Résultants et sous-résultants de polynômes p-adiques

Xavier Caruso

Université Rennes 1

xavier.caruso@normalesup.org

Journées Nationales de Calcul Formel

3 novembre 2014

Nombres p-adiques

Nombres p-adiques

Soit p un nombre premier.

Nombres p-adiques

Soit p un nombre premier.

En pratique, dans tout l'exposé, p sera plutôt petit.

Nombres p-adiques

Soit p un nombre premier.

En pratique, dans tout l'exposé, p sera plutôt petit.

Un entier p-adique est un entier écrit en base p avec une infinité de chiffres :

$$\ldots\ a_n\ a_{n-1}\ \ldots\ a_2\ a_1\ a_0 \qquad \text{avec} \quad 0 \leqslant a_i < p.$$

Nombres p-adiques

Soit p un nombre premier.

En pratique, dans tout l'exposé, p sera plutôt petit.

Un entier p-adique est un entier écrit en base p avec une infinité de chiffres :

$$\ldots\ a_n\, a_{n-1}\ \ldots\ a_2\, a_1\, a_0 \qquad \text{avec} \quad 0 \leqslant a_i < p.$$

Un nombre p-adique est un nombre de la forme :

$$\ldots\ a_n\, a_{n-1}\ \ldots\ a_2\, a_1\, a_0\, , a_{-1} a_{-2}\ \ldots\ a_v.$$

Nombres p-adiques

Soit p un nombre premier.

En pratique, dans tout l'exposé, p sera plutôt petit.

Un entier p-adique est un entier écrit en base p avec une infinité de chiffres :

$$\ldots\ a_n\, a_{n-1}\ \ldots\ a_2\, a_1\, a_0 \qquad \text{avec} \quad 0 \leqslant a_i < p.$$

Un nombre p-adique est un nombre de la forme :

$$\ldots\ a_n\, a_{n-1}\ \ldots\ a_2\, a_1\, a_0\, , a_{-1} a_{-2}\ \ldots\ a_v.$$

Ces nombres s'additionnent et se multiplient selon les règles habituelles.

Nombres p-adiques

Soit p un nombre premier.

En pratique, dans tout l'exposé, p sera plutôt petit.

Un entier p-adique est un entier écrit en base p avec une infinité de chiffres :

$$\ldots\ a_n\, a_{n-1}\ \ldots\ a_2\, a_1\, a_0 \qquad \text{avec} \quad 0 \leqslant a_i < p.$$

Un nombre p-adique est un nombre de la forme :

$$\ldots\ a_n\, a_{n-1}\ \ldots\ a_2\, a_1\, a_0\, , a_{-1} a_{-2}\ \ldots\ a_v.$$

Ces nombres s'additionnent et se multiplient selon les règles habituelles.

Sur machine, on travaille avec des p-adiques tronqués.

Algorithme d'Euclide et précision p-adique

Un exemple

Un exemple

x^5	x^4	x^3	x^2	x	1
1	...11011	...01011	...00101	...10010	...11001
1	...11000	...11001	...01100	...00011	...01010

Un exemple

x^5	x^4	x^3	x^2	x	1
1	...11011	...01011	...00101	...10010	...11001
1	...11000	...11001	...01100	...00011	...01010
	...00011	...10010	...11001	...01111	...01111

Un exemple

	x^5	x^4	x^3	x^2	x	1
	1	...11011	...01011	...00101	...10010	...11001
	1	...11000	...11001	...01100	...00011	...01010
		...00011	...10010	...11001	...01111	...01111
$p\times$			...1101	...1000,1	...0010	...1000

Un exemple

	x^5	x^4	x^3	x^2	x	1
	1	...11011	...01011	...00101	...10010	...11001
	1	...11000	...11001	...01100	...00011	...01010
		...00011	...10010	...11001	...01111	...01111
$p\times$			...1101	...1000,1	...0010	...1000
$p^{-2}\times$				...0011	...11000	...01100

Un exemple

	$\mathbf{x^5}$	$\mathbf{x^4}$	$\mathbf{x^3}$	$\mathbf{x^2}$	$\mathbf{x}$	$\mathbf{1}$
	1	...11011	...01011	...00101	...10010	...11001
	1	...11000	...11001	...01100	...00011	...01010
		...00011	...10010	...11001	...01111	...01111
$p\times$			...1101	...1000,1	...0010	...1000
$p^{-2}\times$				...0011	...11000	...01100
$p^2\times$					...101	...011

Un exemple

	x^5	x^4	x^3	x^2	x	1
	1	...11011	...01011	...00101	...10010	...11001
	1	...11000	...11001	...01100	...00011	...01010
		...00011	...10010	...11001	...01111	...01111
$p\times$			...1101	...1000,1	...0010	...1000
$p^{-2}\times$				...0011	...11000	...01100
$p^{2}\times$					...101	...011
$p^{-2}\times$						...111

