# Tracking $p$-adic precision

MAP 2014

Tristan Vaccon (with X.Caruso & D.Roe)

Université de Rennes I

27 mai 2014

# Motivation for $p$-adic algorithm

## Why should one work with $p$-adic numbers ?

- Going from $\mathbb{F}_p$ to $\mathbb{Z}_p$ and then back to $\mathbb{F}_p$ enables more computation ;

# Motivation for $p$-adic algorithm

## Why should one work with $p$-adic numbers ?

- Going from $\mathbb{F}_p$ to $\mathbb{Z}_p$ and then back to $\mathbb{F}_p$ enables more computation ;
- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;

# Motivation for $p$-adic algorithm

## Why should one work with $p$-adic numbers ?

- Going from $\mathbb{F}_p$ to $\mathbb{Z}_p$ and then back to $\mathbb{F}_p$ enables more computation ;
- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;
- Some questions or algorithms are $p$-adic by nature.

# Motivation for $p$-adic algorithm

## Why should one work with $p$-adic numbers ?

- Going from $\mathbb{F}_p$ to $\mathbb{Z}_p$ and then back to $\mathbb{F}_p$ enables more computation ;
- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;
- Some questions or algorithms are $p$-adic by nature.

## Some examples of essentially $p$-adic algorithms

- Polynomial factorization with Hensel lemma ;

# Motivation for $p$-adic algorithm

## Why should one work with $p$-adic numbers ?

- Going from $\mathbb{F}_p$ to $\mathbb{Z}_p$ and then back to $\mathbb{F}_p$ enables more computation ;
- Working in $\mathbb{Q}_p$ instead of $\mathbb{Q}$, one can handle more efficiently the coefficients growth ;
- Some questions or algorithms are $p$-adic by nature.

## Some examples of essentially $p$-adic algorithms

- Polynomial factorization with Hensel lemma ;
- Kedlaya's counting-point algorithm on hyperelliptic curves with $p$-adic cohomology ;

UNIVERSITÉ DE RENNES 1

# Norms over a field

## Definition

A norm over a field $K$ is a mapping $|\cdot| : K \to \mathbb{R}_+, x \mapsto |x|$ such that :

$$(i)\ |x| = 0 \Leftrightarrow x = 0;$$
$$(ii)\ |xy| = |x||y|;$$
$$(iii)\ |x+y| \leqslant |x| + |y|.$$

# Norms over a field

## Definition

A norm over a field $K$ is a mapping $|\cdot| \ : \ K \to \mathbb{R}_+, x \mapsto |x|$ such that :

$$(i)\ |x| = 0 \Leftrightarrow x = 0;$$
$$(ii)\ |xy| = |x||y|;$$
$$(iii)\ |x+y| \leqslant |x| + |y|.$$

It is called **ultrametric** if :

$$(iii')\ |x+y| \leqslant \sup(|x|, |y|).$$

# Norms over a vector space

## Definition

Let $K$ be a normed field. A norm over a $K$-vector space $E$ is a mapping $\|\cdot\| : E \to \mathbb{R}_+, x \mapsto \|x\|$ such that :

$$(i)\ \|x\| = 0 \Leftrightarrow x = 0;$$
$$(ii)\ \|\alpha y\| = |\alpha|\|y\|;$$
$$(iii)\ \|x + y\| \leqslant \|x\| + \|y\|.$$

# Norms over a vector space

## Definition

Let $K$ be a normed field. A norm over a $K$-vector space $E$ is a mapping $\|\cdot\| : E \to \mathbb{R}_+, x \mapsto \|x\|$ such that :

$$(i)\ \|x\| = 0 \Leftrightarrow x = 0;$$
$$(ii)\ \|\alpha y\| = |\alpha|\|y\|;$$
$$(iii)\ \|x+y\| \leqslant \|x\| + \|y\|.$$

It is called **ultrametric** if :

$$(iii')\ \|x+y\| \leqslant \sup(\|x\|, \|y\|).$$

# An ultrametric norm over $\mathbb{Q}$

## Definition

For any $p$ prime in $\mathbb{N}$, we define the $p$-adic valuation $v_p : \mathbb{Q} \to \mathbb{Z}$ by :

# An ultrametric norm over $\mathbb{Q}$

## Definition

For any $p$ prime in $\mathbb{N}$, we define the $p$-adic valuation $v_p : \mathbb{Q} \to \mathbb{Z}$ by :

$$v_p(n) = \max\left\{k \in \mathbb{N},\ p^k \mid n\right\},$$

# An ultrametric norm over $\mathbb{Q}$

## Definition

For any $p$ prime in $\mathbb{N}$, we define the $p$-adic valuation $v_p : \mathbb{Q} \to \mathbb{Z}$ by :

$$v_p(n) = \max\left\{k \in \mathbb{N},\ p^k \mid n\right\},$$
$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

# An ultrametric norm over $\mathbb{Q}$

## Definition

For any $p$ prime in $\mathbb{N}$, we define the $p$-adic valuation $v_p : \mathbb{Q} \to \mathbb{Z}$ by :

$$v_p(n) = \max\left\{k \in \mathbb{N},\ p^k \mid n\right\},$$
$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

## Definition

For any $x \in \mathbb{Q}$,

$$|x|_p = p^{-v_p(x)}.$$

# An ultrametric norm over $\mathbb{Q}$

## Definition

For any $p$ prime in $\mathbb{N}$, we define the $p$-adic valuation $v_p : \mathbb{Q} \to \mathbb{Z}$ by :

$$v_p(n) = \max\left\{k \in \mathbb{N},\ p^k \mid n\right\},$$
$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

## Definition

For any $x \in \mathbb{Q}$,

$$|x|_p = p^{-v_p(x)}.$$

$|\cdot|_p$ is an **ultrametric norm** over $\mathbb{Q}$.

# Definition of $\mathbb{Q}_p$

## Definition

We define $\mathbb{Q}_p$ as "the" **completion** of $\mathbb{Q}$ for $|\cdot|_p$.

# Definition of $\mathbb{Q}_p$

## Definition

We define $\mathbb{Q}_p$ as "the" **completion** of $\mathbb{Q}$ for $|\cdot|_p$.
$|\cdot|_p$ and $v_p$ extend to $\mathbb{Q}_p$

# Definition of $\mathbb{Q}_p$

## Definition

We define $\mathbb{Q}_p$ as "the" **completion** of $\mathbb{Q}$ for $|\cdot|_p$.
$|\cdot|_p$ and $v_p$ extend to $\mathbb{Q}_p$ $|\cdot|_p$ is still **ultrametric**.

## Definition

We write :

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p,\ v_p(x) \geq 0\} = \{x \in \mathbb{Q}_p,\ |x|_p \leq 1\} = B'_{\mathbb{Q}_p}(0,1).$$

# Definition of $\mathbb{Q}_p$

## Definition

We define $\mathbb{Q}_p$ as "the" **completion** of $\mathbb{Q}$ for $|\cdot|_p$.
$|\cdot|_p$ and $v_p$ extend to $\mathbb{Q}_p$ $|\cdot|_p$ is still **ultrametric**.

## Definition

We write :

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p,\ v_p(x) \geq 0\} = \{x \in \mathbb{Q}_p,\ |x|_p \leq 1\} = B'_{\mathbb{Q}_p}(0,1).$$

$\mathbb{Z}_p$ is a sub-ring of $\mathbb{Q}_p$.

# Working with $\mathbb{Q}_p$

## Proposition

*If $x \in \mathbb{Z}_p$, we can write*

$$x = \sum_{i \geq 0}^{+\infty} a_i p^i.$$

# Working with $\mathbb{Q}_p$

## Proposition

*If $x \in \mathbb{Z}_p$, we can write*

$$x = \sum_{i \geq 0}^{+\infty} a_i p^i.$$

*If $x \in \mathbb{Q}_p$, we can write*

$$x = \frac{1}{p^k} \sum_{i \geq 0}^{+\infty} a_i p^i.$$

# Working with $\mathbb{Q}_p$

## Proposition

*If $x \in \mathbb{Z}_p$, we can write*

$$x = \sum_{i \geq 0}^{+\infty} a_i p^i.$$

*If $x \in \mathbb{Q}_p$, we can write*

$$x = \frac{1}{p^k} \sum_{i \geq 0}^{+\infty} a_i p^i.$$

## Example

Let $x = \ldots 6666666_7 = \sum_{i \geq 0}^{+\infty} 6 \times 7^i$.

# Working with $\mathbb{Q}_p$

## Proposition

*If $x \in \mathbb{Z}_p$, we can write*

$$x = \sum_{i \geq 0}^{+\infty} a_i p^i.$$

*If $x \in \mathbb{Q}_p$, we can write*

$$x = \frac{1}{p^k} \sum_{i \geq 0}^{+\infty} a_i p^i.$$

## Example

Let $x = \ldots 6666666_7 = \sum_{i \geq 0}^{+\infty} 6 \times 7^i$. Then $x \in \mathbb{Z}_7$. We remark that $x + 1 = 0$.

# Working with $\mathbb{Q}_p$

## Proposition

*If $x \in \mathbb{Z}_p$, we can write*

$$x = \sum_{i \geq 0}^{+\infty} a_i p^i.$$

*If $x \in \mathbb{Q}_p$, we can write*

$$x = \frac{1}{p^k} \sum_{i \geq 0}^{+\infty} a_i p^i.$$

## Example

Let $x = \ldots 6666666_7 = \sum_{i \geq 0}^{+\infty} 6 \times 7^i$. Then $x \in \mathbb{Z}_7$. We remark that $x + 1 = 0$.

We also have :

$$\ldots 44445_7 = \frac{1}{3} \in \mathbb{Z}_7,$$

# Working with $\mathbb{Q}_p$

## Proposition

*If $x \in \mathbb{Z}_p$, we can write*

$$x = \sum_{i \geq 0}^{+\infty} a_i p^i.$$

*If $x \in \mathbb{Q}_p$, we can write*

$$x = \frac{1}{p^k} \sum_{i \geq 0}^{+\infty} a_i p^i.$$

## Example

Let $x = \ldots 6666666_7 = \sum_{i \geq 0}^{+\infty} 6 \times 7^i$. Then $x \in \mathbb{Z}_7$. We remark that $x + 1 = 0$.

We also have :

$$\ldots 44445_7 = \frac{1}{3} \in \mathbb{Z}_7,$$

And,

$$\ldots 4444,6_7 = \frac{4}{21}.$$

# Topology and ultrametricity

**Proposition**

*If $E$ is an ultrametric vector space, then **any** point in a ball of $E$ is its **center**.*

# Algebraic point of view

## Proposition

$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

# Algebraic point of view

## Proposition

$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

*More precisely,*

$$\forall k \in \mathbb{N}, \mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}.$$

# Algebraic point of view

## Proposition

$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}.$$

*More precisely,*

$$\forall k \in \mathbb{N}, \mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}.$$

## Remark

$$\begin{tikzcd} \mathbb{Q}_p \arrow[dr, dash] & & \mathbb{R} \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

$$\begin{tikzcd} \mathbb{Z}_p \arrow[r] \arrow[d, two heads] \arrow[dr, phantom, "\circlearrowright"] & \mathbb{Z}_p \\ \mathbb{Z} \arrow[r, two heads] \arrow[u, hook] & \mathbb{Z}/p^k\mathbb{Z} \end{tikzcd}$$

# Table of contents



UNIVERSITÉ DE RENNES 1

# Definition of the precision

## Finite-precision $p$-adics

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=-l}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ and $p$ a prime number.
While working with a computer, we usually only can consider the beginning of this power serie expansion: we only consider elements of the following form $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, with $l \in \mathbb{Z}$.

# Definition of the precision

## Finite-precision $p$-adics

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=-l}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ and $p$ a prime number.
While working with a computer, we usually only can consider the beginning of this power serie expansion: we only consider elements of the following form $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, with $l \in \mathbb{Z}$.

## Definition

The **order**, or the **absolute precision** of $\sum_{i=k}^{d-1} a_i p^i + O(p^d)$ is $d$.

# Definition of the precision

## Finite-precision $p$-adics

Elements of $\mathbb{Q}_p$ can be written $\sum_{i=-l}^{+\infty} a_i p^i$, with $a_i \in [\![0, p-1]\!]$, $l \in \mathbb{Z}$ and $p$ a prime number.
While working with a computer, we usually only can consider the beginning of this power serie expansion: we only consider elements of the following form $\sum_{i=l}^{d-1} a_i p^i + O(p^d)$, with $l \in \mathbb{Z}$.

## Definition

The **order**, or the **absolute precision** of $\sum_{i=k}^{d-1} a_i p^i + O(p^d)$ is $d$.

## Example

The order of $3 * 7^{-1} + 4 * 7^0 + 5 * 7^1 + 6 * 7^2 + O(7^3)$ is 3.

# $p$-adic algorithms : an example

## Hensel factorization

We would like to factor $Q \in \mathbb{Z}[X]$ :

# $p$-adic algorithms : an example

## Hensel factorization

We would like to factor $Q \in \mathbb{Z}[X]$ :

1. Chose a $p$ that is well-suited to the problem ;

# $p$-adic algorithms : an example

## Hensel factorization

We would like to factor $Q \in \mathbb{Z}[X]$ :

1. Chose a $p$ that is well-suited to the problem ;
2. Factor $\overline{Q} \in \mathbb{Z}/p\mathbb{Z}[X]$ ;

# $p$-adic algorithms : an example

## Hensel factorization

We would like to factor $Q \in \mathbb{Z}[X]$ :

1. Chose a $p$ that is well-suited to the problem ;
2. Factor $\overline{Q} \in \mathbb{Z}/p\mathbb{Z}[X]$ ;
3. Lift the factors into $\mathbb{Z}/p^k\mathbb{Z}[X]$ (with *Hensel's lemma*) ;

# $p$-adic algorithms : an example

## Hensel factorization

We would like to factor $Q \in \mathbb{Z}[X]$ :

1. Chose a $p$ that is well-suited to the problem ;
2. Factor $\overline{Q} \in \mathbb{Z}/p\mathbb{Z}[X]$ ;
3. Lift the factors into $\mathbb{Z}/p^k\mathbb{Z}[X]$ (with *Hensel's lemma*) ;
4. If $p^k$ is big enough (*Mignotte's bound*), we can obtain a factorization over $\mathbb{Q}$ (up to the recombination of some factors).

# Table of contents

# $p$-adic precion *vs* real precision

The quintessential idea of the step-by-step analysis is the following :

**Proposition ($p$-adic errors don't add)**

*Indeed,*

$$(a + O(p^{k})) + (b + O(p^{k})) = a + b + O(p^{k}).$$

*That is to say, if $a$ and $b$ are known up to precision $O(p^k)$, then so is $a + b$.*

# $p$-adic precion *vs* real precision

The quintessential idea of the step-by-step analysis is the following :

**Proposition ($p$-adic errors don't add)**

*Indeed,*

$$(a + O(p^{k})) + (b + O(p^{k})) = a + b + O(p^{k}).$$

*That is to say, if $a$ and $b$ are known up to precision $O(p^k)$, then so is $a + b$.*

# $p$-adic precion *vs* real precision

The quintessential idea of the step-by-step analysis is the following :

**Proposition ($p$-adic errors don't add)**

*Indeed,*

$$(a + O(p^k)) + (b + O(p^k)) = a + b + O(p^k).$$

*That is to say, if $a$ and $b$ are known up to precision $O(p^k)$, then so is $a + b$.*

**Remark**

It is quite the opposite to when dealing with real numbers, because of **Round-off error** :

$$(1 + 5 * 10^{-2}) + (2 + 6 * 10^{-2}) = 3 + 1 * 10^{-1} + 1 * 10^{-2}.$$

That is to say, if $a$ and $b$ are known up to precision $10^{-n}$, then $a + b$ is known up to $10^{(-n+1)}$.

# $p$-adic precion *vs* real precision

The quintessential idea of the step-by-step analysis is the following :

**Proposition ($p$-adic errors don't add)**

*Indeed,*

$$(a + O(p^{k})) + (b + O(p^{k})) = a + b + O(p^{k}).$$

*That is to say, if $a$ and $b$ are known up to precision $O(p^k)$, then so is $a + b$.*

**Remark**

It is quite the opposite to when dealing with real numbers, because of **Round-off error** :

$$(1 + 5 * 10^{-2}) + (2 + 6 * 10^{-2}) = 3 + 1 * 10^{-1} + 1 * 10^{-2}.$$

That is to say, if $a$ and $b$ are known up to precision $10^{-n}$, then $a + b$ is known up to $10^{(-n+1)}$.

# Precision formulae

## Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{min(k_0,k_1)})$$

# Precision formulae

## Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{min(k_0,k_1)})$$

## Proposition (multiplication)

$$(x_0 + O(p^{k_0})) * (x_1 + O(p^{k_1})) = x_0 * x_1 + O(p^{min(k_0+v_p(x_1),k_1+v_p(x_0))})$$

# Precision formulae

## Proposition (addition)

$$(x_0 + O(p^{k_0})) + (x_1 + O(p^{k_1})) = x_0 + x_1 + O(p^{min(k_0,k_1)})$$

## Proposition (multiplication)

$$(x_0 + O(p^{k_0})) * (x_1 + O(p^{k_1})) = x_0 * x_1 + O(p^{min(k_0+v_p(x_1),k_1+v_p(x_0))})$$

## Proposition (division)

$$\frac{xp^a + O(p^b)}{yp^c + O(p^d)} = x * y^{-1}p^{a-c} + O(p^{min(d+a-2c,b-c)})$$

*In particular,*

$$\frac{1}{p^c y + O(p^d)} = y^{-1}p^{-c} + O(p^{d-2c})$$

# Optimality

## Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_p^2 & \to & \mathbb{Q}_p^2 \\ (x, y) & \mapsto & (x + y, x - y). \end{array}$

# Optimality

## Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_p^2 & \to & \mathbb{Q}_p^2 \\ (x,y) & \mapsto & (x+y, x-y). \end{array}$

We would like to compute $f \circ f(x,y)$ with

$(x,y) = (1 + \boxed{O(p^{10})}, 1 + O(p))$.

# Optimality

## Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_p^2 & \to & \mathbb{Q}_p^2 \\ (x,y) & \mapsto & (x+y, x-y). \end{array}$

We would like to compute $f \circ f(x,y)$ with

$(x,y) = (1 + \boxed{O(p^{10})}, 1 + O(p))$.

- If we apply $f$ two times, we get :

$$f \circ f(x,y) = (2 + \boxed{O(p)}, 2 + O(p)).$$

# Optimality

## Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_p^2 & \to & \mathbb{Q}_p^2 \\ (x,y) & \mapsto & (x+y, x-y). \end{array}$

We would like to compute $f \circ f(x,y)$ with

$(x,y) = (1 + \boxed{O(p^{10})}, 1 + O(p))$.

- If we apply $f$ two times, we get :

$$f \circ f(x,y) = (2 + \boxed{O(p)}, 2 + O(p)).$$

- If we remark that $f \circ f = 2Id$, we get :

$$f \circ f(x,y) = (2 + \boxed{O(p^{10})}, 2 + O(p)).$$

# Optimality

## Step-by-step analysis is not optimal.

Let $f : \begin{array}{ccc} \mathbb{Q}_p^2 & \to & \mathbb{Q}_p^2 \\ (x,y) & \mapsto & (x+y, x-y). \end{array}$

We would like to compute $f \circ f(x,y)$ with

$(x,y) = (1 + \boxed{O(p^{10})}, 1 + O(p))$.

- If we apply $f$ two times, we get :

$$f \circ f(x,y) = (2 + \boxed{O(p)}, 2 + O(p)).$$

- If we remark that $f \circ f = 2Id$, we get :

$$f \circ f(x,y) = (2 + \boxed{O(p^{10})}, 2 + O(p)).$$

# Non intrinsic

**X.Caruso (12) : Step-by-step analysis is algorithm-dependent.**

Let $M \in M_d(\mathbb{Z}_p)$ be a random matrix whose all entries are known up to precision $O(p^N)$.

