delta_1^1 \Delta_2^k + \cdots + \Delta_1^k \Delta_2^1)\tilde{Y}^{k+1} = \prod_{i=1}^{2} G_i^{(k)}$$

Now for $j = 3, \ldots, r$, define

$$P_j^k \equiv P_{j-1}^k G_j^{(k-1)} \mod S_{k+1}$$

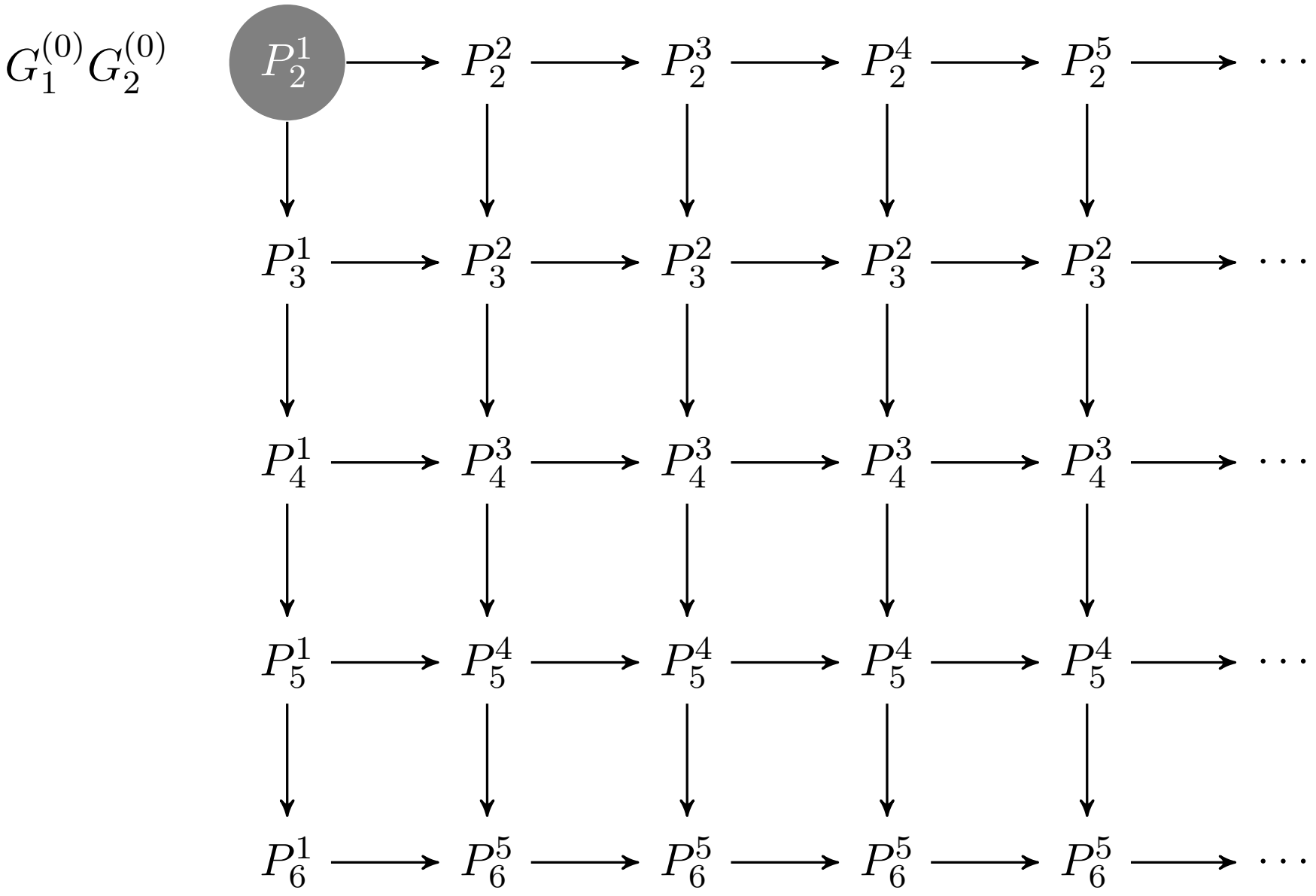
and assume q_j^{k+1} is recursively given by

$$q_j^{k+1} = p_{j-1}^{k+1,0} \Delta_j^k + q_{j-1}^{k+1} \Delta_j^0 \text{ with } q_2^{k+1} = \Delta_2^k \Delta_1^0 + \Delta_2^0 \Delta_1^k. \quad (3)$$