Un exemple

	x^5	x^4	x^3	x^2	x	1
	1	$\ldots 11011$	$\ldots 01011$	$\ldots 00101$	$\ldots 10010$	$\ldots 11001$
	1	$\ldots 11000$	$\ldots 11001$	$\ldots 01100$	$\ldots 00011$	$\ldots 01010$
		$\ldots 00011$	$\ldots 10010$	$\ldots 11001$	$\ldots 01111$	$\ldots 01111$
$p\times$			$\ldots 1101$	$\ldots 1000{,}1$	$\ldots 0010$	$\ldots 1000$
$p^{-2}\times$				$\ldots 0011$	$\ldots 11000$	$\ldots 01100$
$p^{2}\times$					$\ldots 101$	$\ldots 011$
$p^{-2}\times$						$\ldots 111$

On constate une perte de précision...

Un exemple

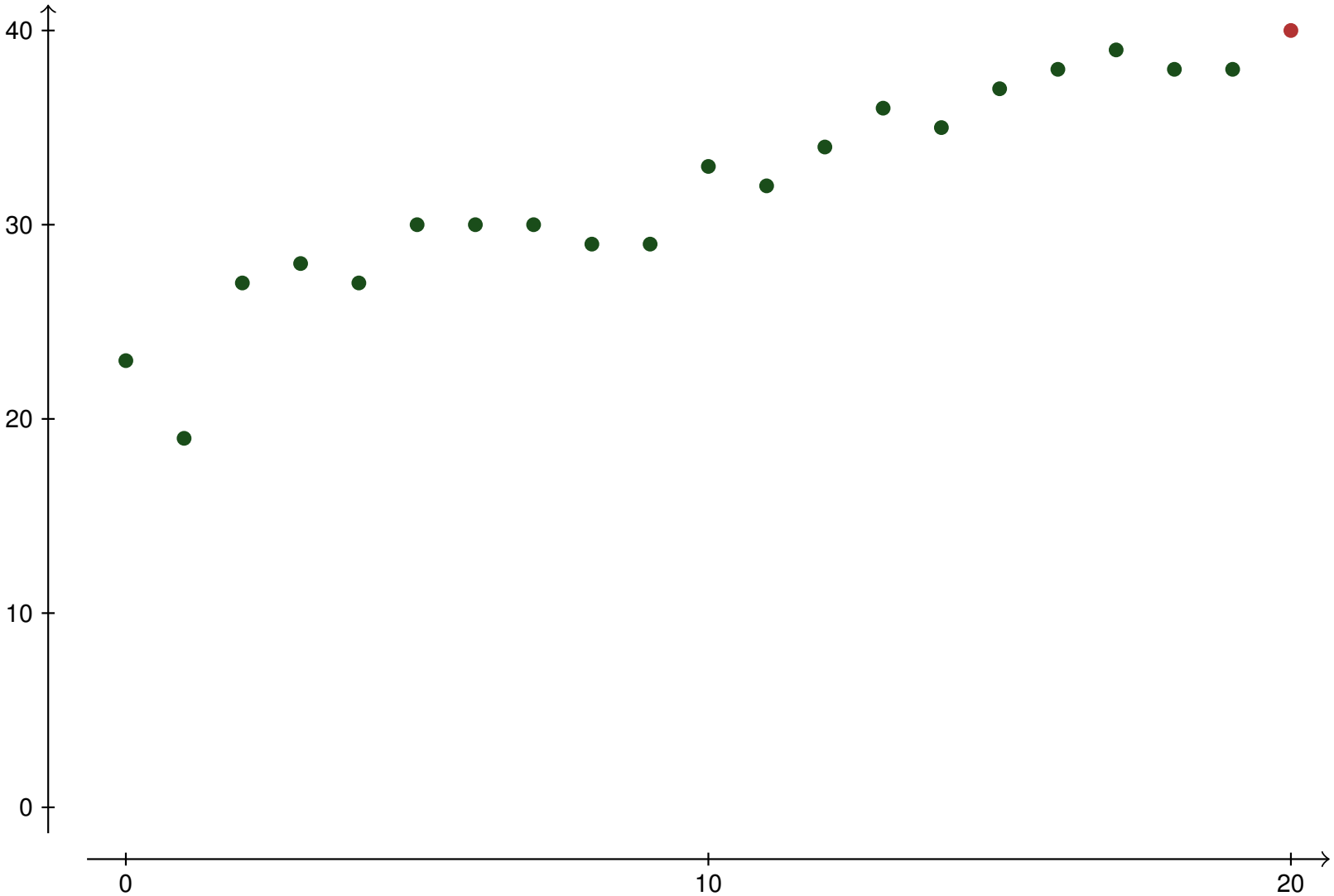
	x^5	x^4	x^3	x^2	x	1
	1	...11011	...01011	...00101	...10010	...11001
	1	...11000	...11001	...01100	...00011	...01010
		...00011	...10010	...11001	...01111	...01111
$p\times$			...1101	...1000,1	...0010	...1000
$p^{-2}\times$				...0011	...11000	...01100
$p^2\times$					...101	...011
$p^{-2}\times$						...111

On constate une perte de précision...