# Non intrinsic

**X.Caruso (12) : Step-by-step analysis is algorithm-dependent.**

Let $M \in M_d(\mathbb{Z}_p)$ be a random matrix whose all entries are known up to precision $O(p^N)$.
We would like to compute $M = LU$ the $LU$ factorization of $M$. Then :

# Non intrinsic

**X.Caruso (12) : Step-by-step analysis is algorithm-dependent.**

Let $M \in M_d(\mathbb{Z}_p)$ be a random matrix whose all entries are known up to precision $O(p^N)$.
We would like to compute $M = LU$ the $LU$ factorization of $M$. Then :

- If we apply Gaussian elimination, the average precision on $L$ is $O(p^{n-\frac{2d}{p-1}})$.

# Non intrinsic

**X.Caruso (12) : Step-by-step analysis is algorithm-dependent.**

Let $M \in M_d(\mathbb{Z}_p)$ be a random matrix whose all entries are known up to precision $O(p^N)$.
We would like to compute $M = LU$ the $LU$ factorization of $M$. Then :

- If we apply Gaussian elimination, the average precision on $L$ is $O(p^{n-\frac{2d}{p-1}})$.
- If we study Cramer-style formulae, the intrinsic precision determined for $L$ is $O(p^{n-2\log_p(d)})$.

# Table of contents

# The Main lemma of $p$-adic differential precision

**Lemma**

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a* ***differentiable*** *mapping.*

# The Main lemma of $p$-adic differential precision

**Lemma**

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a **differentiable** mapping.*
*Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is **surjective**.*

# The Main lemma of $p$-adic differential precision

**Lemma**

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a **differentiable** mapping.*
*Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is **surjective**.*
*Then for any ball $B = B(0, r)$ **small enough**,*

$$f(x + B) = f(x) + f'(x) \cdot B.$$

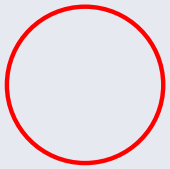
# Geometrical meaning

## Interpretation

$x+$

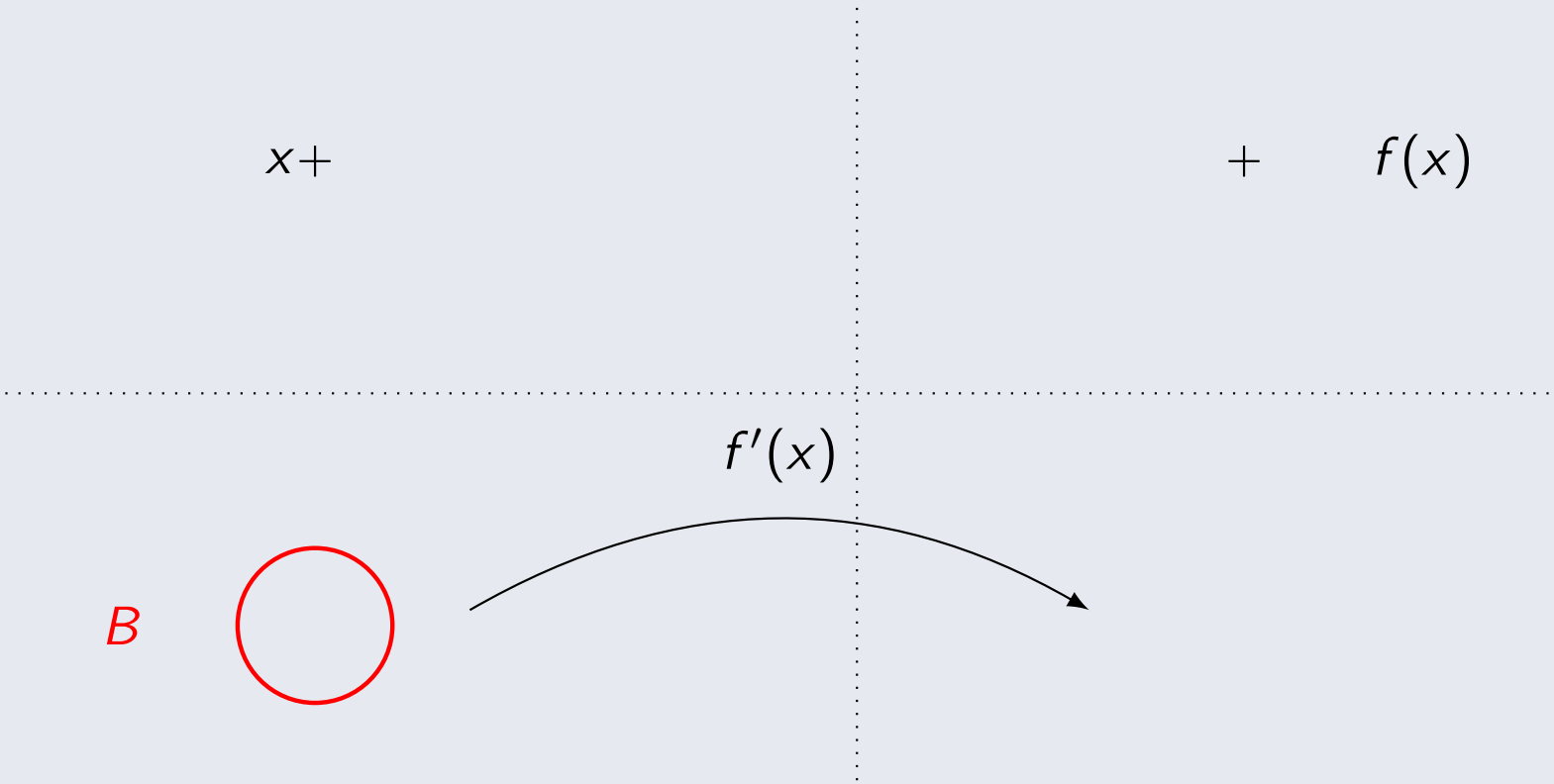
$+ \quad f(x)$

$B$



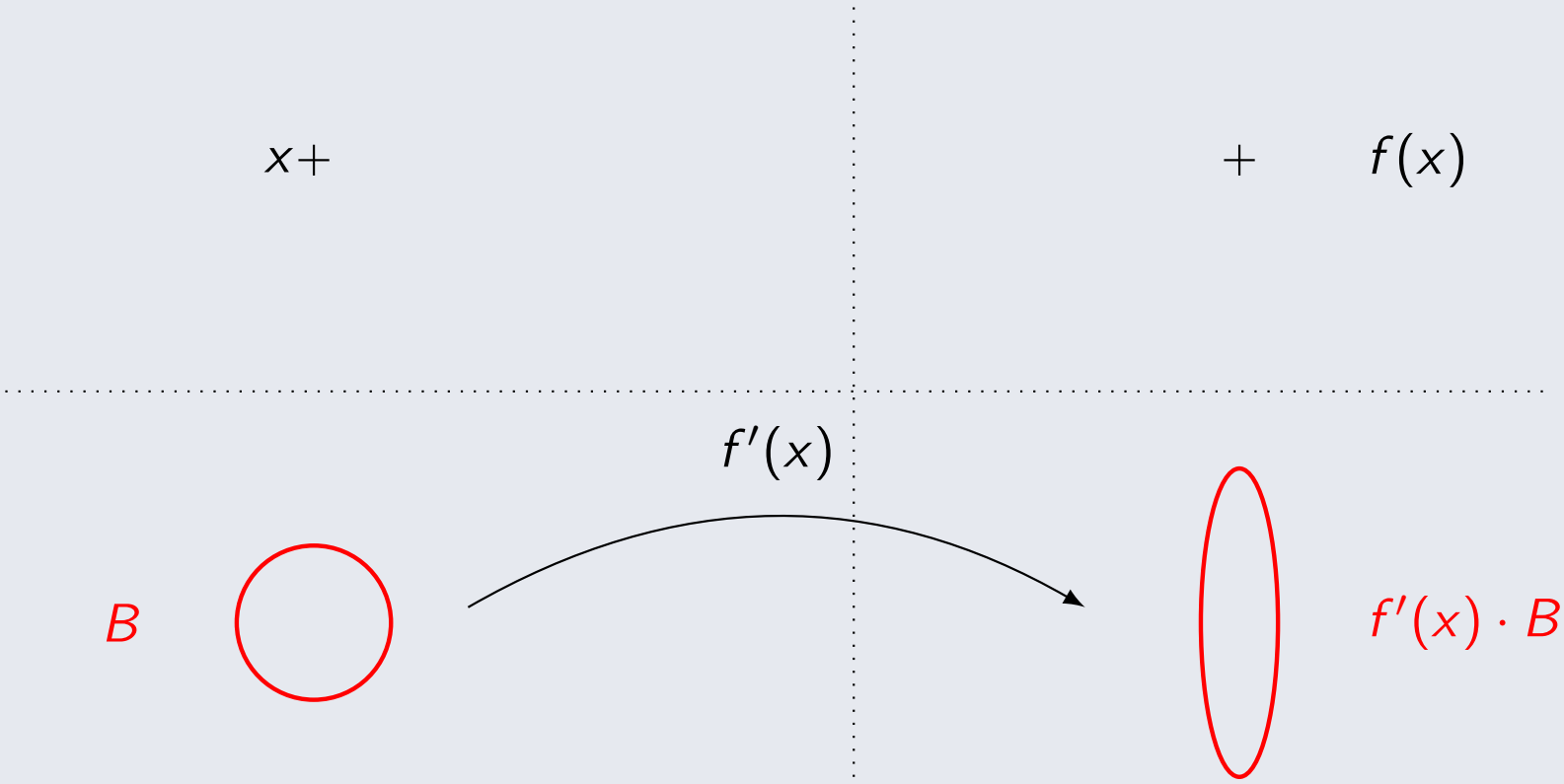
# Geometrical meaning

## Interpretation



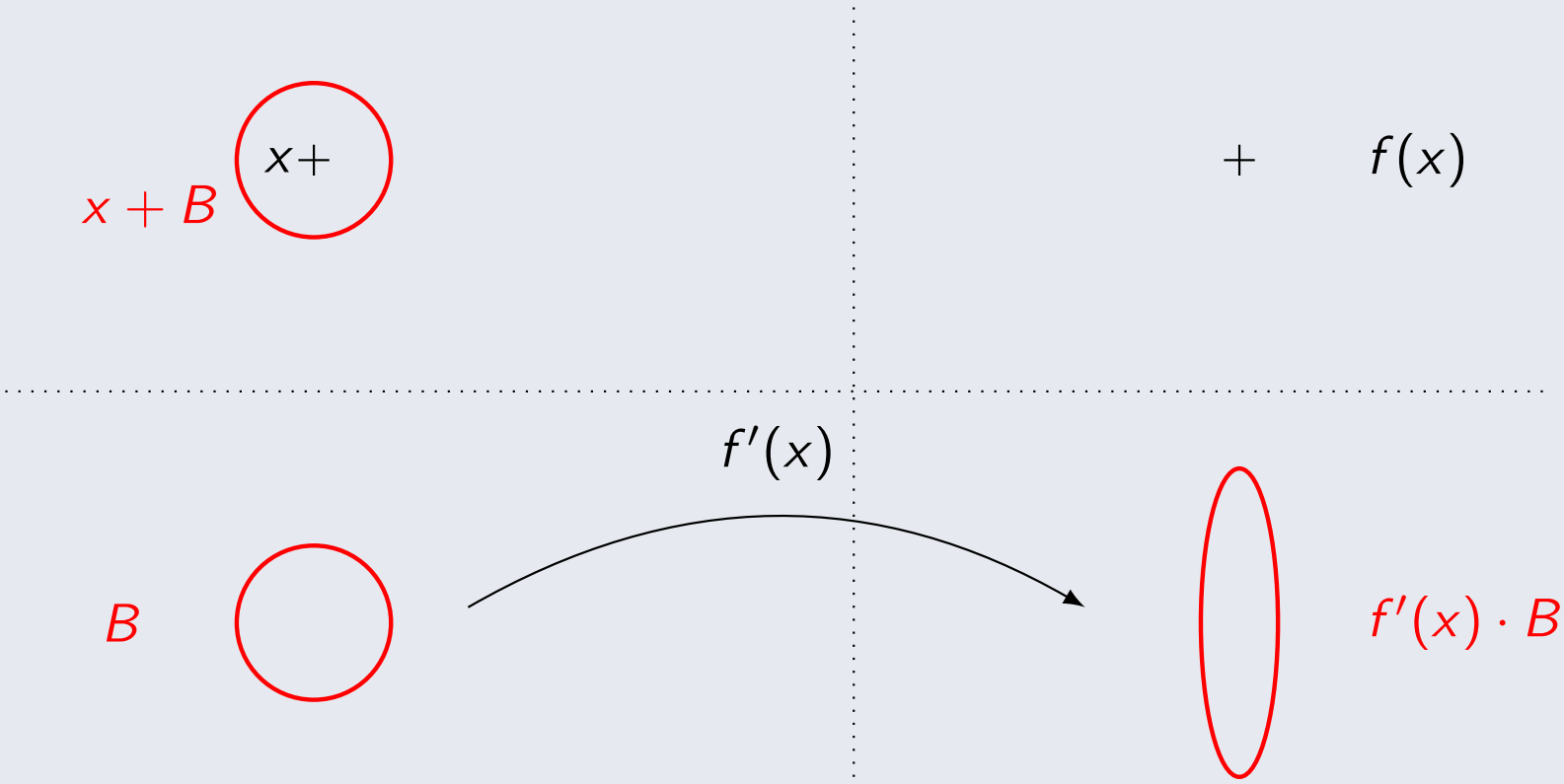
# Geometrical meaning

## Interpretation



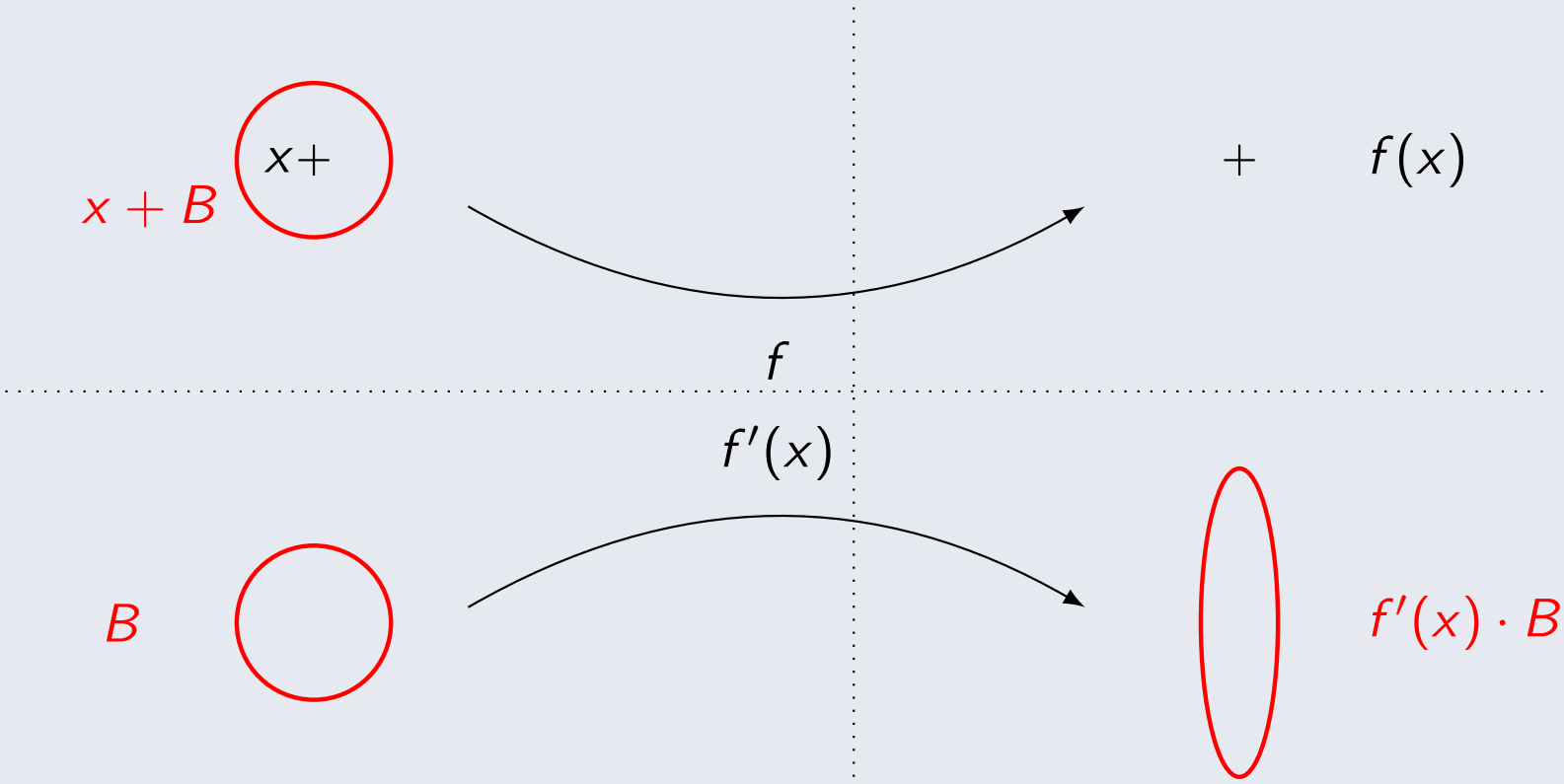
# Geometrical meaning

## Interpretation



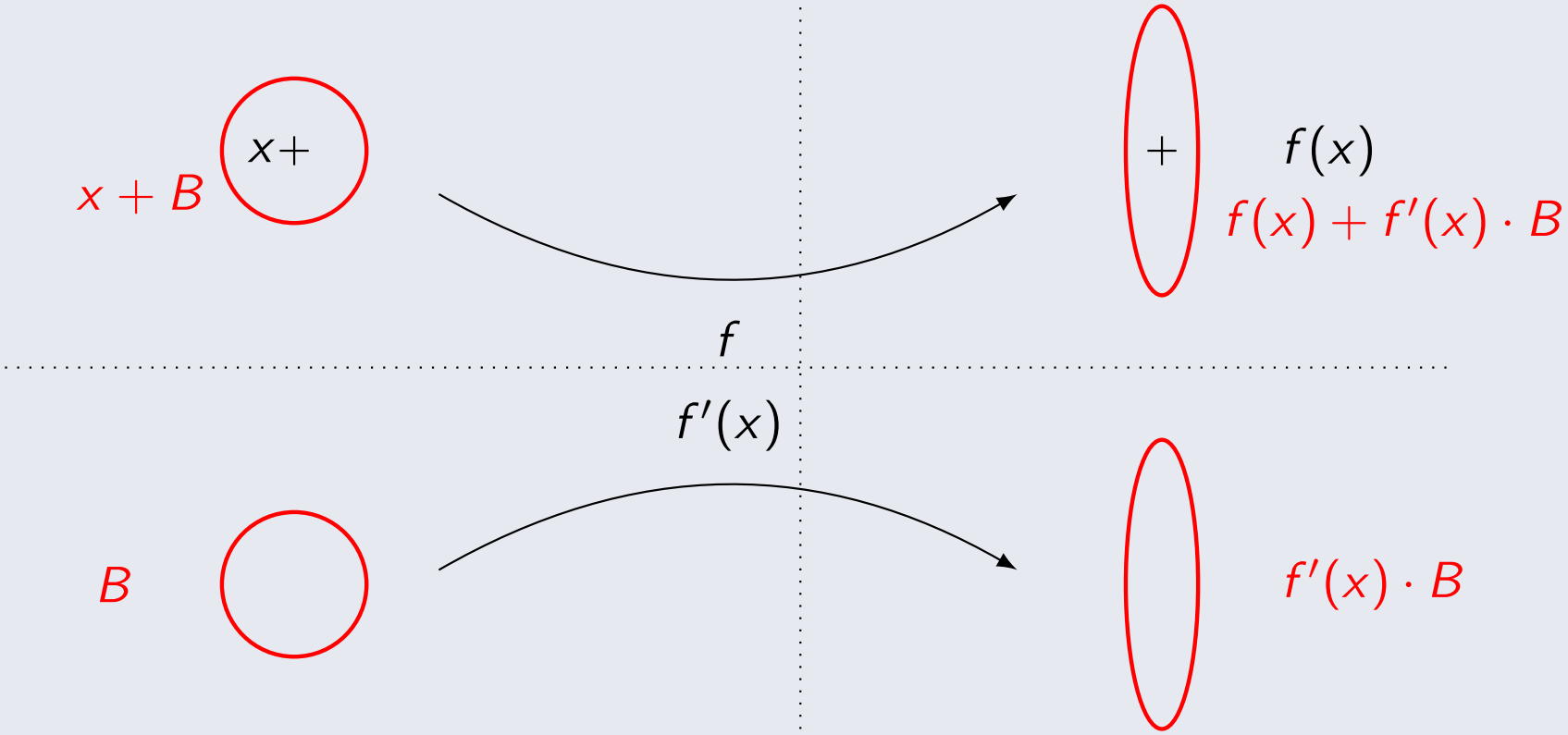
# Geometrical meaning

## Interpretation



# Geometrical meaning

## Interpretation



# Table of contents

# Introduction to the Somos-4 sequence

## Definition

We define the **Somos-4** sequence by recursion, with :

$$x_0, x_1, x_2, x_3 \in \mathbb{Z}_p^\times,$$

$$x_{n+4} = \frac{x_{n+1}x_{n+3} + x_{n+2}^2}{x_n}.$$

# Introduction to the Somos-4 sequence

## Definition

We define the **Somos-4** sequence by recursion, with :

$$x_0, x_1, x_2, x_3 \in \mathbb{Z}_p^\times,$$

$$x_{n+4} = \frac{x_{n+1}x_{n+3} + x_{n+2}^2}{x_n}.$$

## Remark

This formula comes from the $Z$-coordinate of $[m]\,P + Q$ for some $P, Q$ points on the **elliptic curve** $y^2 + y = x^3 + x$.