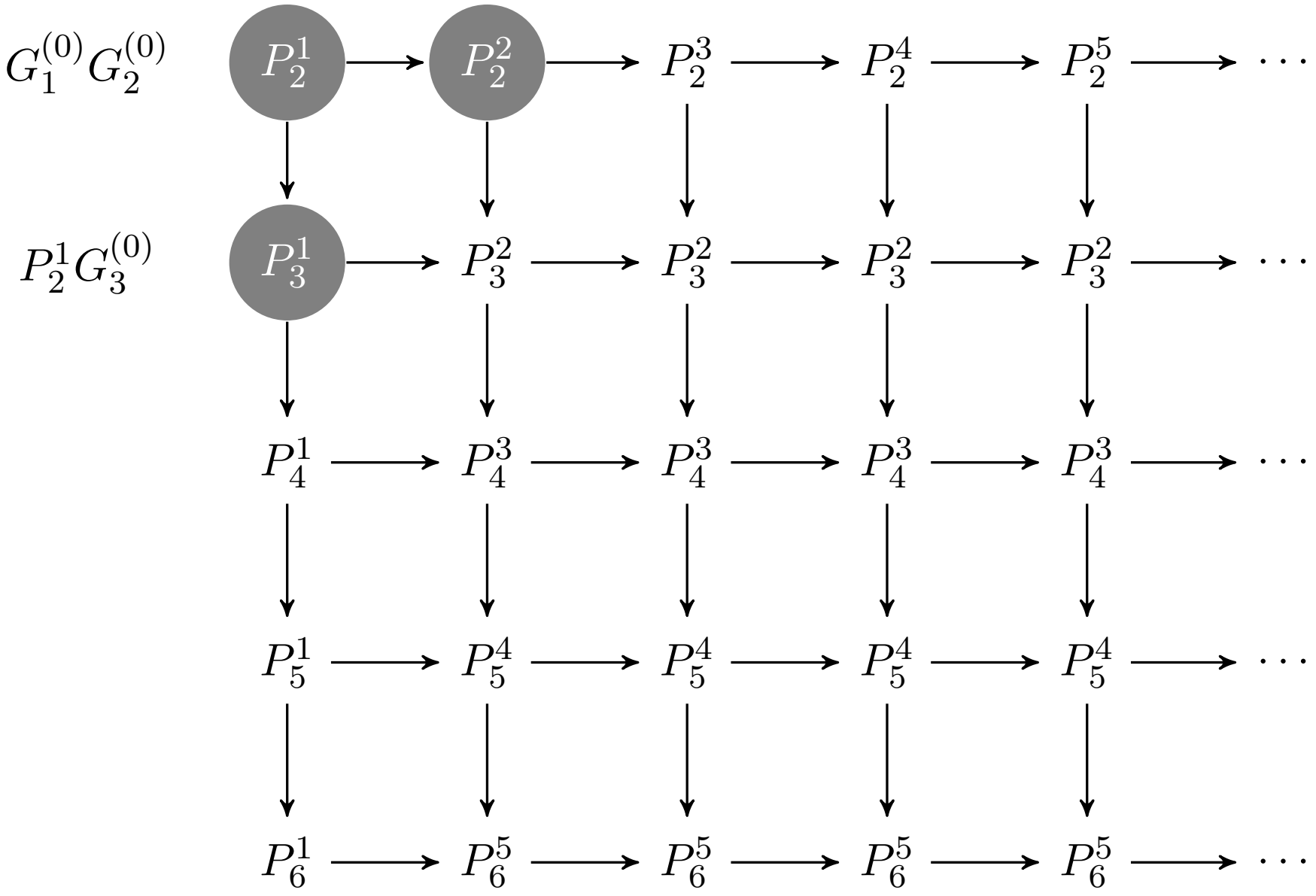
where $p_{j-1}^{k+1,0}$ is the coefficient of $\tilde{Y}^0$ in P_{j-1}^{k+1}. We can compute

$$P_j^{k+1} = P_j^k + q_j^{k+1}\tilde{Y}^k + \left(p_{j-1}^{k+1,1}\Delta_j^k + \cdots + p_{j-1}^{k+1,k+1}\Delta_j^0\right)\tilde{Y}^{k+1} = \prod_{i=1}^{j} G_i^{(k)}$$

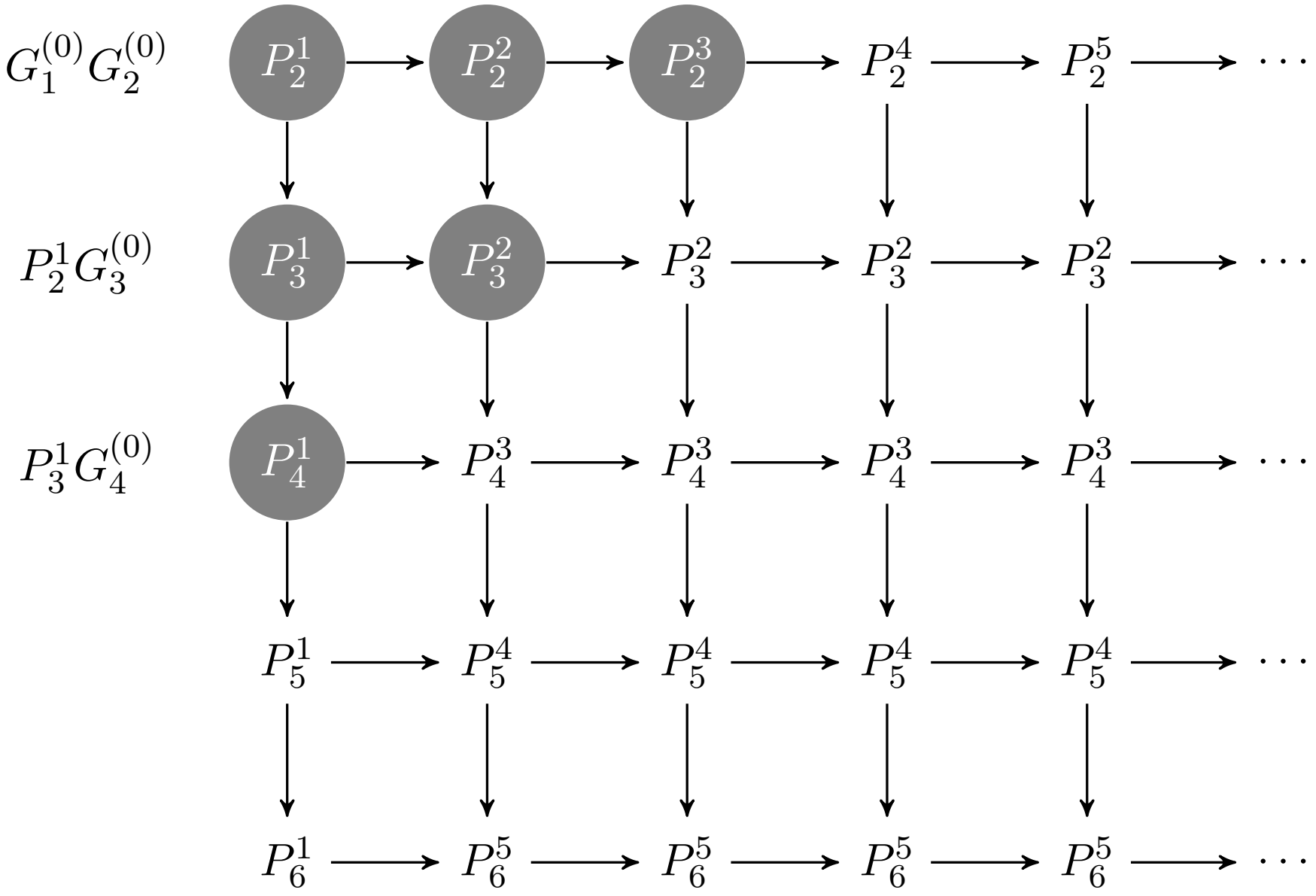
Computing $\Delta F^{(j)}(X, Y)$



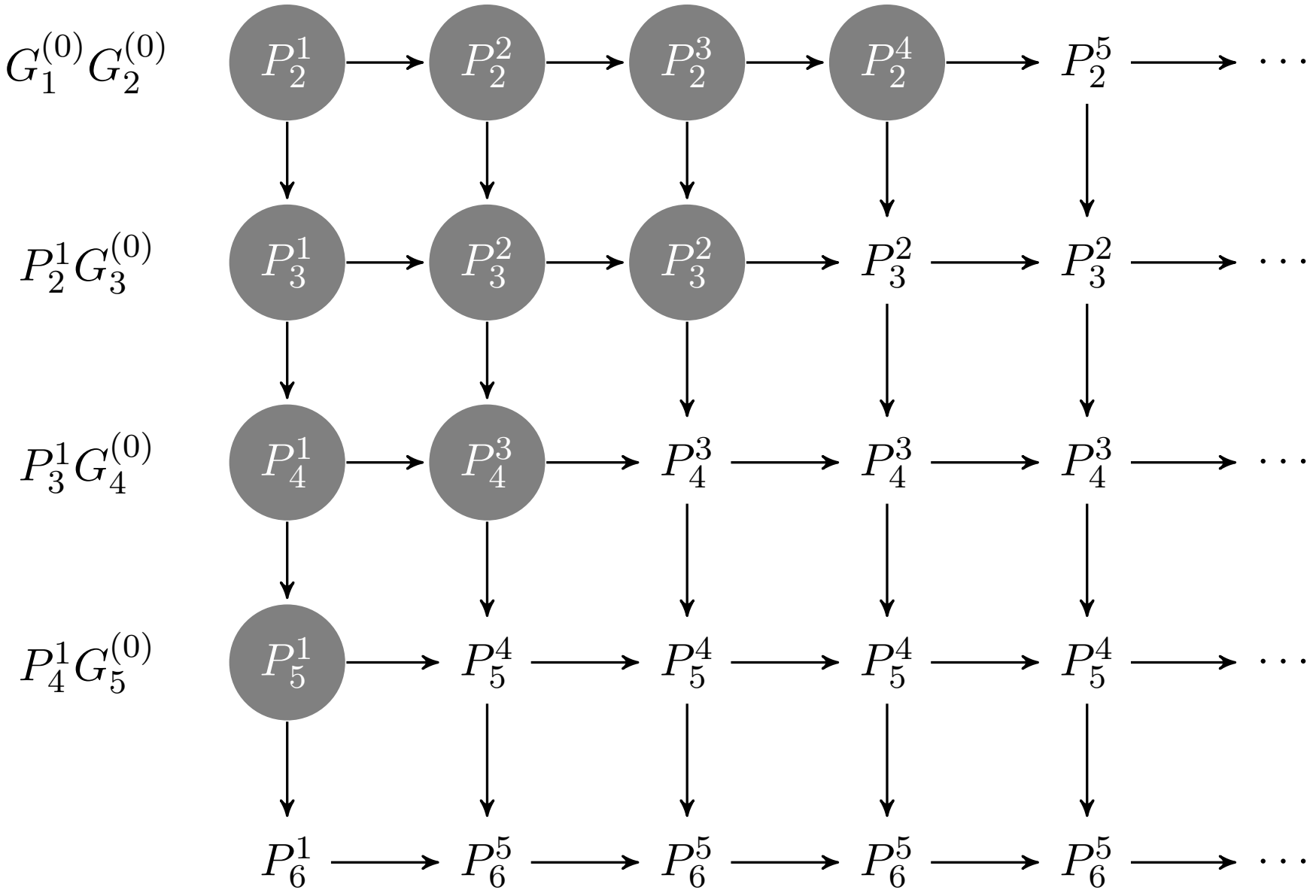
Computing $\Delta F^{(j)}(X, Y)$



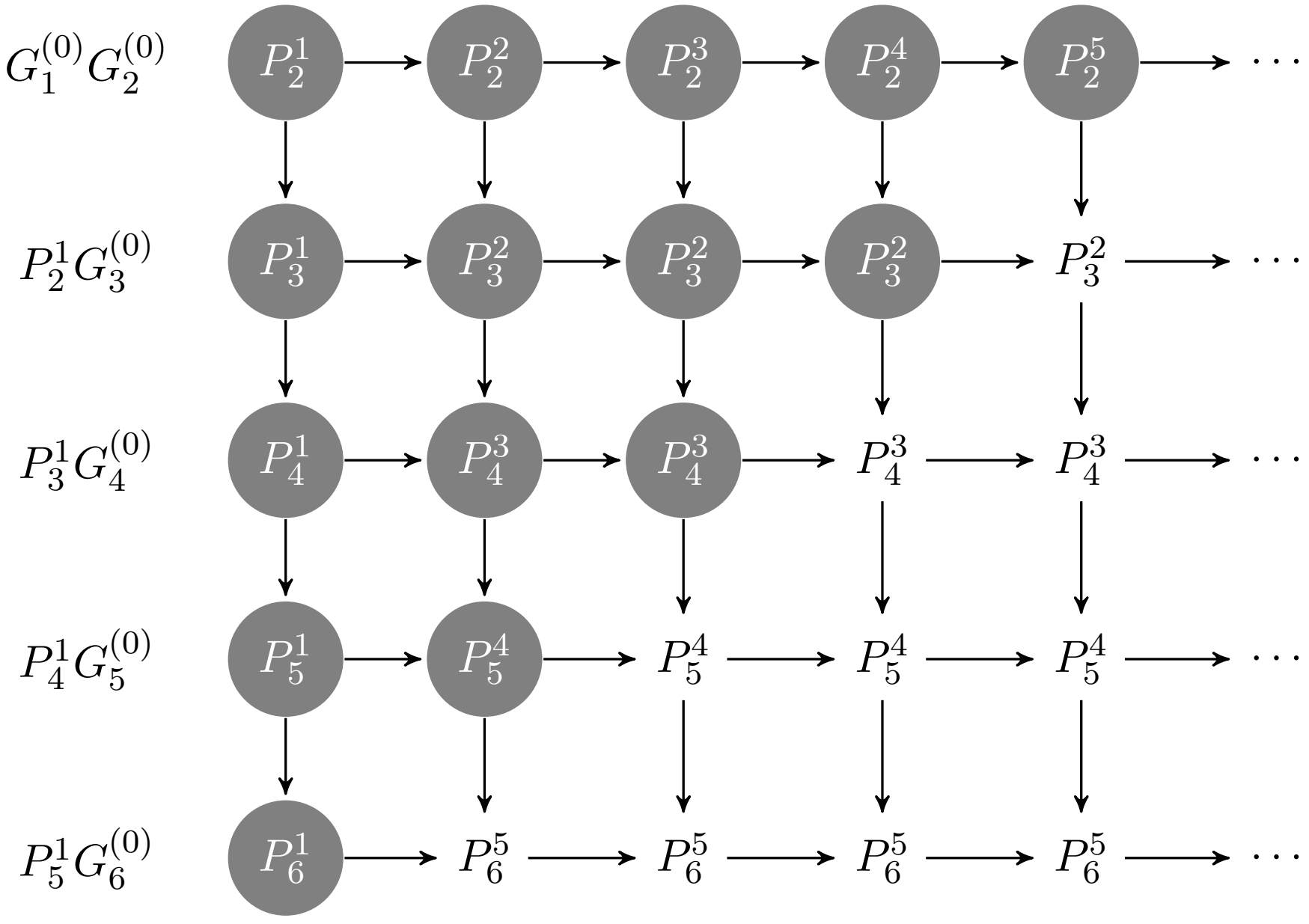
Computing $\Delta F^{(j)}(X, Y)$



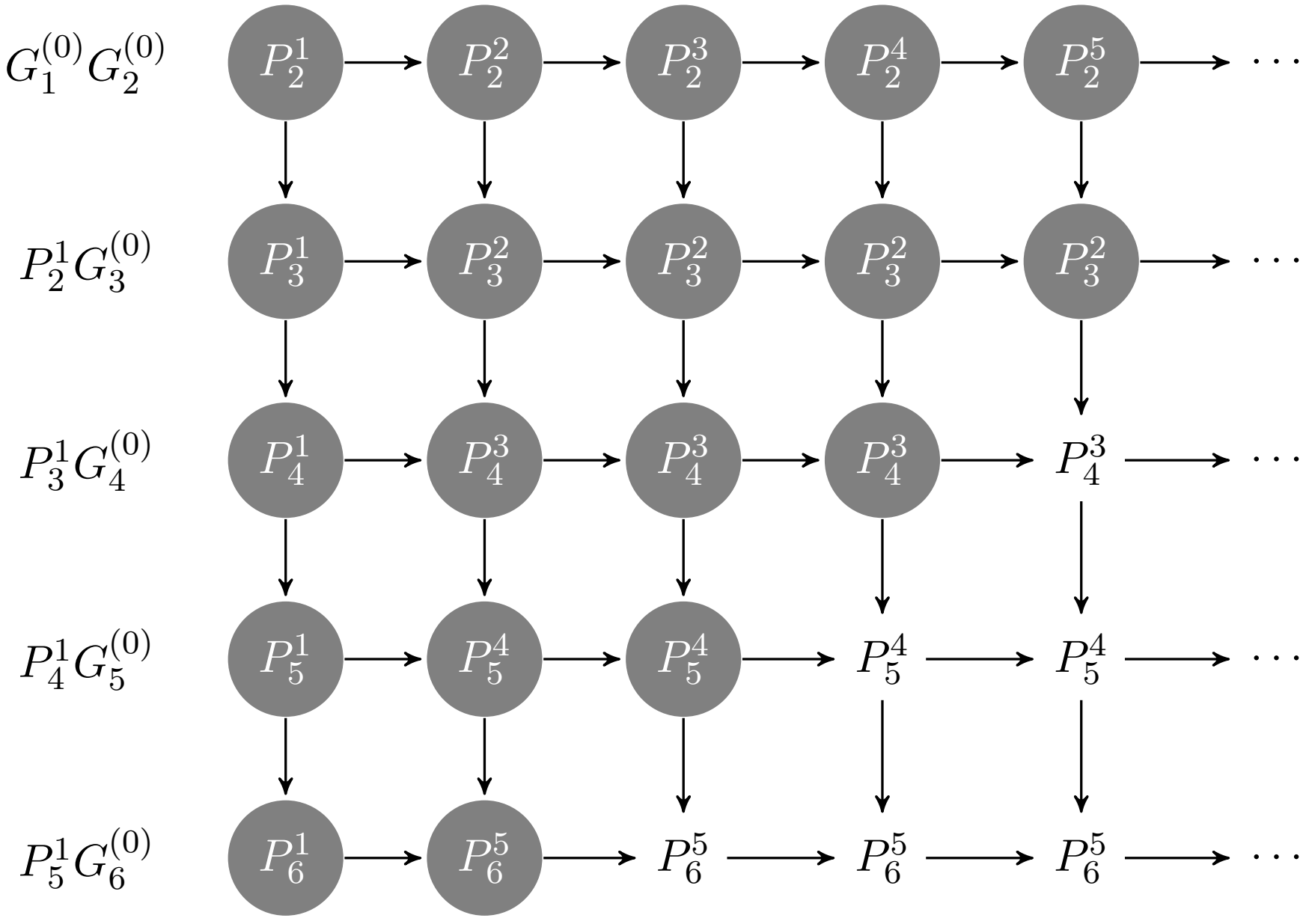