# Introduction to the Somos-4 sequence

## Definition

We define the **Somos-4** sequence by recursion, with :

$$x_0, x_1, x_2, x_3 \in \mathbb{Z}_p^\times,$$

$$x_{n+4} = \frac{x_{n+1}x_{n+3} + x_{n+2}^2}{x_n}.$$

## Remark

This formula comes from the $Z$-coordinate of $[m]\,P + Q$ for some $P, Q$ points on the **elliptic curve** $y^2 + y = x^3 + x$.

## Proposition

*For all $n$, $x_n \in \mathbb{Z}_p$, i.e. $v_p(x_n) \geq 0$.*

# The Laurent phenomenon

## Remark

If $x_0, x_1, x_2, x_3$ are known up to $O(p^m)$, then because of the division by $x_n$, a naive step-by-step analysis show that $x_{n+4}$ is known up to $O(p^{m-\sum_{k=0}^{n} v_p(x_k)})$.

# The Laurent phenomenon

## Remark

If $x_0, x_1, x_2, x_3$ are known up to $O(p^m)$, then because of the division by $x_n$, a naive step-by-step analysis show that $x_{n+4}$ is known up to $O(p^{m-\sum_{k=0}^{n} v_p(x_k)})$.

## Theorem (Fomin, Zelevinsky)

*Let $P_n$ be the rational fraction defined by the recursion formula defining Somos-4 :*

$$x_n = P_n(x_0, x_1, x_2, x_3).$$

# The Laurent phenomenon

## Remark

If $x_0, x_1, x_2, x_3$ are known up to $O(p^m)$, then because of the division by $x_n$, a naive step-by-step analysis show that $x_{n+4}$ is known up to $O(p^{m-\sum_{k=0}^{n} v_p(x_k)})$.

## Theorem (Fomin, Zelevinsky)

*Let $P_n$ be the rational fraction defined by the recursion formula defining Somos-4 :*

$$x_n = P_n(x_0, x_1, x_2, x_3).$$

*Then $P_n \in \mathbb{Z}[x_0^{\pm 1}, x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$.*

# Consequence

# Consequence

**Theorem**

$P_n \in \mathbb{Z}[x_0^{\pm 1}, x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$.

# Consequence

## Theorem

$P_n \in \mathbb{Z}[x_0^{\pm 1}, x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$.

## Remark

If $m$ is big enough,

$$\begin{aligned} &P_n(x_0 + O(p^m), x_1 + O(p^m), x_2 + O(p^m), x_3 + O(p^m)) \\ &\quad = x_n + P'_n(x_0, x_1, x_2, x_3) \cdot (O(p^m), O(p^m), O(p^m), O(p^m))^t. \end{aligned}$$

# Consequence

## Theorem

$P_n \in \mathbb{Z}[x_0^{\pm 1}, x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$.

## Remark

If $m$ is big enough,

$$\begin{aligned} &P_n(x_0 + O(p^m), x_1 + O(p^m), x_2 + O(p^m), x_3 + O(p^m)) \\ &\quad = x_n + P'_n(x_0, x_1, x_2, x_3) \cdot (O(p^m), O(p^m), O(p^m), O(p^m))^t. \end{aligned}$$

Coefficients of $P'_n(x_0, x_1, x_2, x_3)$ are in $\mathbb{Z}_p$.

# Consequence

## Theorem

$P_n \in \mathbb{Z}[x_0^{\pm 1}, x_1^{\pm 1}, x_2^{\pm 1}, x_3^{\pm 1}]$.

## Remark

If $m$ is big enough,

$$\begin{aligned} &P_n(x_0 + O(p^m), x_1 + O(p^m), x_2 + O(p^m), x_3 + O(p^m)) \\ &\quad = x_n + P'_n(x_0, x_1, x_2, x_3) \cdot (O(p^m), O(p^m), O(p^m), O(p^m))^t. \end{aligned}$$

Coefficients of $P'_n(x_0, x_1, x_2, x_3)$ are in $\mathbb{Z}_p$.

## Corollary

*There is no intrinsic loss of precision : $x_n$ is determined up to $O(p^m)$.*

# Table of contents

# Lattices

# Lattices

## Lemma

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a **differentiable** mapping.*
*Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is **surjective**.*
*Then for any ball $B = B(0, r)$ **small enough**,*

$$f(x + B) = f(x) + f'(x) \cdot B.$$

# Lattices

## Lemma

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a **differentiable** mapping.*
*Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is **surjective**.*
*Then for any ball $B = B(0, r)$ **small enough**, for any open **lattice** $H \subset B$*

$$f(x + H) = f(x) + f'(x) \cdot H.$$

# Lattices

## Lemma

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a **differentiable** mapping.*
*Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is **surjective**.*
*Then for any ball $B = B(0, r)$ **small enough**, for any open **lattice** $H \subset B$*

$$f(x + H) = f(x) + f'(x) \cdot H.$$

## Remark

This allows more models of precision, like

$$(x, y) = (1 + O(p^{10}), 1 + O(p)).$$

# Lattices

## Lemma

*Let $f : \mathbb{Q}_p^n \to \mathbb{Q}_p^m$ be a* ***differentiable*** *mapping.*
*Let $x \in \mathbb{Q}_p^n$. We assume that $f'(x)$ is* ***surjective****.*
*Then for any ball $B = B(0, r)$* ***small enough****, for any open* ***lattice*** *$H \subset B$*

$$f(x + H) = f(x) + f'(x) \cdot H.$$

## Remark

This allows more models of precision, like

$$(x, y) = (1 + O(p^{10}), 1 + O(p)).$$

## Remark

Our framework can be extended to (complete) **ultrametric** $K$-vector spaces (*e.g.* $\mathbb{F}_p((X))^n$, $\mathbb{Q}((X))^m$).

# Higher differentials

# Higher differentials

## What is **small enough**

How can we determine when the lemma applies ?

# Higher differentials

## What is **small enough**

How can we determine when the lemma applies ?
When $f$ is locally analytic, it essentially corresponds to

$$\sum_{k=2}^{+\infty} \frac{1}{k!} f^{(k)}(x) \cdot H^k \subset f'(x) \cdot H.$$

# Higher differentials

## What is **small enough**

How can we determine when the lemma applies ?
When $f$ is locally analytic, it essentially corresponds to

$$\sum_{k=2}^{+\infty} \frac{1}{k!} f^{(k)}(x) \cdot H^k \subset f'(x) \cdot H.$$

This can be determined with **Newton-polygon** techniques.

# Higher differentials

## What is **small enough**

How can we determine when the lemma applies ?
When $f$ is locally analytic, it essentially corresponds to

$$\sum_{k=2}^{+\infty} \frac{1}{k!} f^{(k)}(x) \cdot H^k \subset f'(x) \cdot H.$$

This can be determined with **Newton-polygon** techniques.

## Remark

Concerning the Somos-4 sequence, since $P_n \in \mathbb{Z}[X_0^{\pm 1}, X_1^{\pm 1}, X_2^{\pm 1}, X_3^{\pm 1}]$, all the coefficients of $\frac{1}{k!} f^{(k)}(x)$ are in $\mathbb{Z}$.

# Higher differentials

## What is **small enough**

How can we determine when the lemma applies ?
When $f$ is locally analytic, it essentially corresponds to

$$\sum_{k=2}^{+\infty} \frac{1}{k!} f^{(k)}(x) \cdot H^k \subset f'(x) \cdot H.$$

This can be determined with **Newton-polygon** techniques.

## Remark

Concerning the Somos-4 sequence, since $P_n \in \mathbb{Z}[X_0^{\pm 1}, X_1^{\pm 1}, X_2^{\pm 1}, X_3^{\pm 1}]$, all the coefficients of $\frac{1}{k!} f^{(k)}(x)$ are in $\mathbb{Z}$.
As a consequence,

$$\frac{1}{k!} f^{(k)}(x) \cdot (p^m \mathbb{Z}_p)^k \subset p^m \mathbb{Z}_p.$$

# Table of contents

# Computation in SOMOS-4

## Loss in precision in SOMOS-4 with Sage ?!

$$x_0 = 1 + O(5^{20})$$
$$x_1 = 1 + O(5^{20})$$
$$x_2 = 1 + O(5^{20})$$
$$x_3 = -1 + 5 + O(5^{20})$$

# Computation in SOMOS-4

## Loss in precision in SOMOS-4 with Sage ?!

$$x_0 = 1 + O(5^{20})$$
$$x_1 = 1 + O(5^{20})$$
$$x_2 = 1 + O(5^{20})$$
$$x_3 = -1 + 5 + O(5^{20})$$
$$x_4 = 4 * 5 + \cdots + O(5^{20})$$

# Computation in SOMOS-4

## Loss in precision in SOMOS-4 with Sage ?!

$$x_0 = 1 + O(5^{20})$$
$$x_1 = 1 + O(5^{20})$$
$$x_2 = 1 + O(5^{20})$$
$$x_3 = -1 + 5 + O(5^{20})$$
$$x_4 = 4 * 5 + \cdots + O(5^{20})$$
$$x_8 = 4 + \cdots + O(5^{19})$$

# Computation in SOMOS-4

## Loss in precision in SOMOS-4 with Sage ?!

$$
\begin{aligned}
x_0 &= 1 + O(5^{20}) \\
x_1 &= 1 + O(5^{20}) \\
x_2 &= 1 + O(5^{20}) \\
x_3 &= -1 + 5 + O(5^{20}) \\
x_4 &= 4 * 5 + \cdots + O(5^{20}) \\
x_8 &= 4 + \cdots + O(5^{19}) \\
x_{40} &= 4 + \cdots + O(5^{13})
\end{aligned}
$$

# Computation in SOMOS-4

## Loss in precision in SOMOS-4 with Sage ?!

$$
\begin{aligned}
x_0 &= 1 + O(5^{20}) \\
x_1 &= 1 + O(5^{20}) \\
x_2 &= 1 + O(5^{20}) \\
x_3 &= -1 + 5 + O(5^{20}) \\
x_4 &= 4 * 5 + \cdots + O(5^{20}) \\
x_8 &= 4 + \cdots + O(5^{19}) \\
x_{40} &= 4 + \cdots + O(5^{13})
\end{aligned}
$$

## An explanation

The **gain** in precision in $x_8$ is invisible.