Computing $\Delta F^{(j)}(X, Y)$



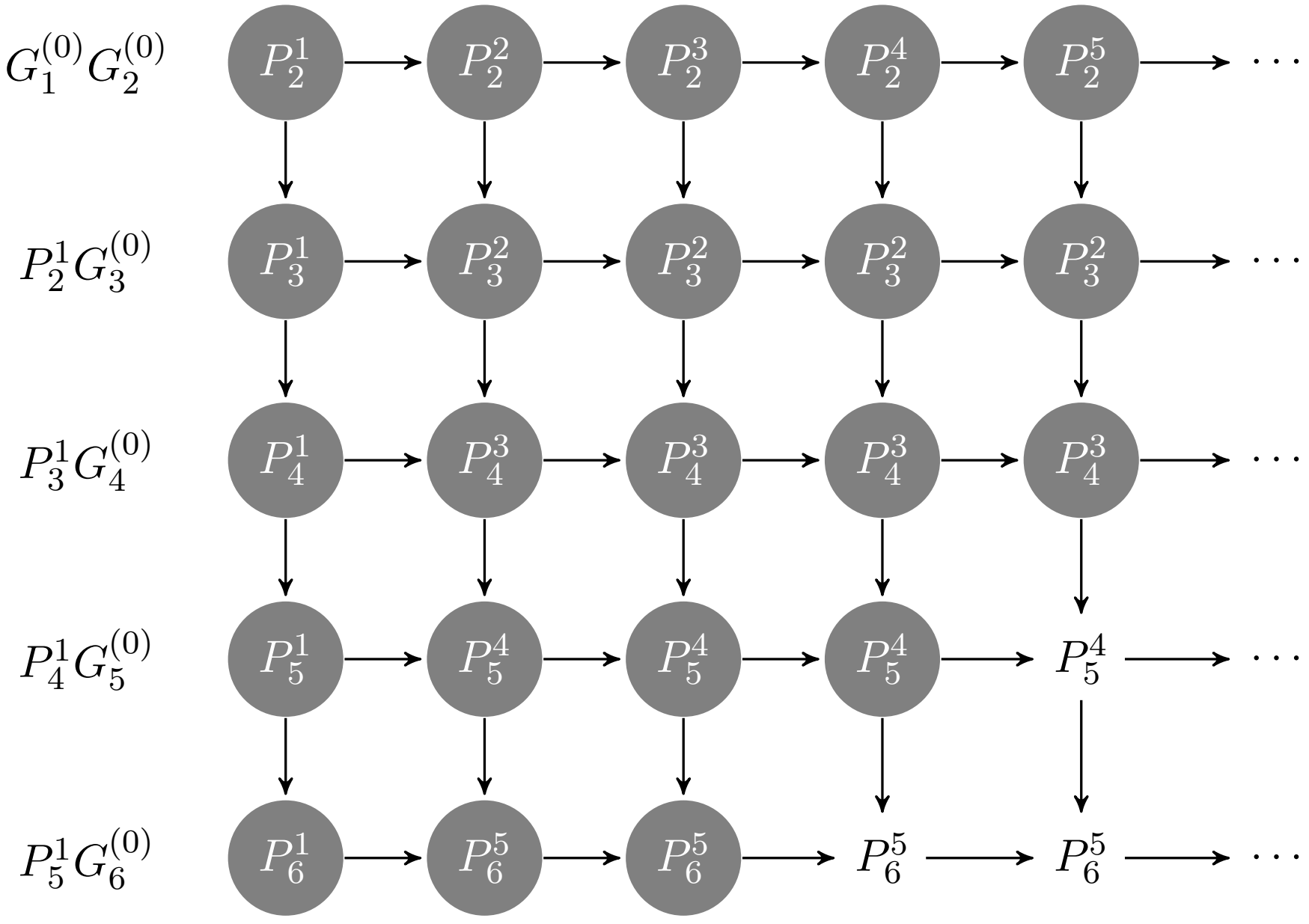
Computing $\Delta F^{(j)}(X, Y)$



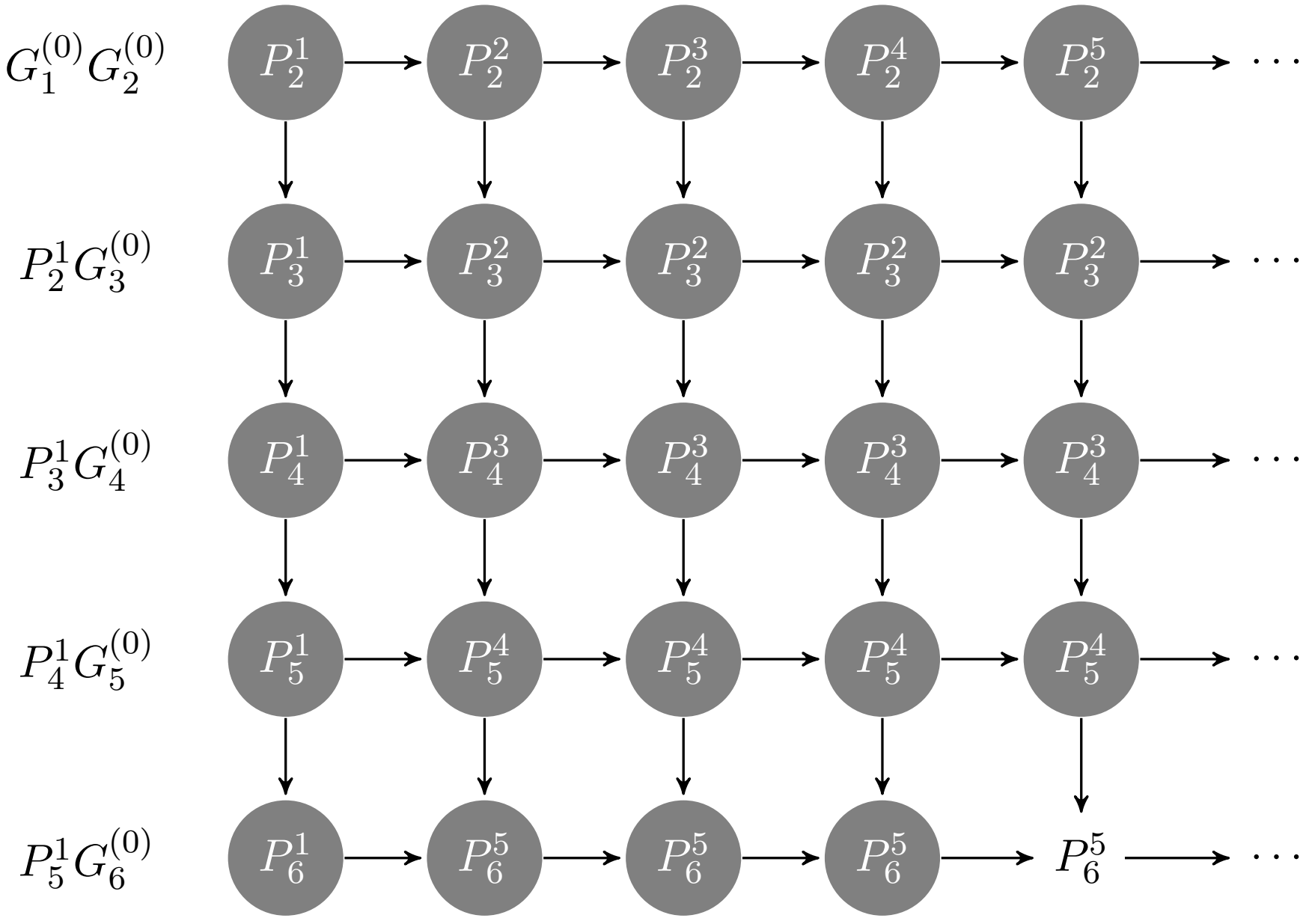
Computing $\Delta F^{(j)}(X, Y)$



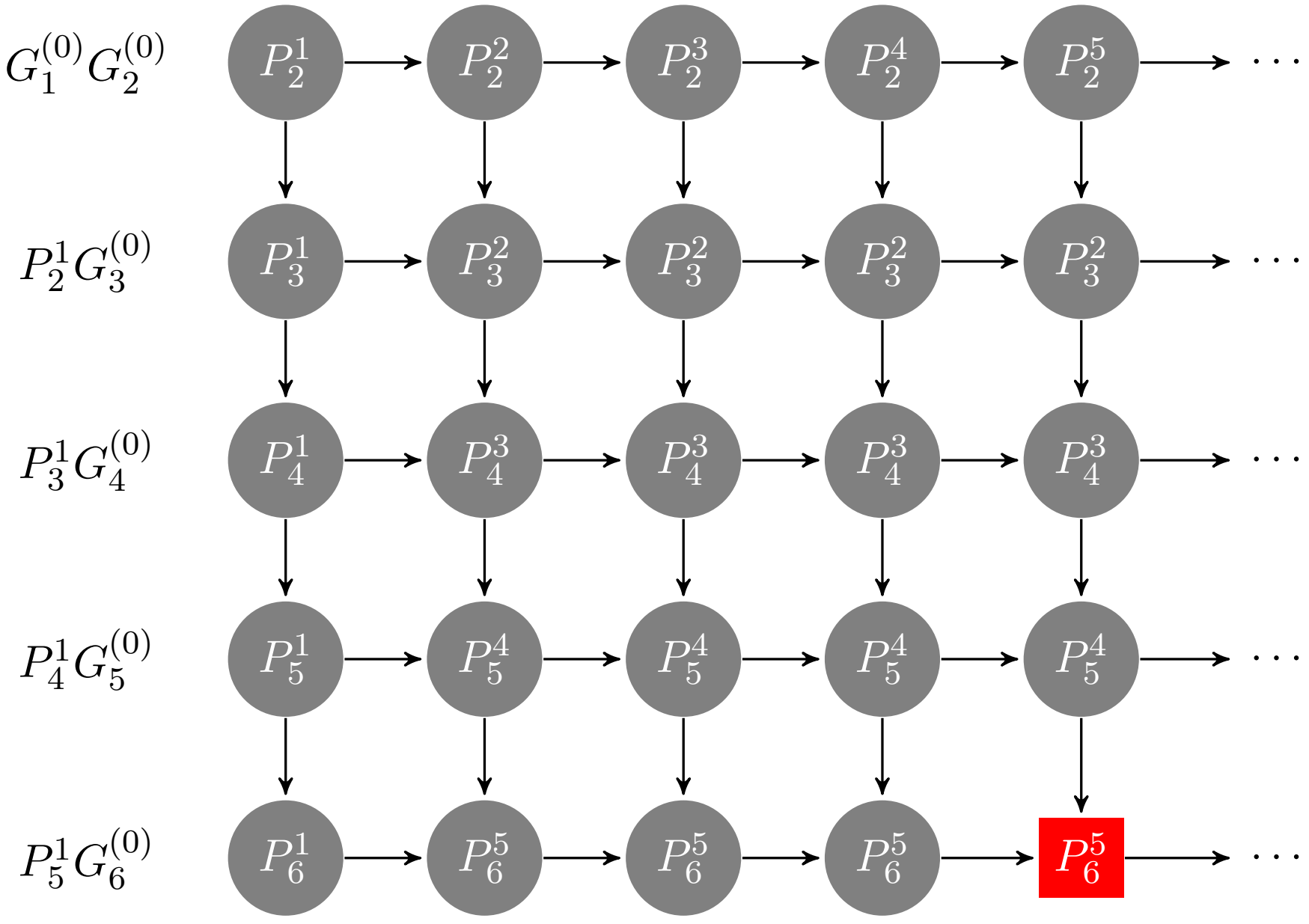
Computing $\Delta F^{(j)}(X, Y)$



Computing $\Delta F^{(j)}(X, Y)$



Computing $\Delta F^{(j)}(X, Y)$



Complexity result:

Theorem 2:

he k-th iteration of Step 9 in the Algorithm 4 runs within

- $\mathcal{O}(k\, d\mathsf{M}(d))$ operations in $\mathbb{C}$,
- $\mathcal{O}(k\, d\mathsf{M}(d)^2)$ operations in the field of coefficients of $F(X, Y)$.

Comparative complexity results

Theorem 3:

Our enhancement of the EHC computes all the branches in $\mathcal{O}(k^2\, d\, \mathsf{M}(d))$ operations in $\mathbb{C}$, using a *linear lifting scheme*.

Kung-Traub, 1987

The first k iterations of Newton-Puiseux on an input bivariate polynomial of degree d computes all branches within

- $\mathcal{O}(d^2\, k\, \mathsf{M}(k))$ operations in $\mathbb{C}$ using a *linear lifting scheme* (Theorem 5.2 in their paper)
- $\mathcal{O}(d^2\, \mathsf{M}(k))$ operations in $\mathbb{C}$ using a *quadratic lifting scheme* (Corollary 5.1 in their paper)

D. V. Chudnovsky and G. V. Chudnovsky, 2015

The latter estimate reported by Kung and Traub is improved to $\mathcal{O}(d^2\, k)$ operations in $\mathbb{C}$ for computing all the branches.

Remark

A quadratic lifting scheme for the EHC is work in progress.