# Table of contents

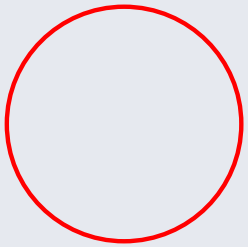
# More on the differential method

## Differential tracking of precision

$x + O(p^N)$

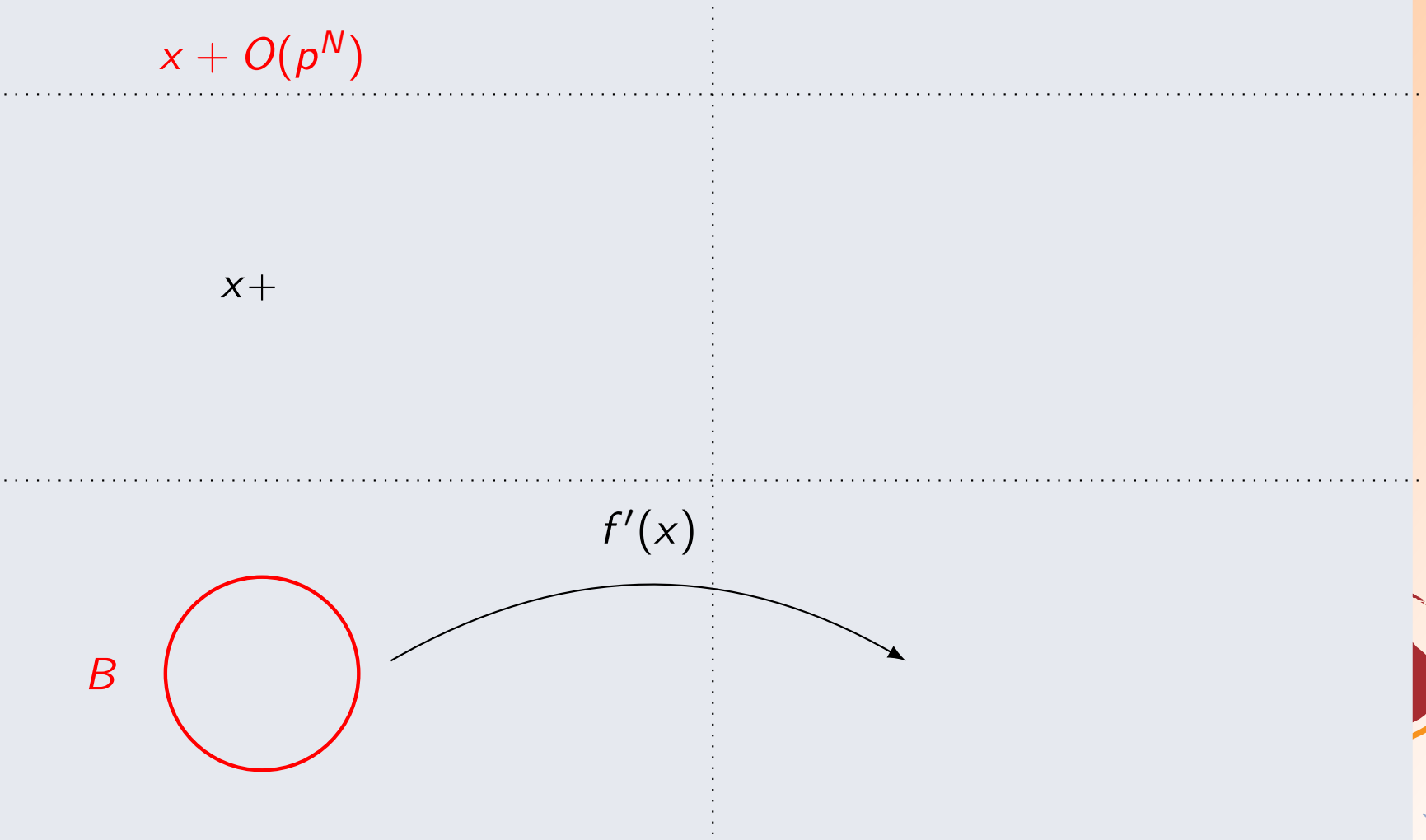
$x+$

$B$



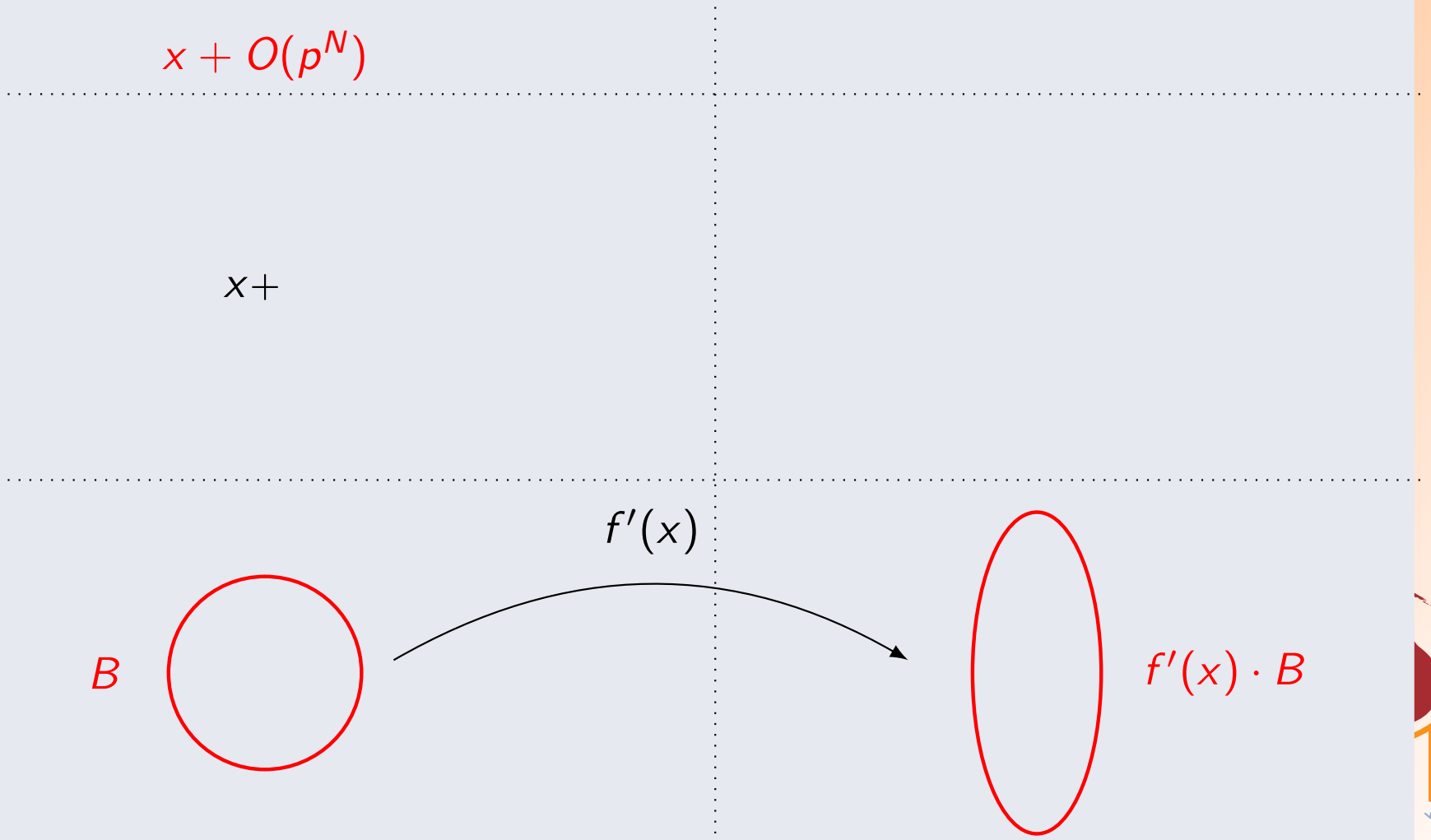
# More on the differential method

## Differential tracking of precision



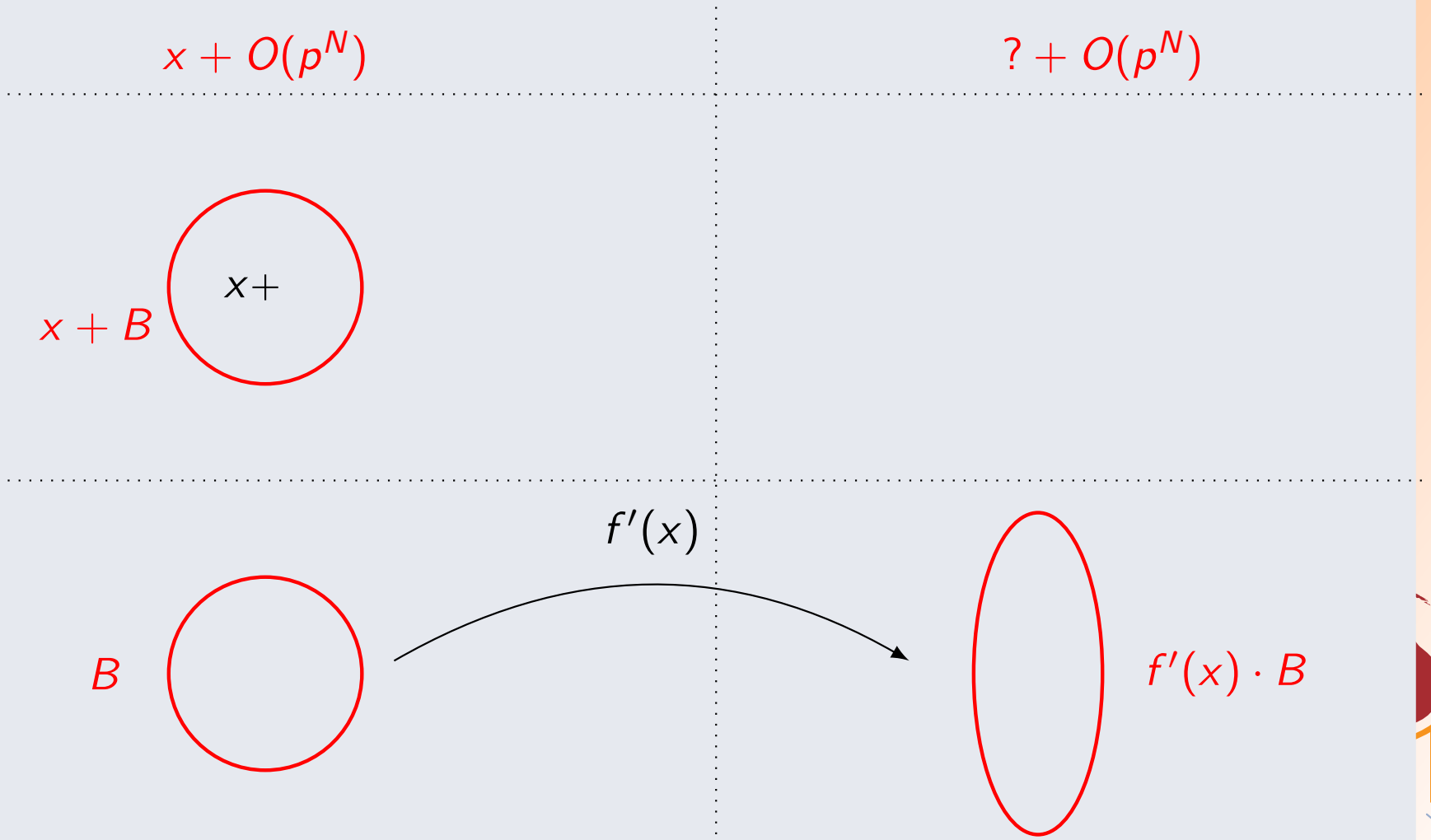
# More on the differential method

## Differential tracking of precision



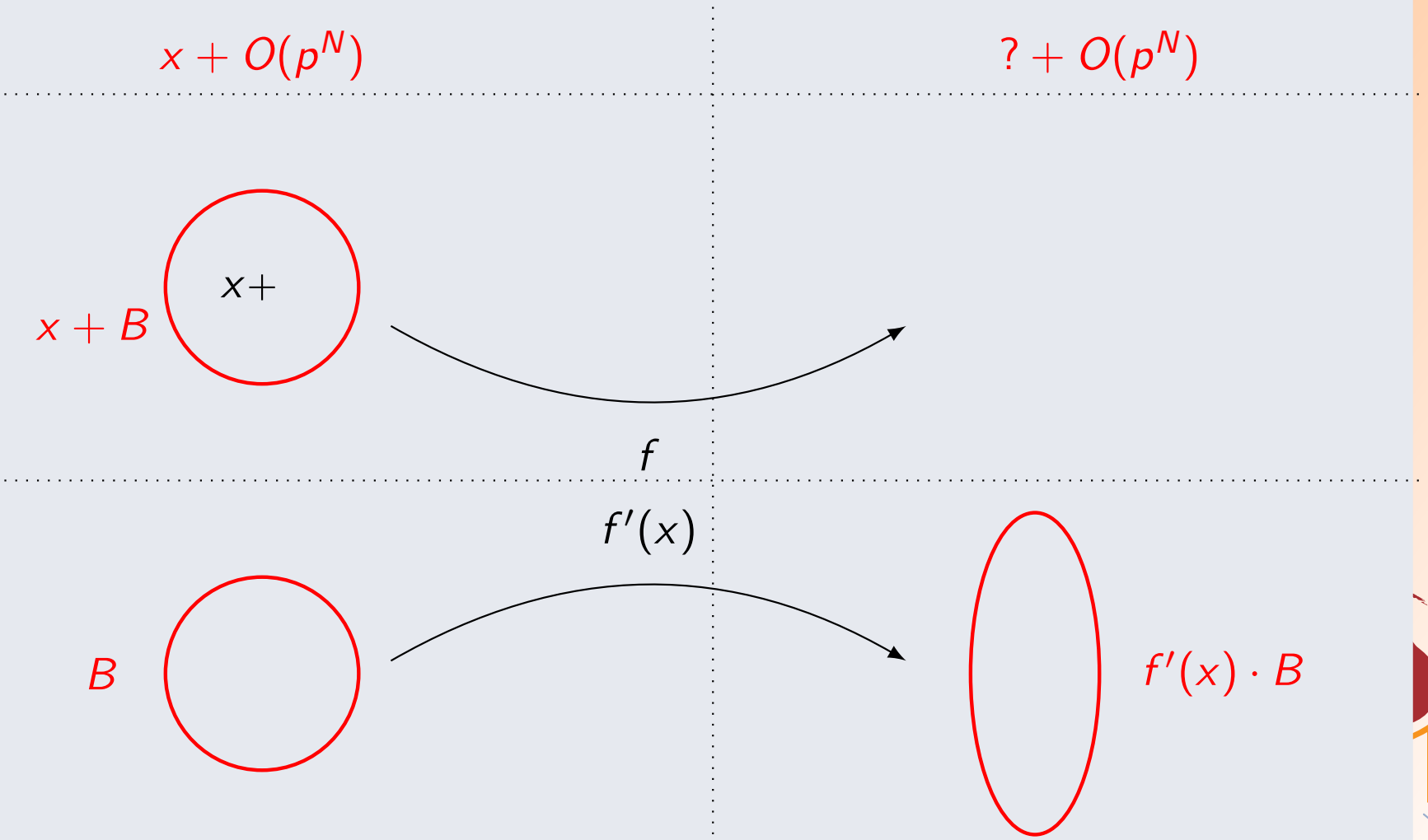
# More on the differential method

## Differential tracking of precision



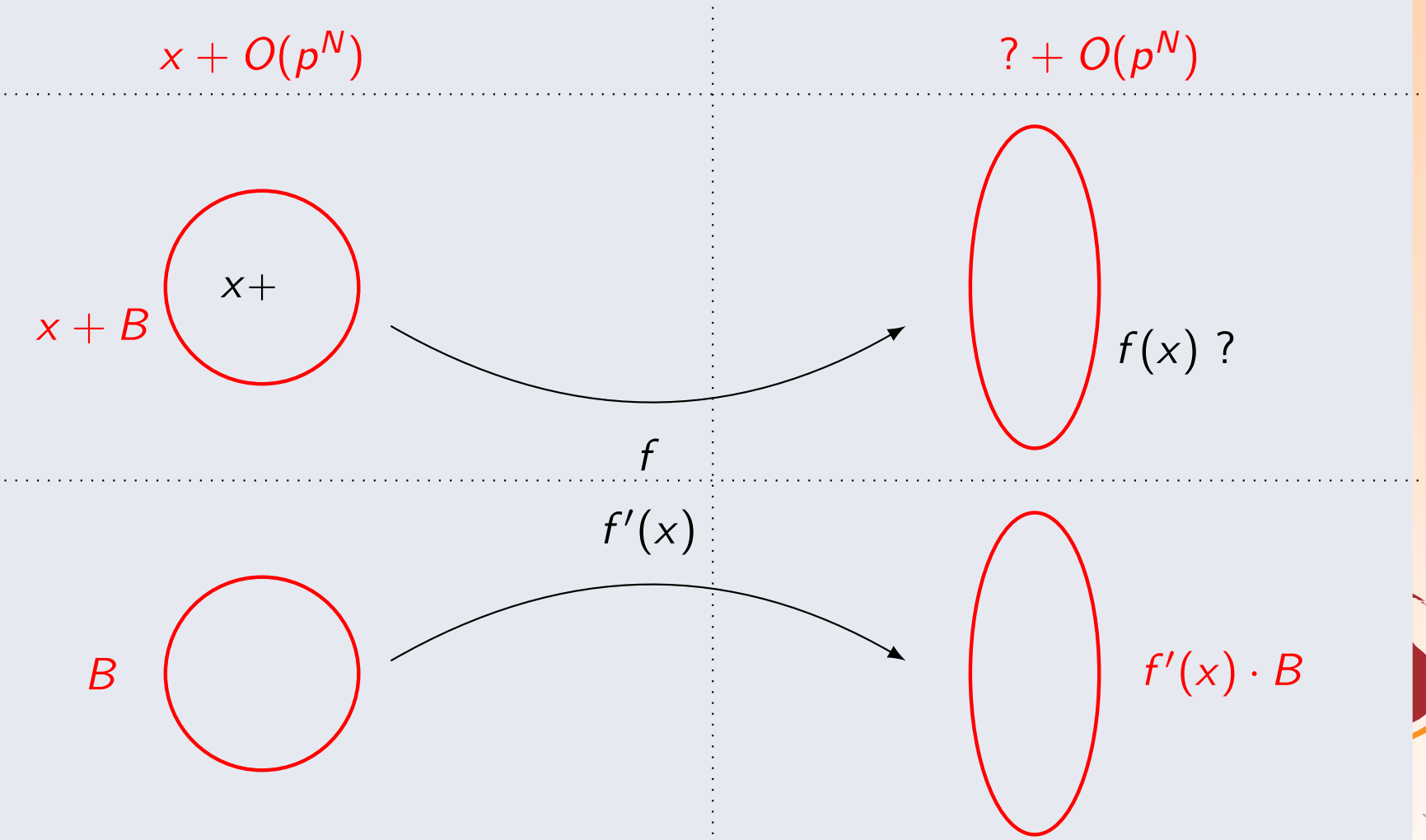
# More on the differential method

## Differential tracking of precision



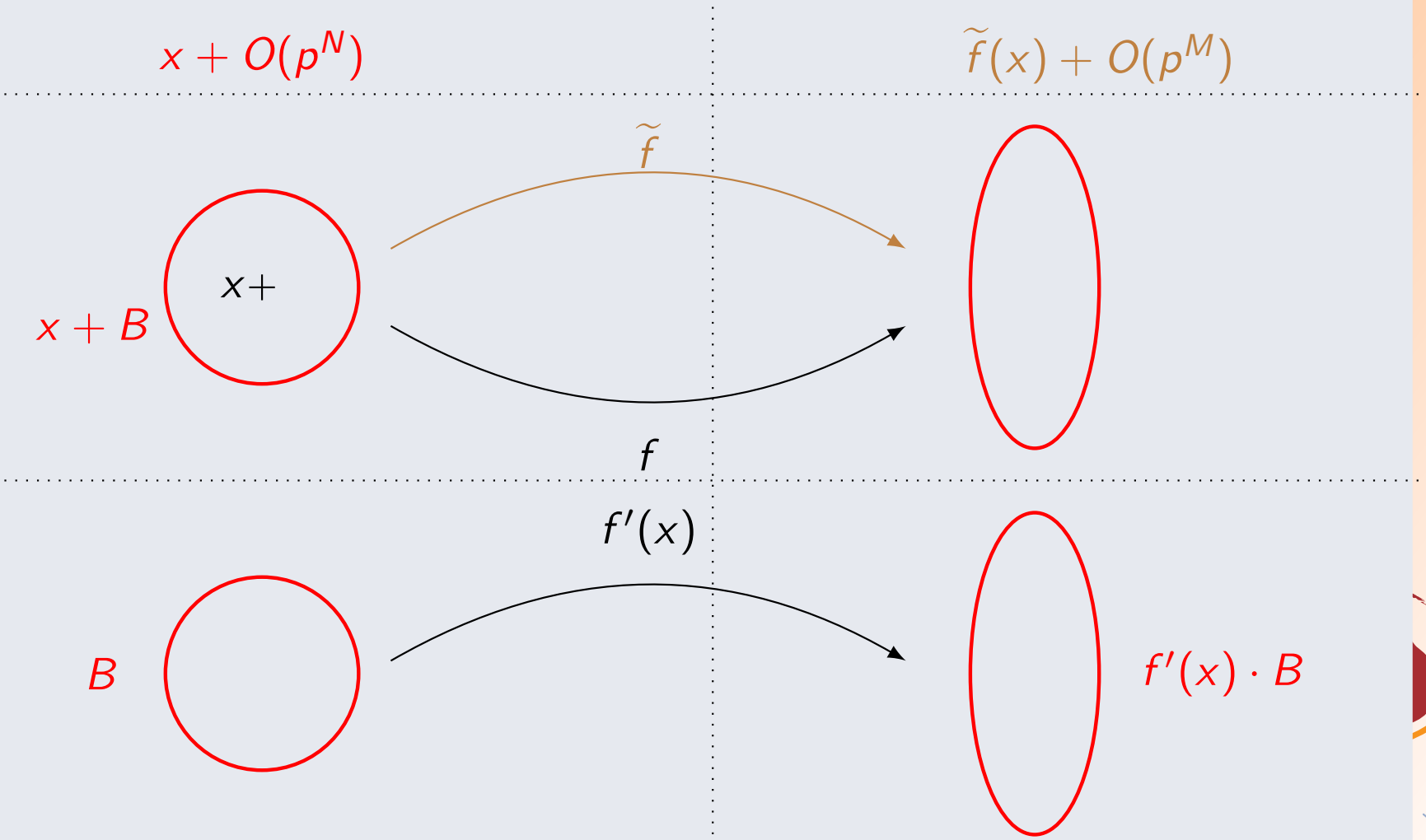
# More on the differential method

## Differential tracking of precision



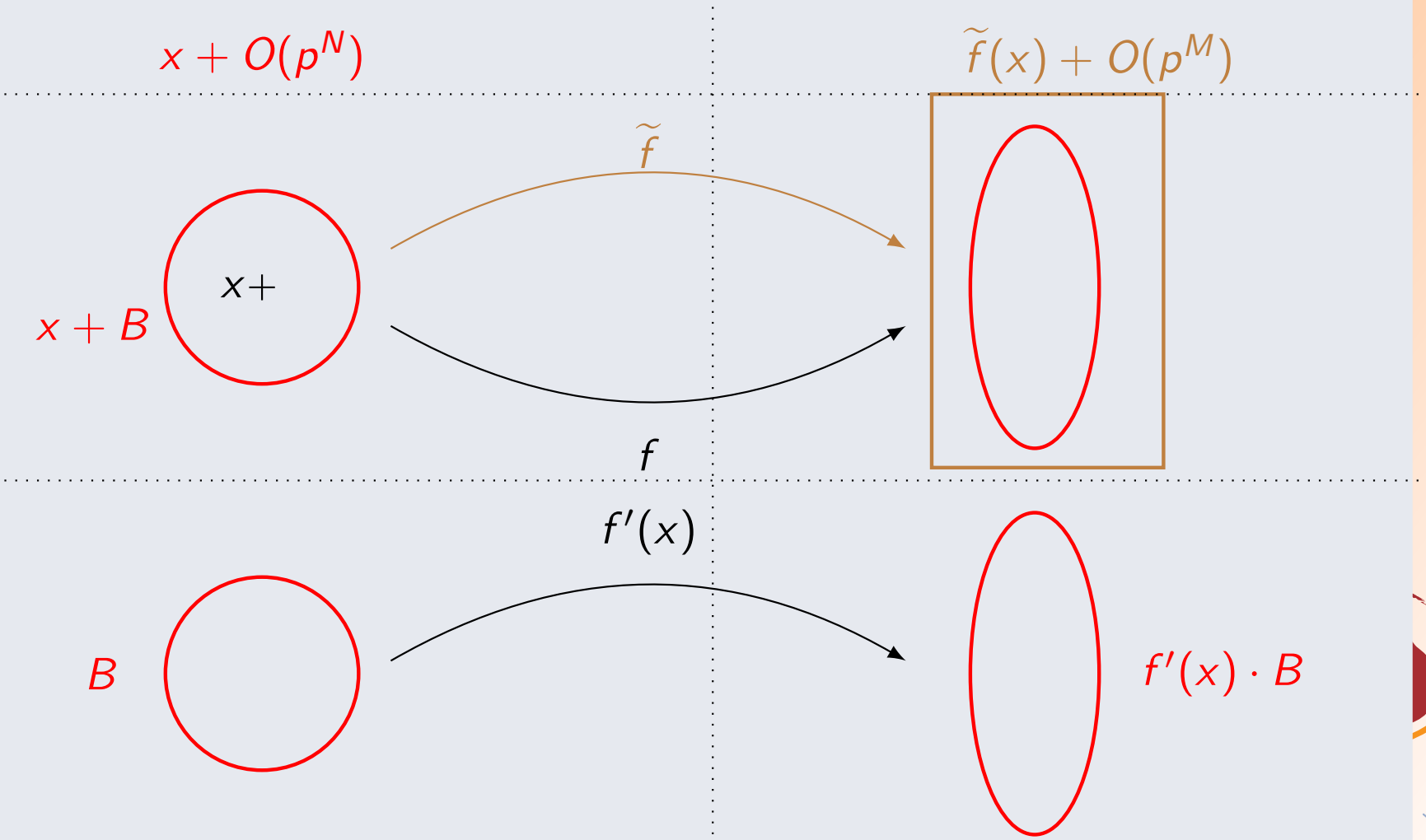
# More on the differential method

## Differential tracking of precision



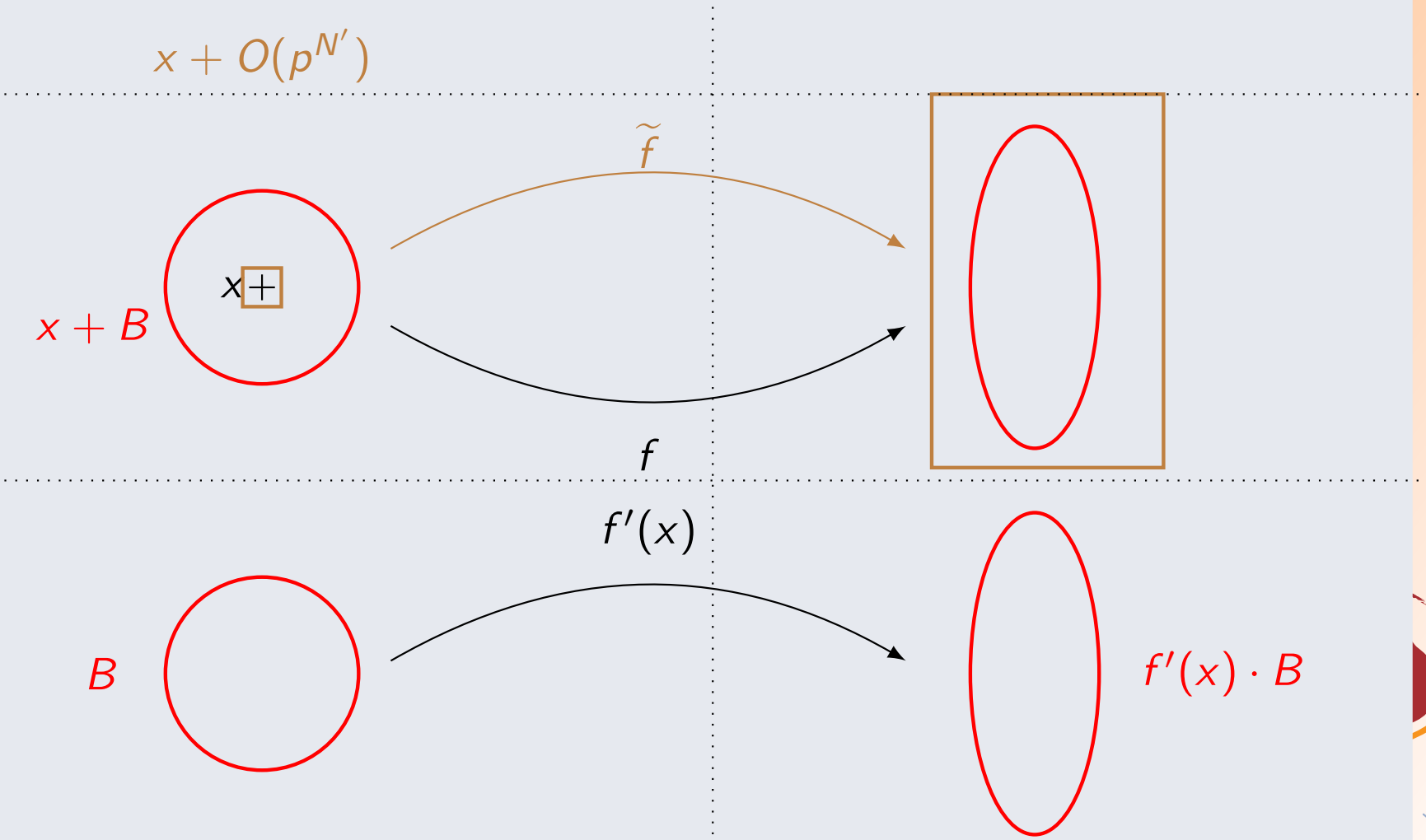
# More on the differential method

## Differential tracking of precision



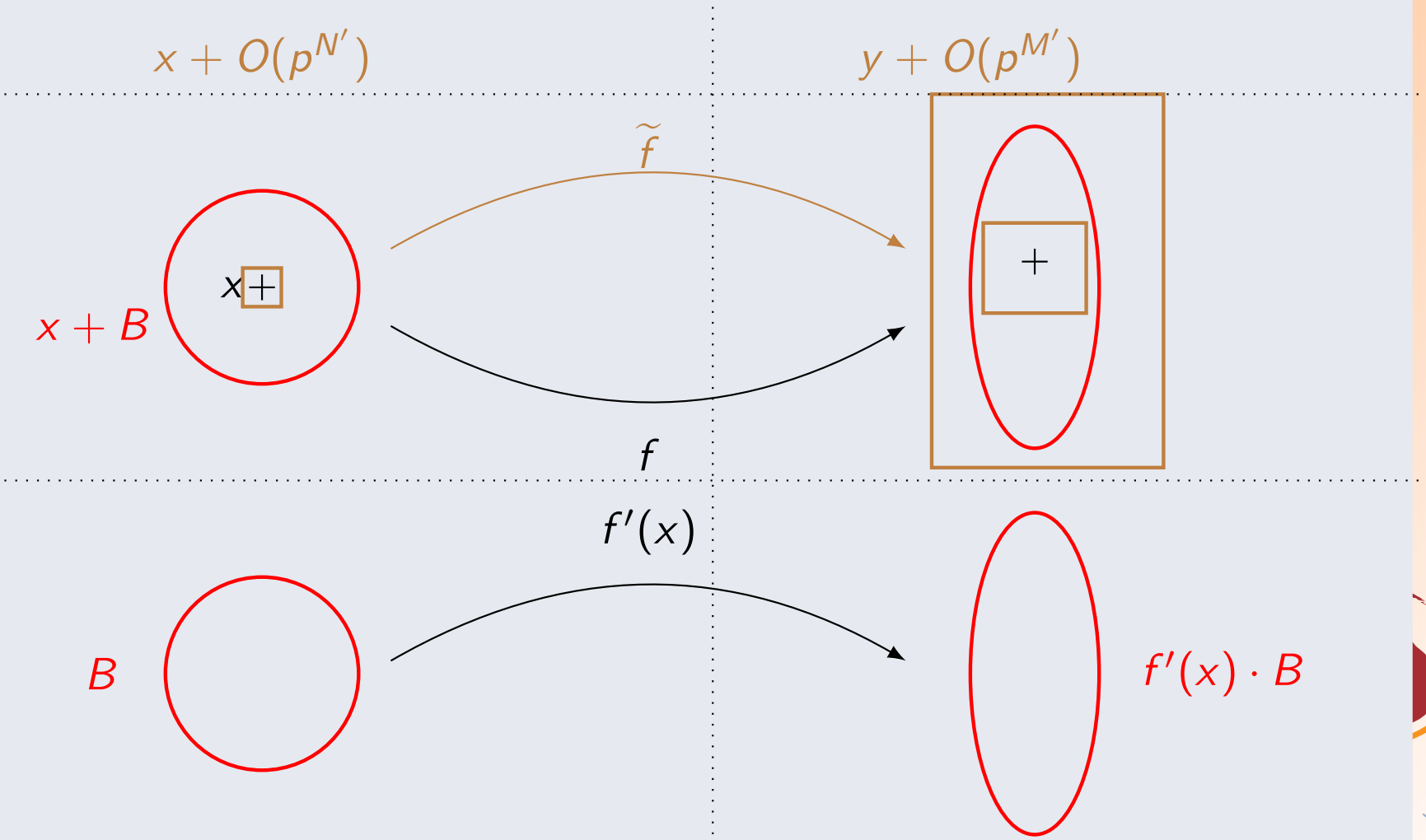
# More on the differential method

## Differential tracking of precision



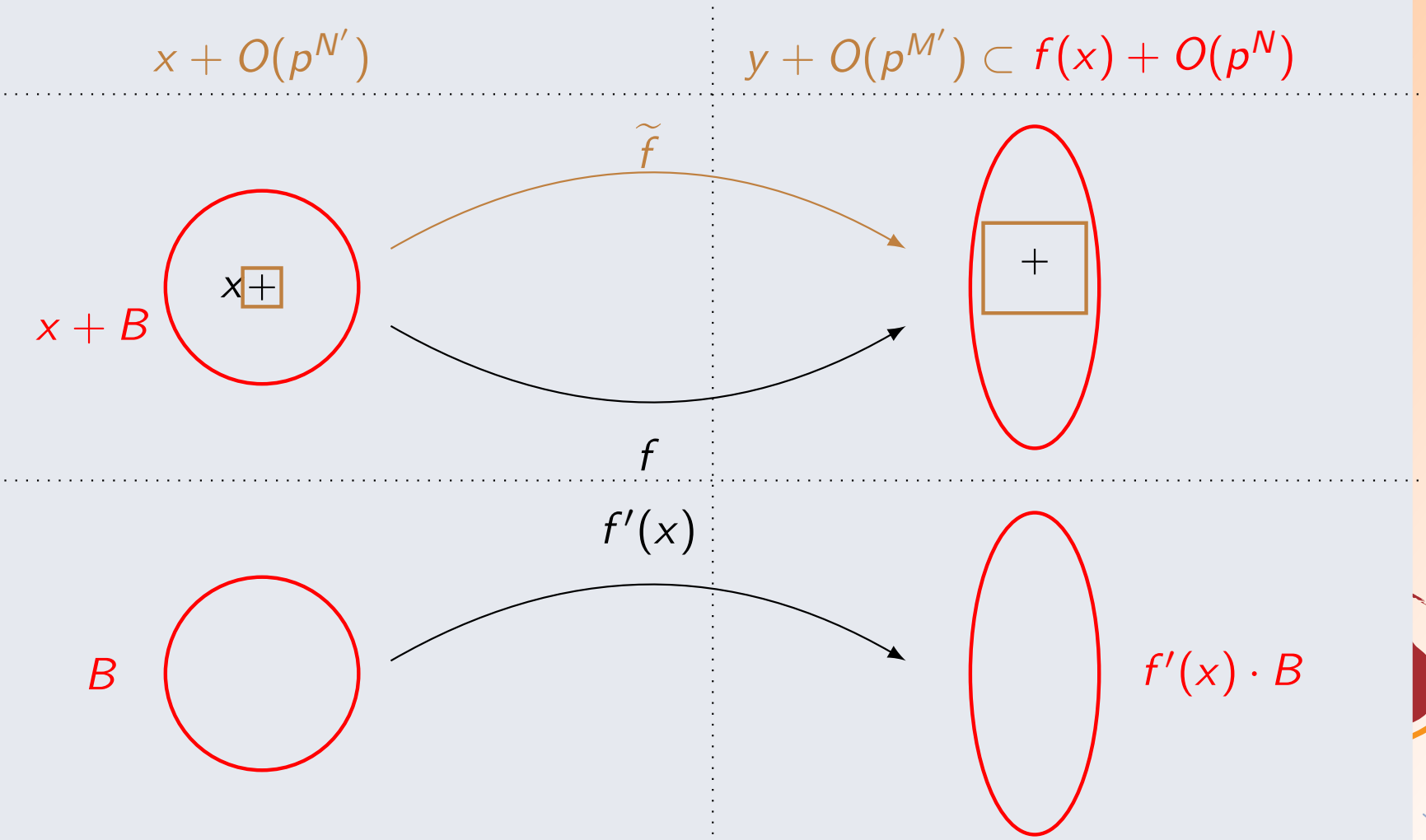
# More on the differential method

## Differential tracking of precision



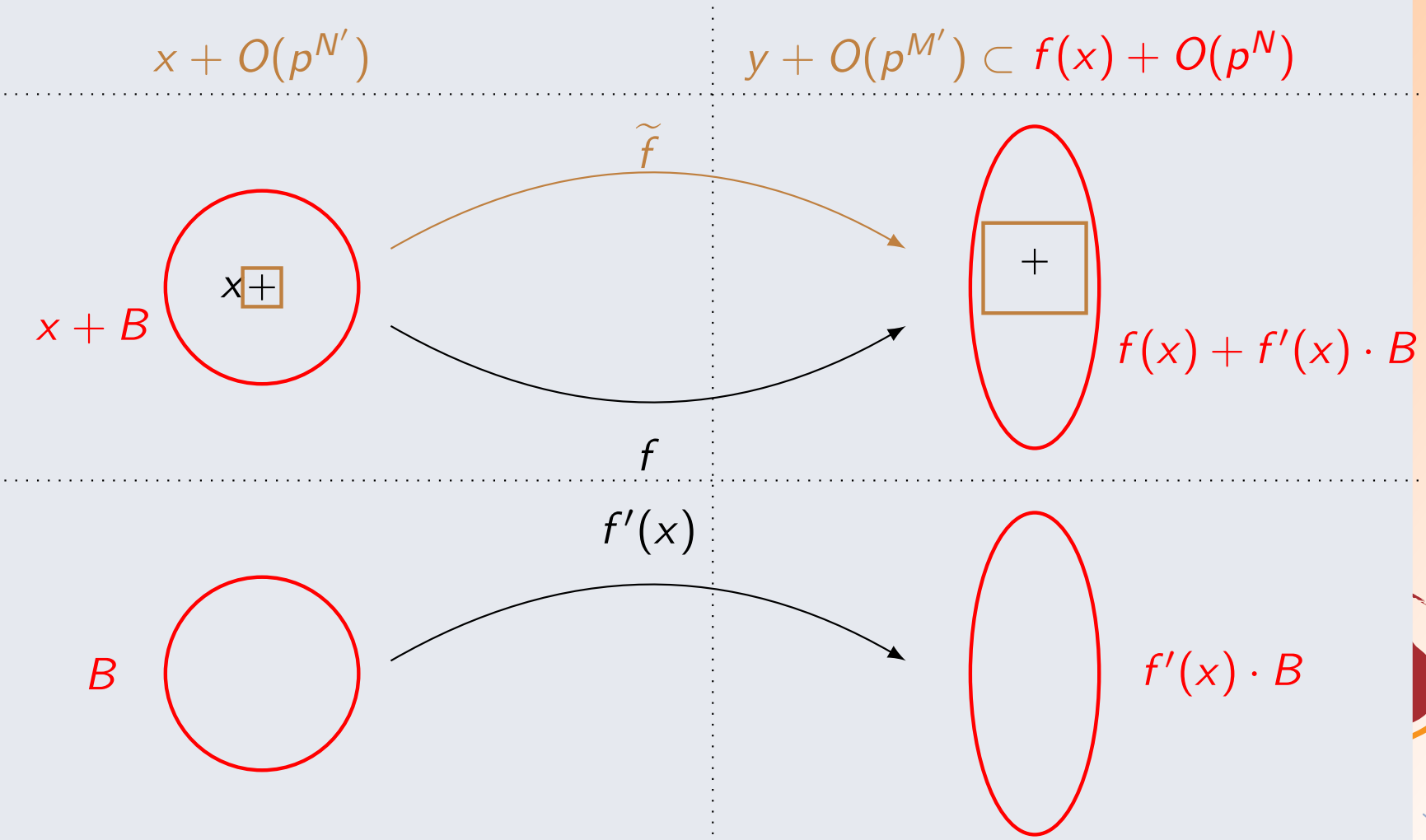
# More on the differential method

## Differential tracking of precision



# More on the differential method

## Differential tracking of precision

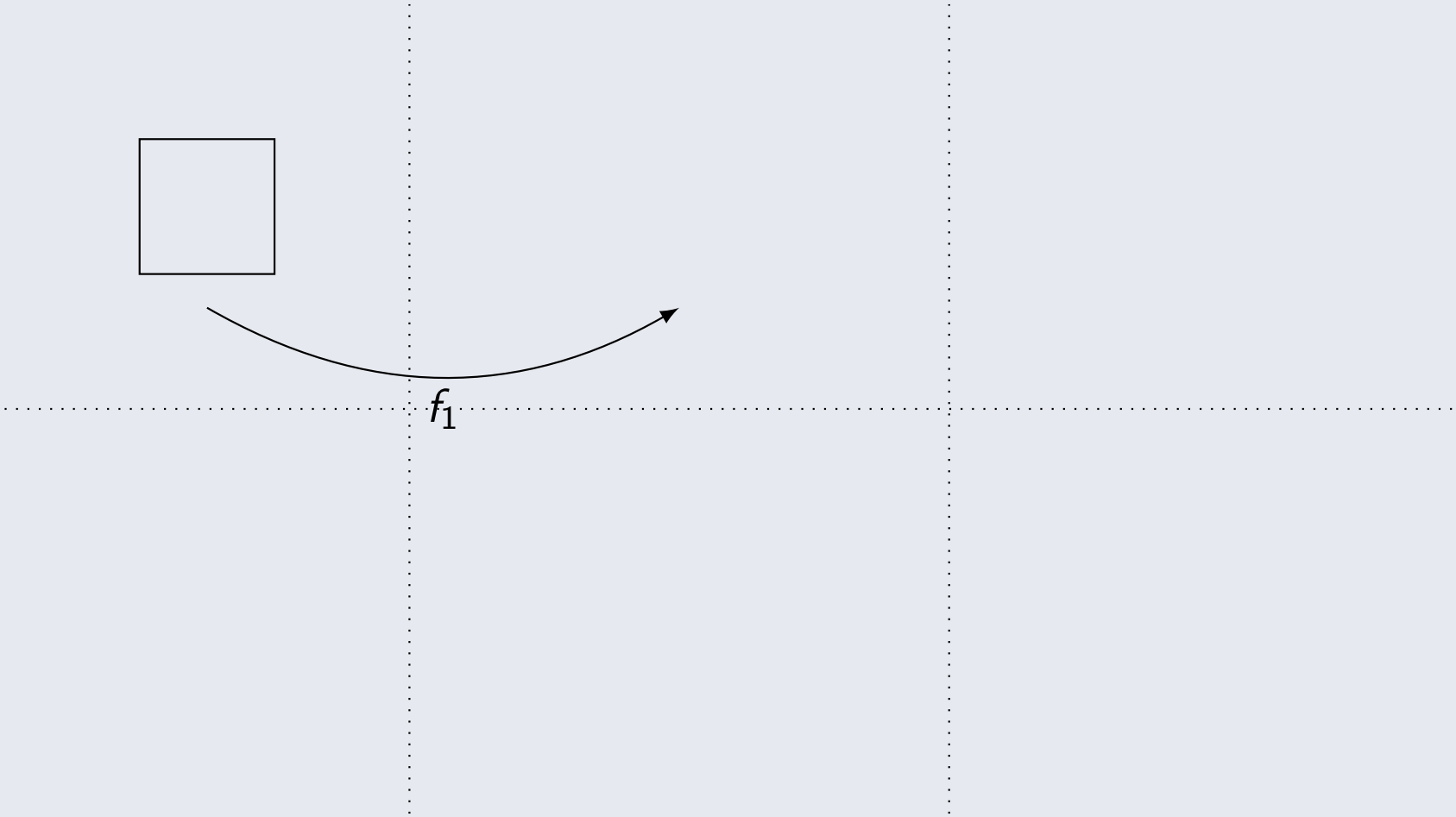


# Lifting techniques

## Methods comparison

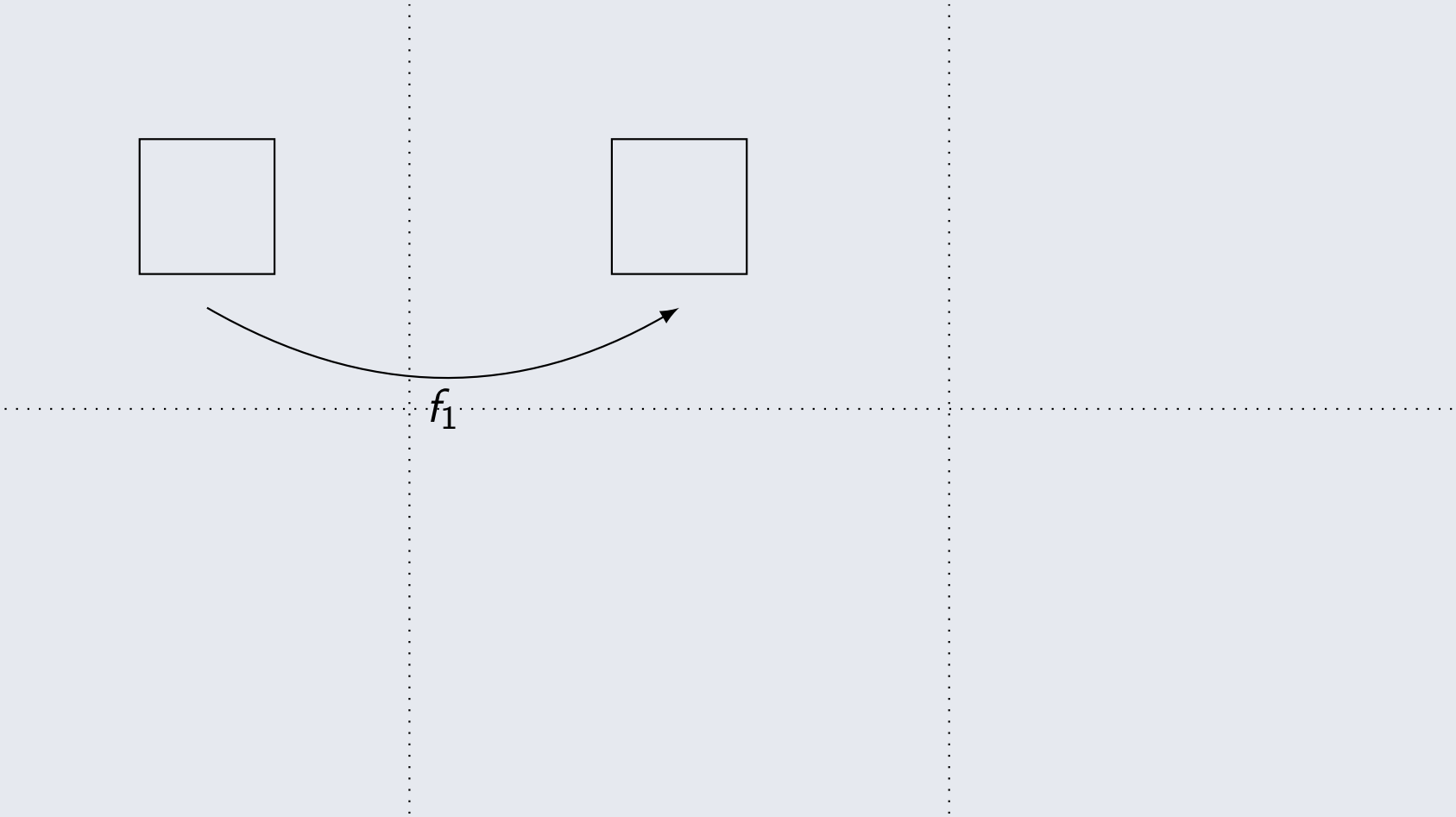
# Lifting techniques

## Methods comparison



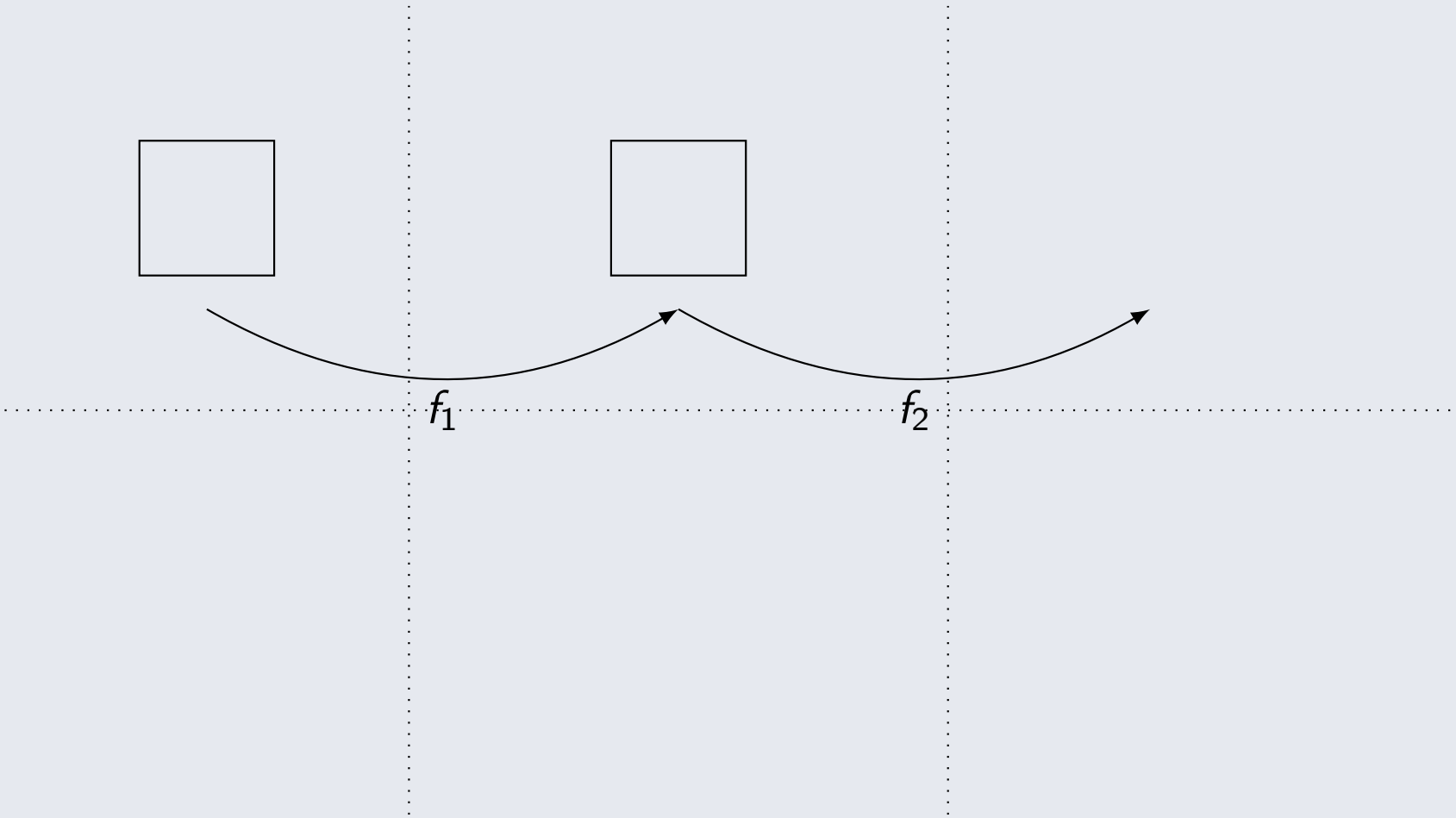
# Lifting techniques

## Methods comparison



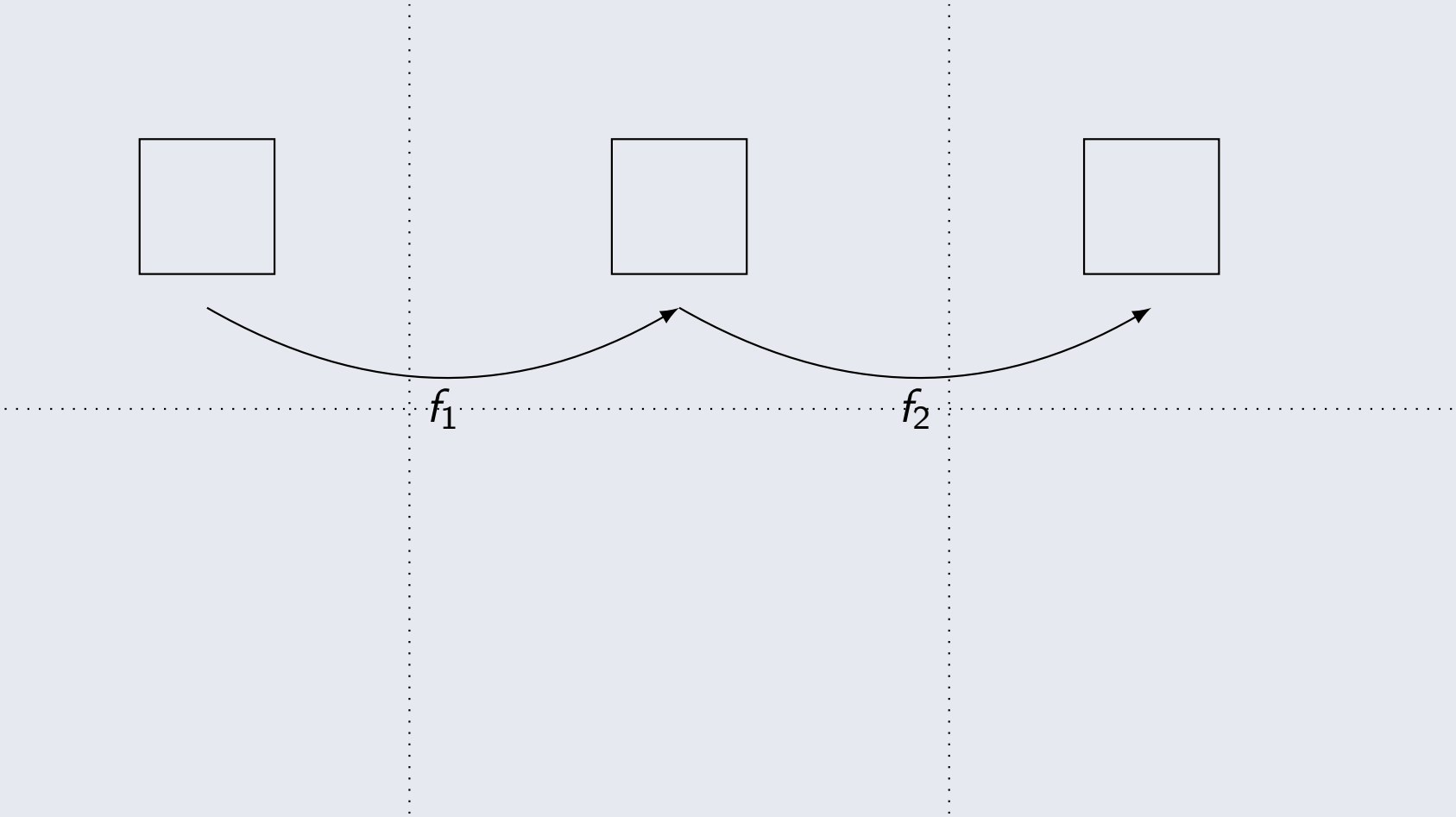
# Lifting techniques

## Methods comparison



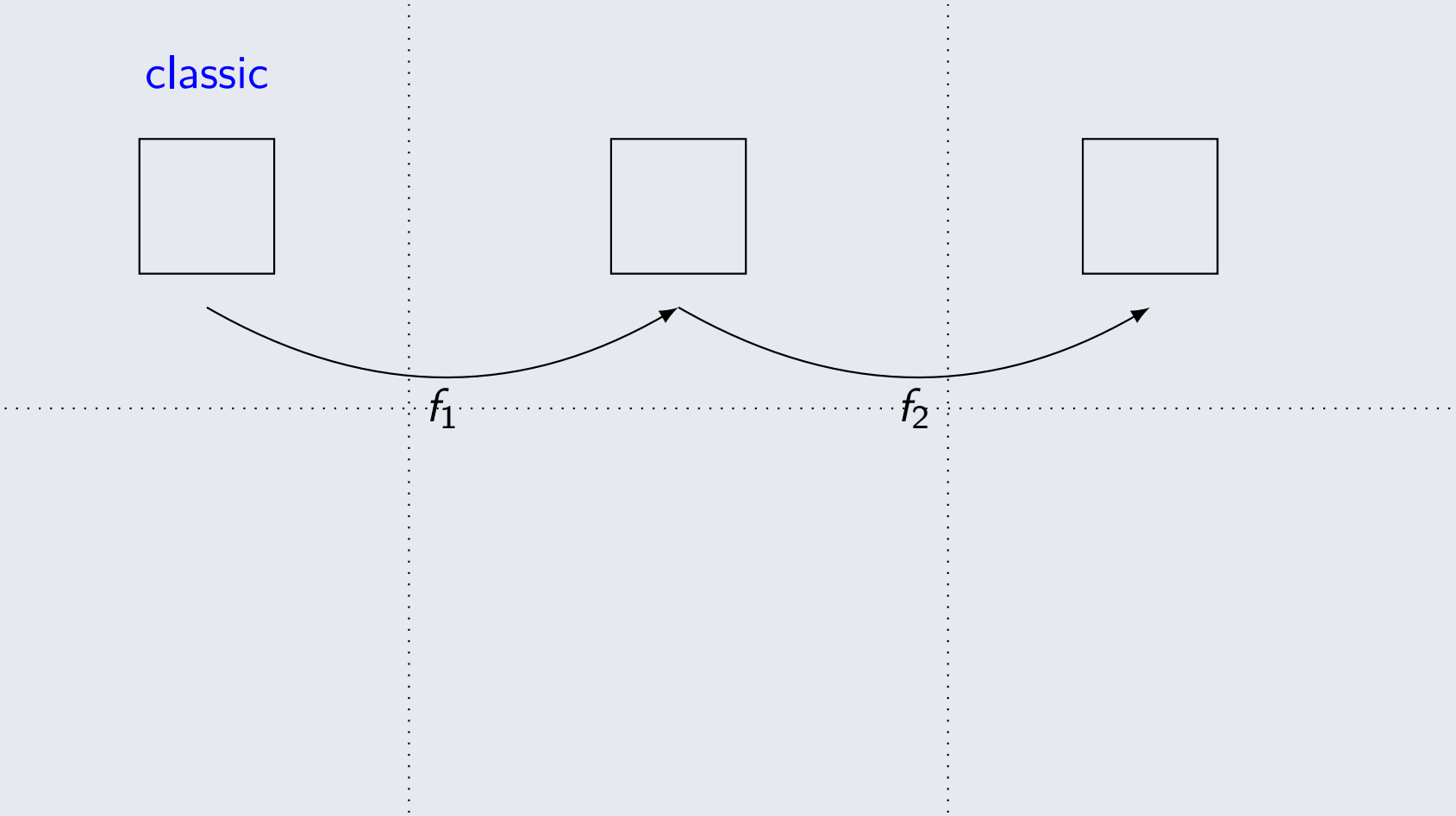
# Lifting techniques

## Methods comparison



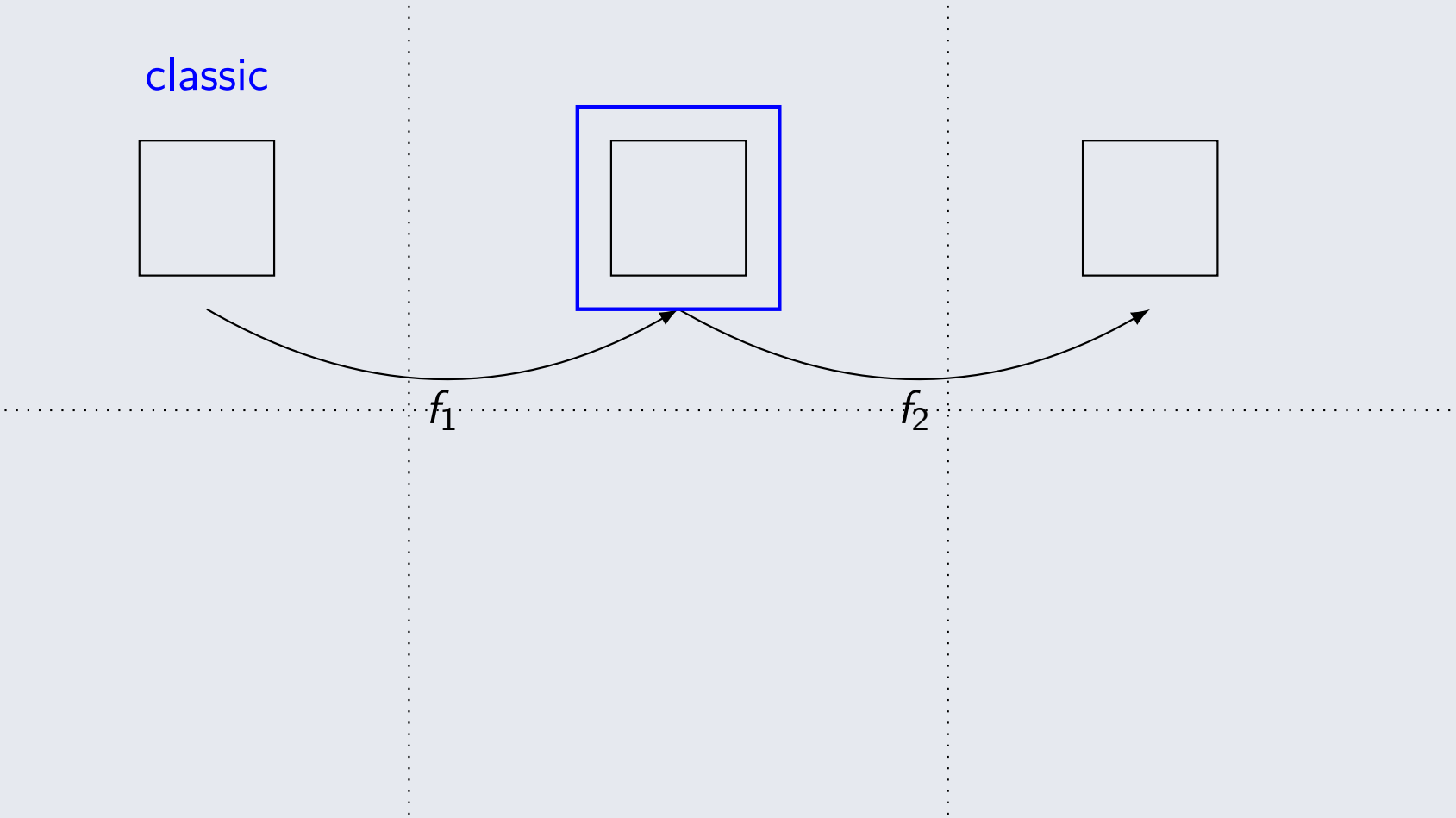
# Lifting techniques

## Methods comparison



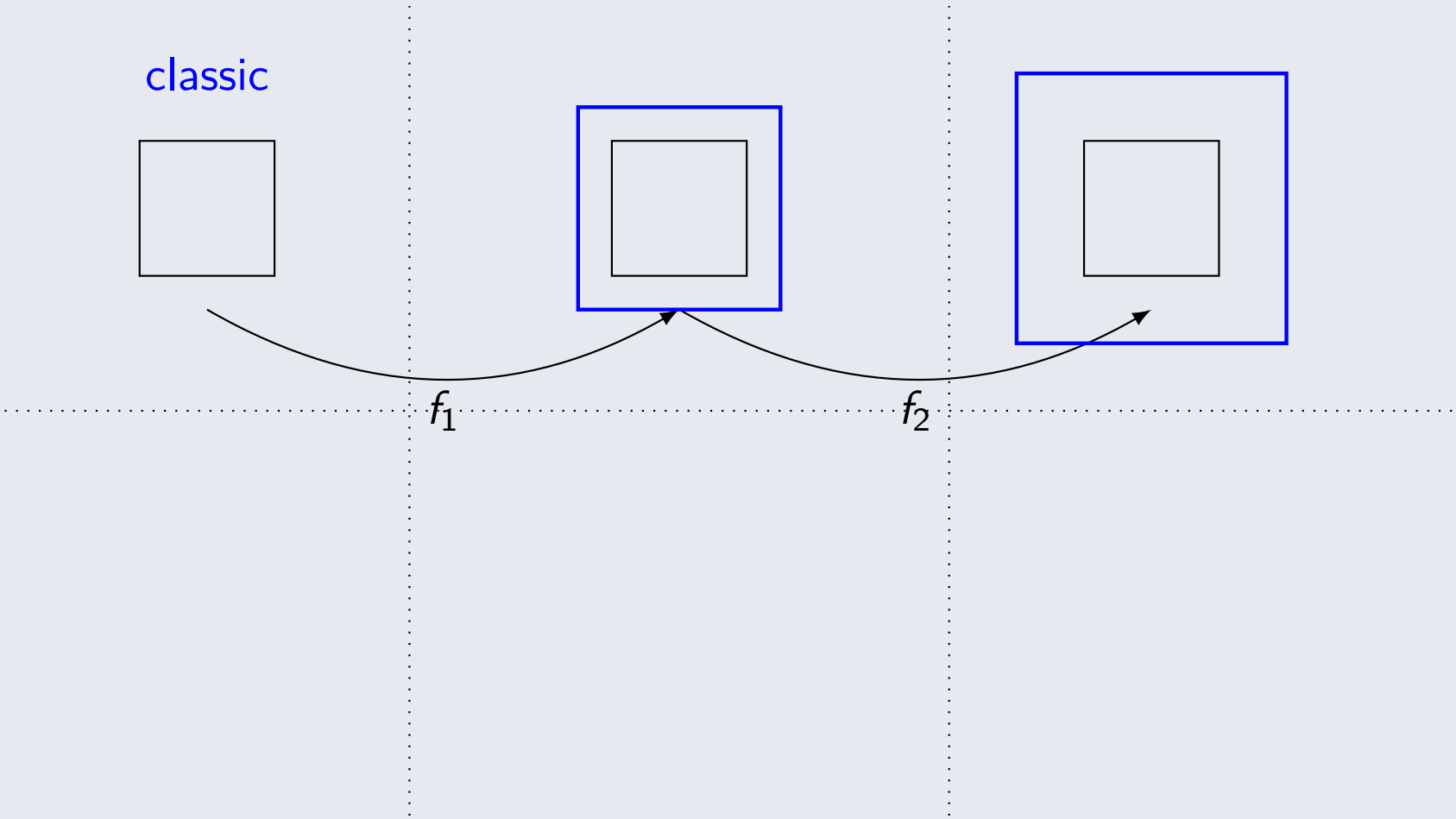
# Lifting techniques

## Methods comparison



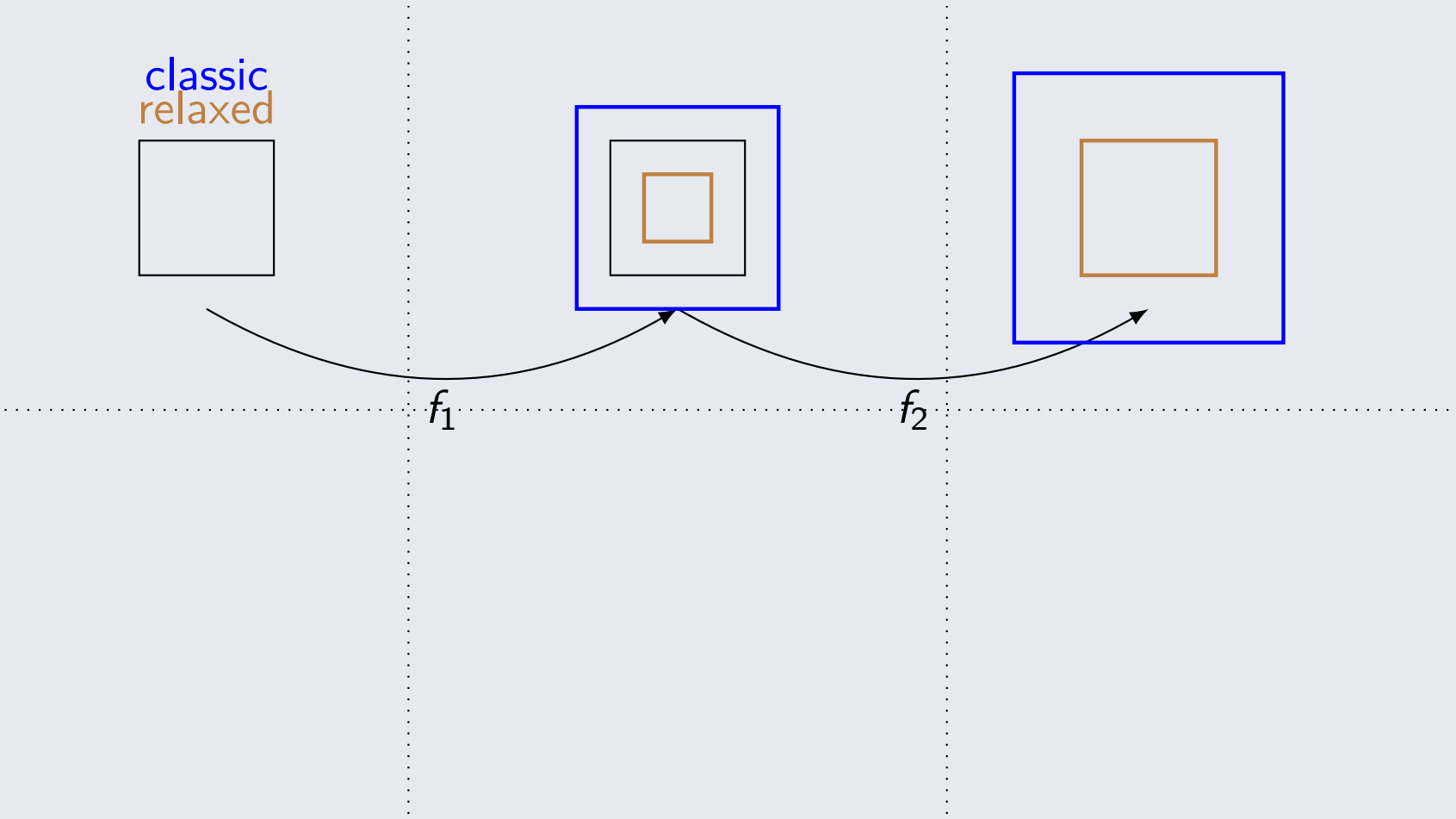
# Lifting techniques

## Methods comparison



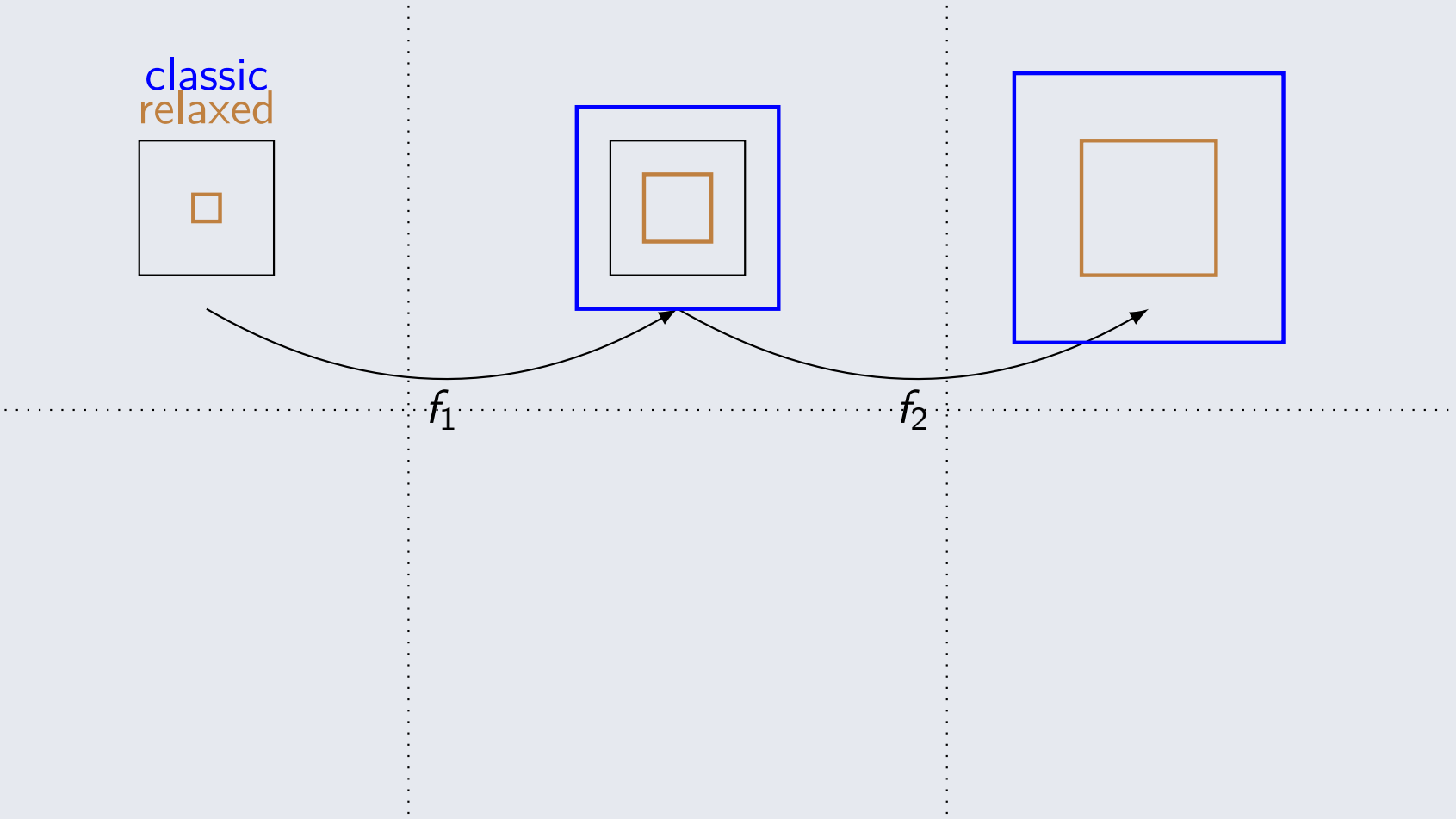
# Lifting techniques

## Methods comparison



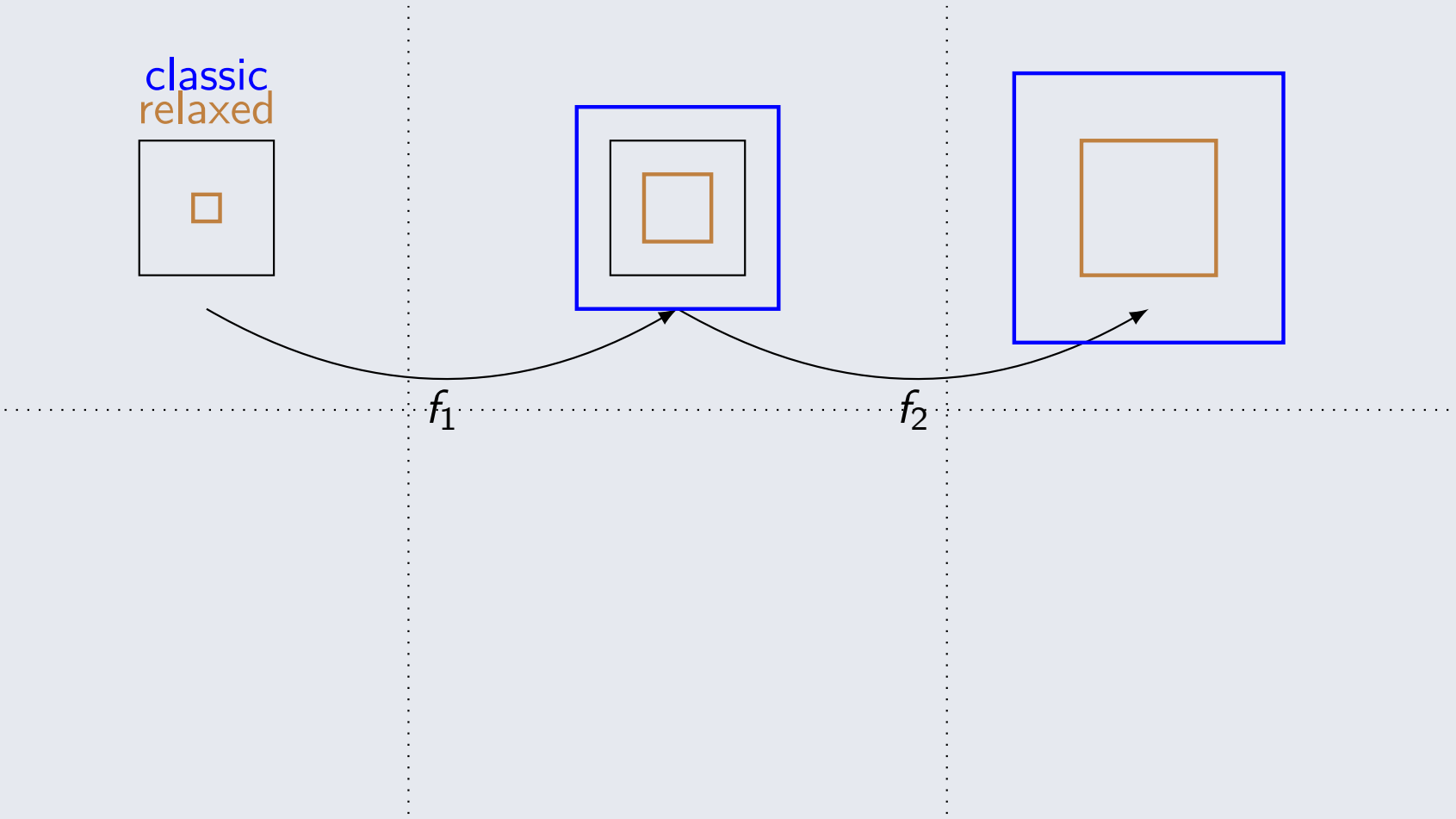
# Lifting techniques

## Methods comparison



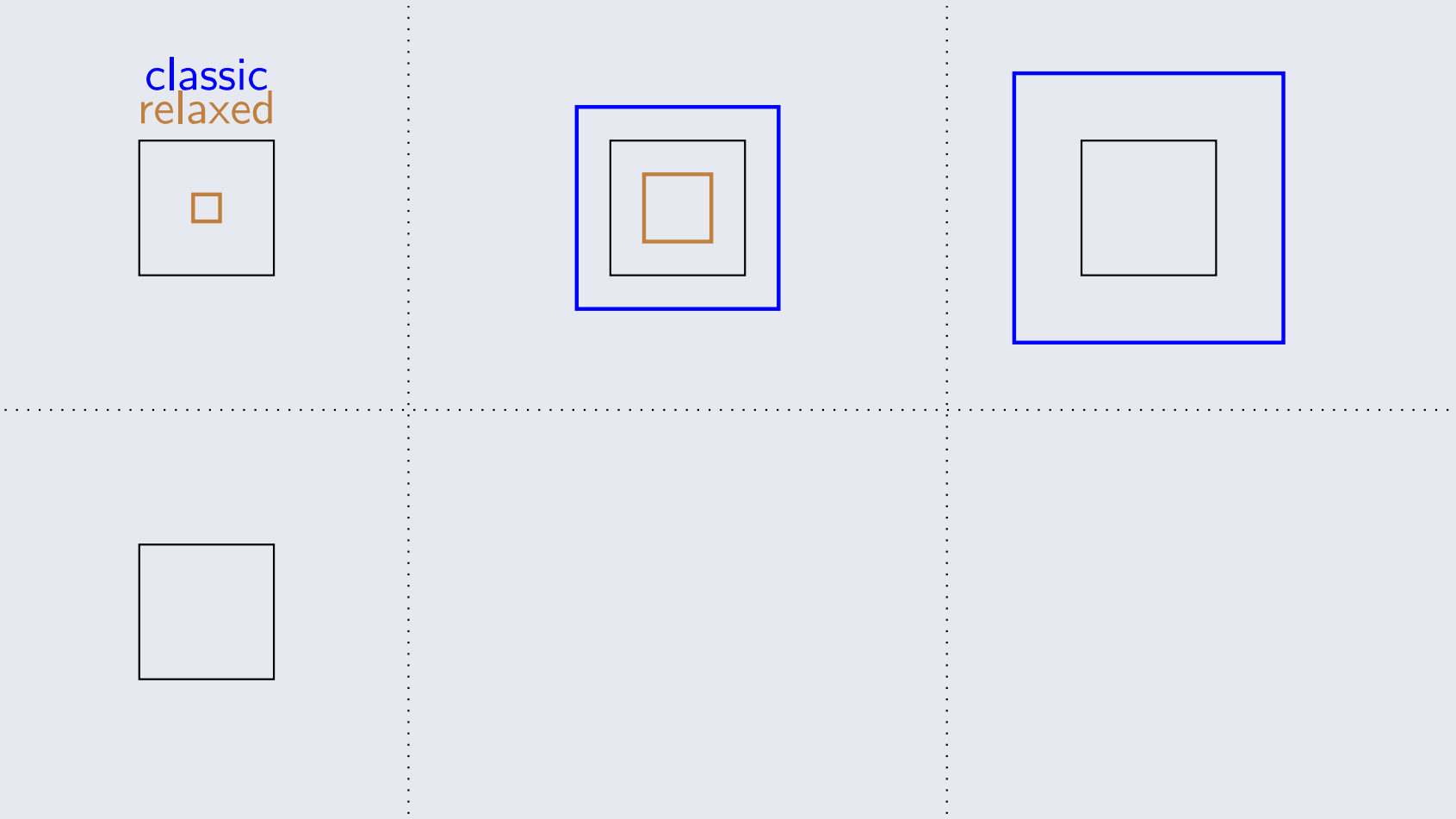
# Lifting techniques

## Methods comparison



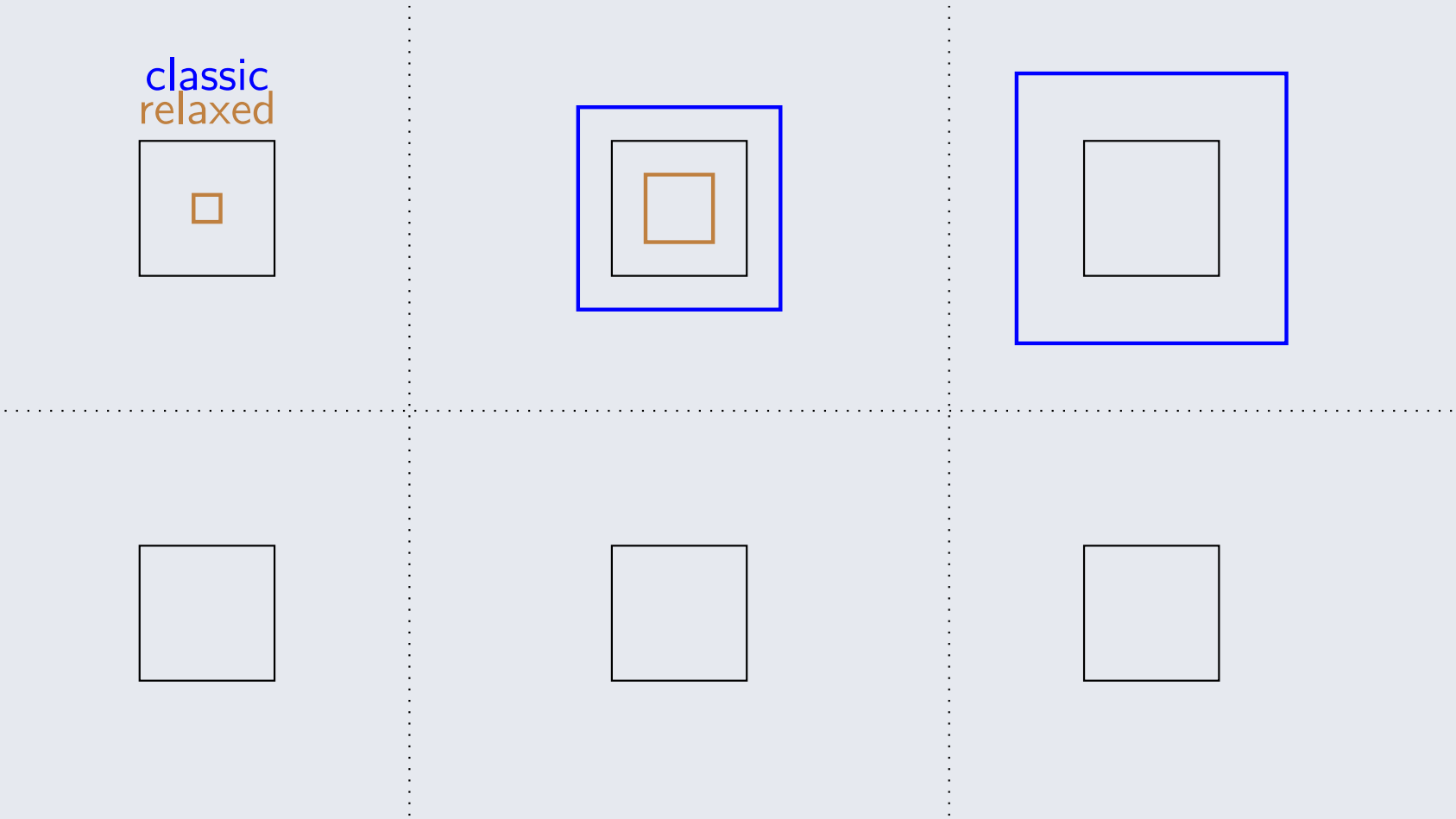
# Lifting techniques

## Methods comparison



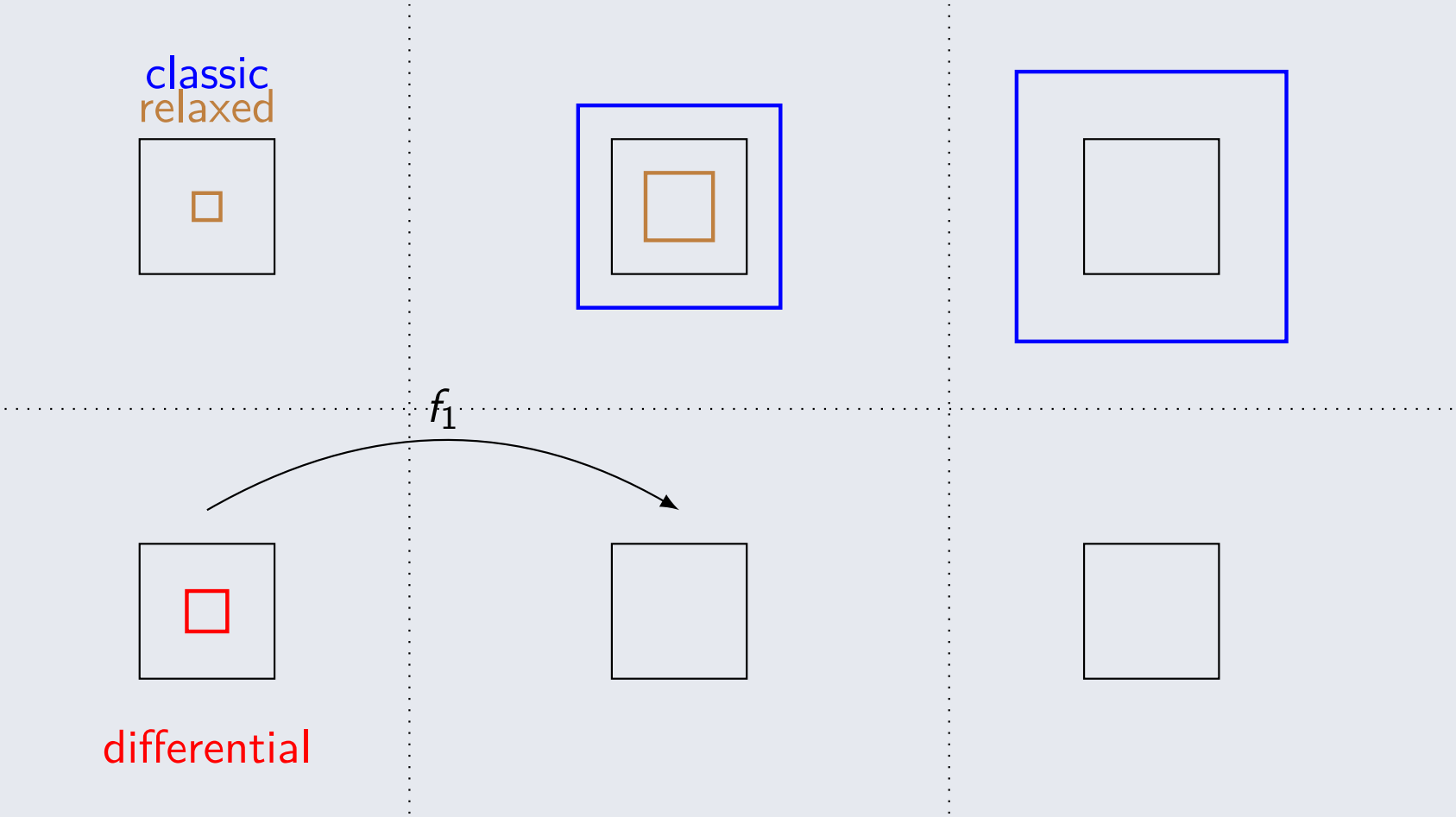
# Lifting techniques

## Methods comparison



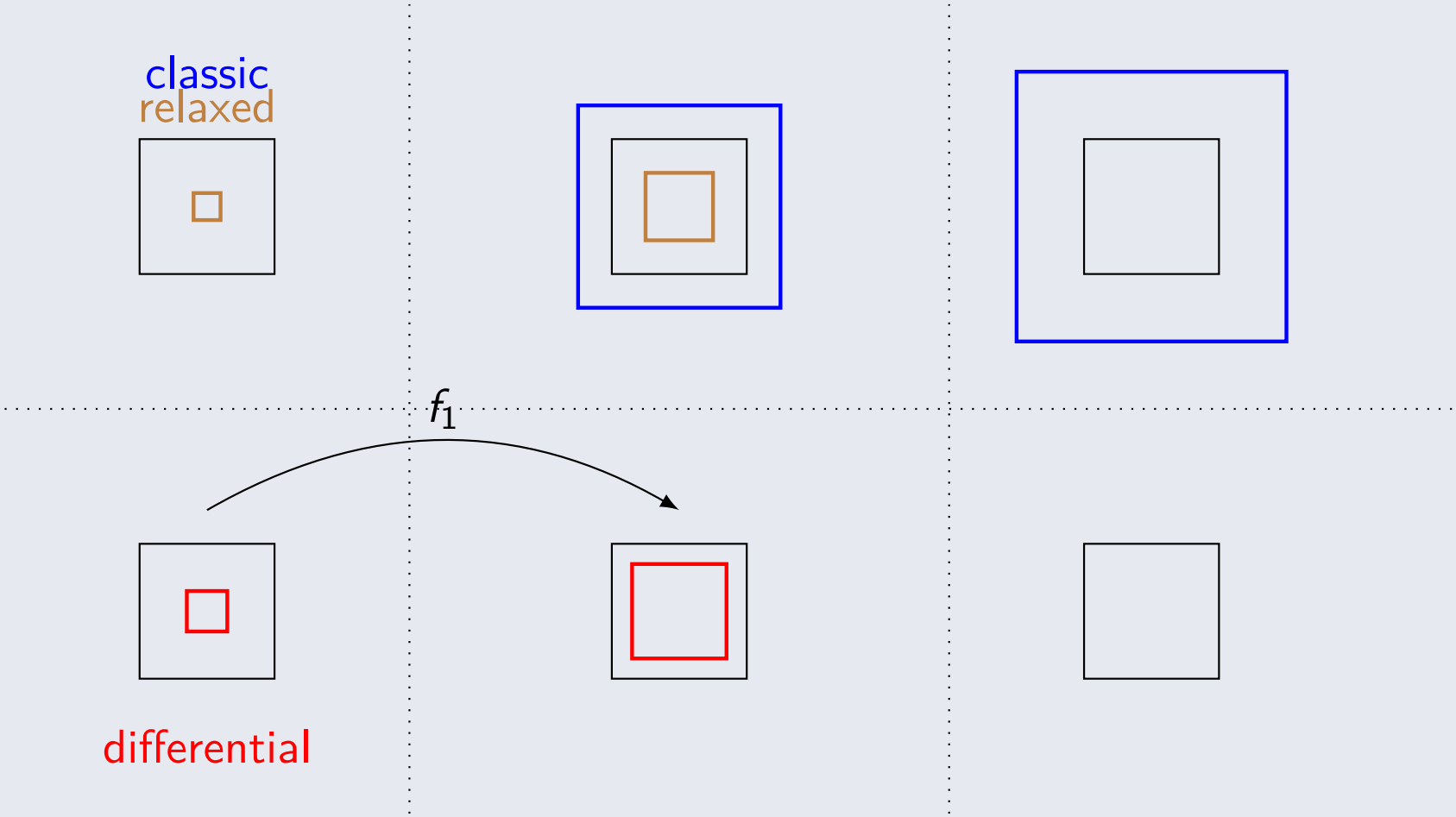
# Lifting techniques

## Methods comparison



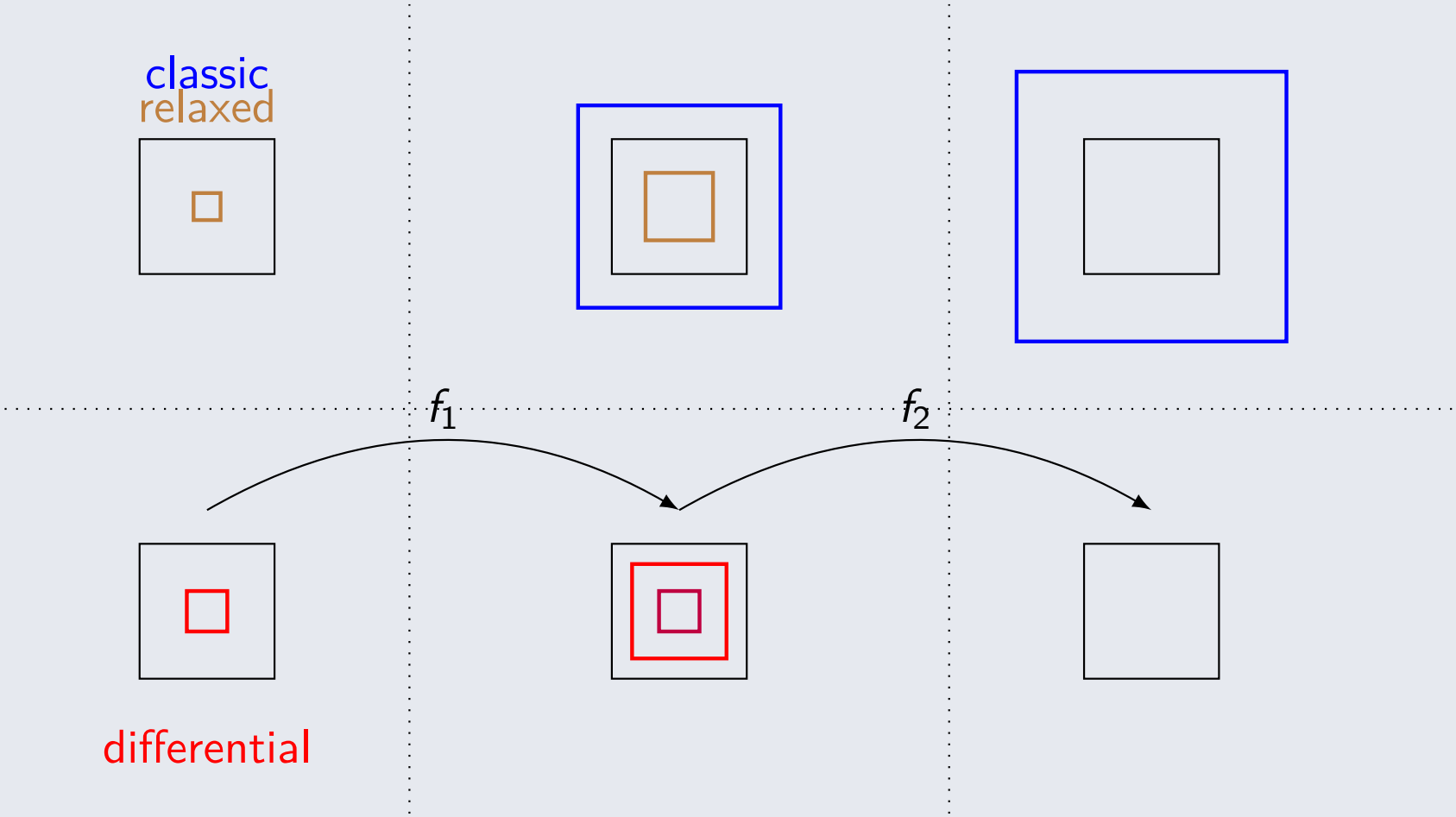
# Lifting techniques

## Methods comparison



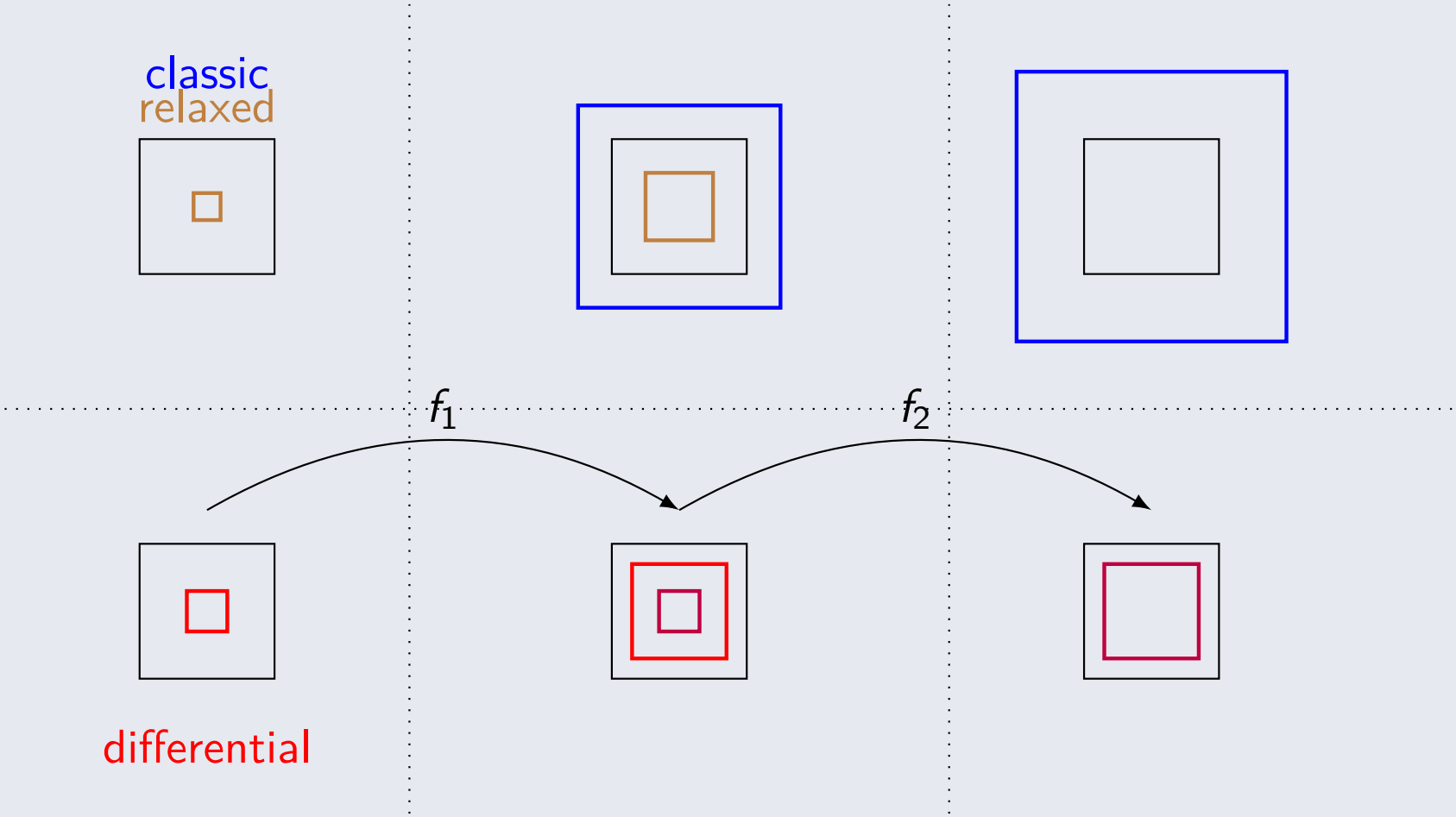
# Lifting techniques

## Methods comparison



# Lifting techniques

## Methods comparison



# Table of contents

# Some calculus

## Differential of the euclidean division

Let $A, B \in \mathbb{Q}_p[X]$. We would like to differentiate $A = BQ + R$.

# Some calculus

## Differential of the euclidean division

Let $A, B \in \mathbb{Q}_p[X]$. We would like to differentiate $A = BQ + R$.
We can write $A + \delta A = (B + \delta B)(Q + \delta Q) + R + \delta R$.

# Some calculus

## Differential of the euclidean division

Let $A, B \in \mathbb{Q}_p[X]$. We would like to differentiate $A = BQ + R$.
We can write $A + \delta A = (B + \delta B)(Q + \delta Q) + R + \delta R$.
Then,

$$\delta A - Q\delta B = B\delta Q + \delta R.$$

# Some calculus

## Differential of the euclidean division

Let $A, B \in \mathbb{Q}_p[X]$. We would like to differentiate $A = BQ + R$.
We can write $A + \delta A = (B + \delta B)(Q + \delta Q) + R + \delta R$.
Then,

$$\delta A - Q\delta B = B\delta Q + \delta R.$$

Therefore, $\delta Q$ and $\delta R$ are determined by the division of $\delta A - Q\delta B$ by $B$.

# Table of contents

# About matrices

## Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

# About matrices

## Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

$$M = LU$$

# About matrices

## Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

$$M = LU$$
$$M + \delta M = (L + \delta L)(U + \delta U)$$

# About matrices

## Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

$$\begin{aligned} M &= LU \\ M + \delta M &= (L + \delta L)(U + \delta U) \\ M + \delta M &= LU + \delta L \times U + L \times \delta U \end{aligned}$$

# About matrices

## Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

$$\begin{aligned} M &= LU \\ M + \delta M &= (L + \delta L)(U + \delta U) \\ M + \delta M &= LU + \delta L \times U + L \times \delta U \\ \delta M &= \delta L \times U + L \times \delta U \end{aligned}$$

# About matrices

## Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

$$
\begin{aligned}
M &= LU \\
M + \delta M &= (L + \delta L)(U + \delta U) \\
M + \delta M &= LU + \delta L \times U + L \times \delta U \\
\delta M &= \delta L \times U + L \times \delta U \\
L^{-1} \times \delta M \times U^{-1} &= L^{-1} \times \delta L + \delta U \times U^{-1}
\end{aligned}
$$

# About matrices

## Differential of the LU factorization

We would like to differentiate $M \mapsto (L, U)$.

$$\begin{aligned} M &= LU \\ M + \delta M &= (L + \delta L)(U + \delta U) \\ M + \delta M &= LU + \delta L \times U + L \times \delta U \\ \delta M &= \delta L \times U + L \times \delta U \\ L^{-1} \times \delta M \times U^{-1} &= L^{-1} \times \delta L + \delta U \times U^{-1} \end{aligned}$$

Therefore, $\begin{aligned} \delta L &= L \times \left(L^{-1} \times \delta M \times U^{-1}\right)_{\text{Low}} \\ \delta U &= \left(L^{-1} \times \delta M \times U^{-1}\right)_{\text{Up}} \times U \end{aligned}$

# To sum up

## On $p$-adic precision

# To sum up

## On $p$-adic precision

- Step-by-step analysis : as a first step. Can show differentiability.

# To sum up

## On $p$-adic precision

- Step-by-step analysis : as a first step. Can show differentiability.
- Differential calculus : **intrinsic** and can handle both **gain** and **loss**.

# To sum up

## On $p$-adic precision

- Step-by-step analysis : as a first step. Can show differentiability.
- Differential calculus : **intrinsic** and can handle both **gain** and **loss**.
- New framework : differentials and lattices.

## Future works

- Implement automatic computation of differentials, within the computation.

# References

## Over $p$-adic analysis

- Peter Schneider $p$-adic Lie groups. (Springer).

## Over $p$-adic precision

- Xavier Caruso Random matrix over a DVR and LU factorization, preprint.
- Xavier Caruso, David Roe and Tristan Vaccon Tracking $p$-adic precision, preprint.