Le même phénomène se produit avec les coefficients de Bézout calculés par l'algorithme d'Euclide étendu.

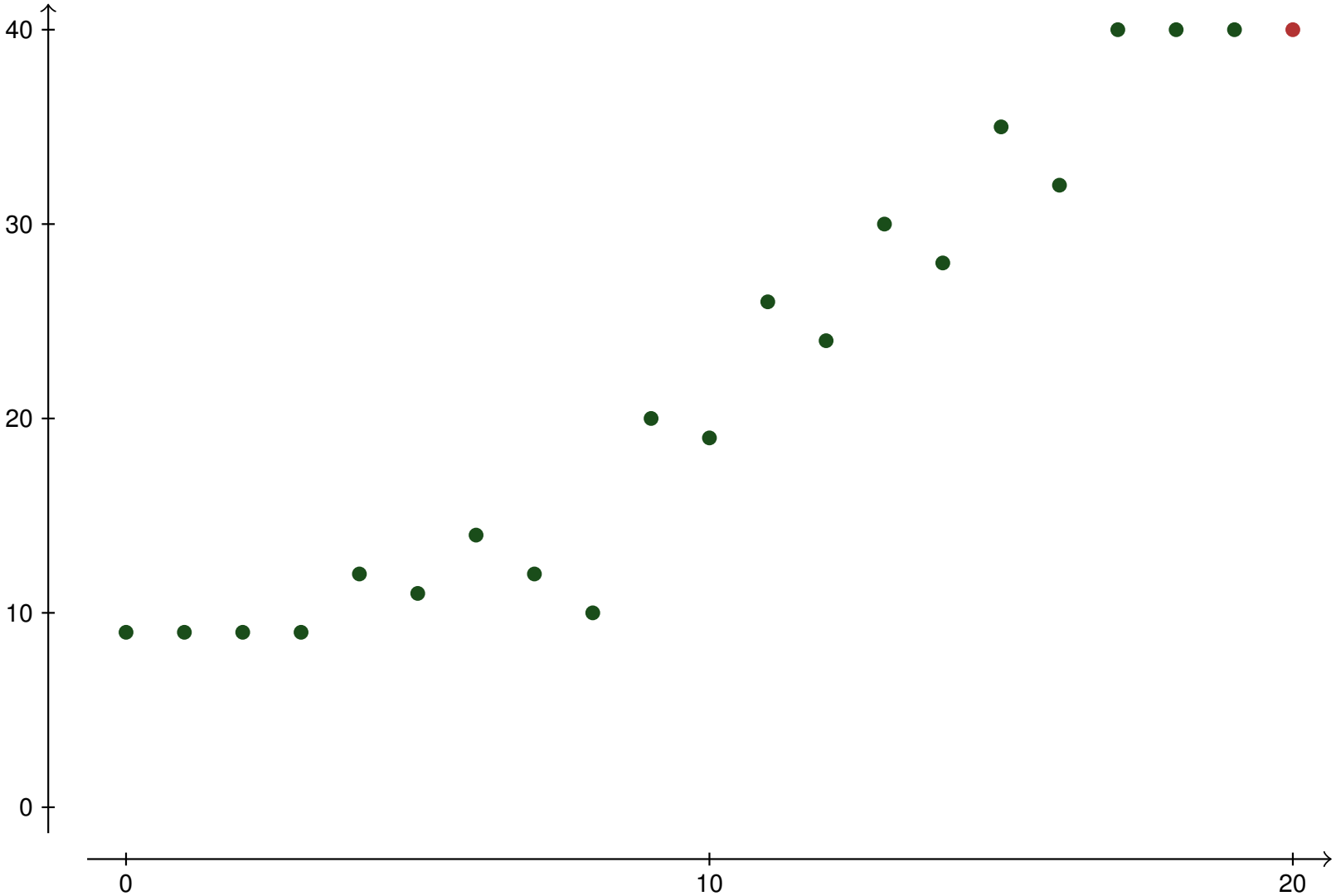
Pertes de précision

$p = 2$, $d = 20$



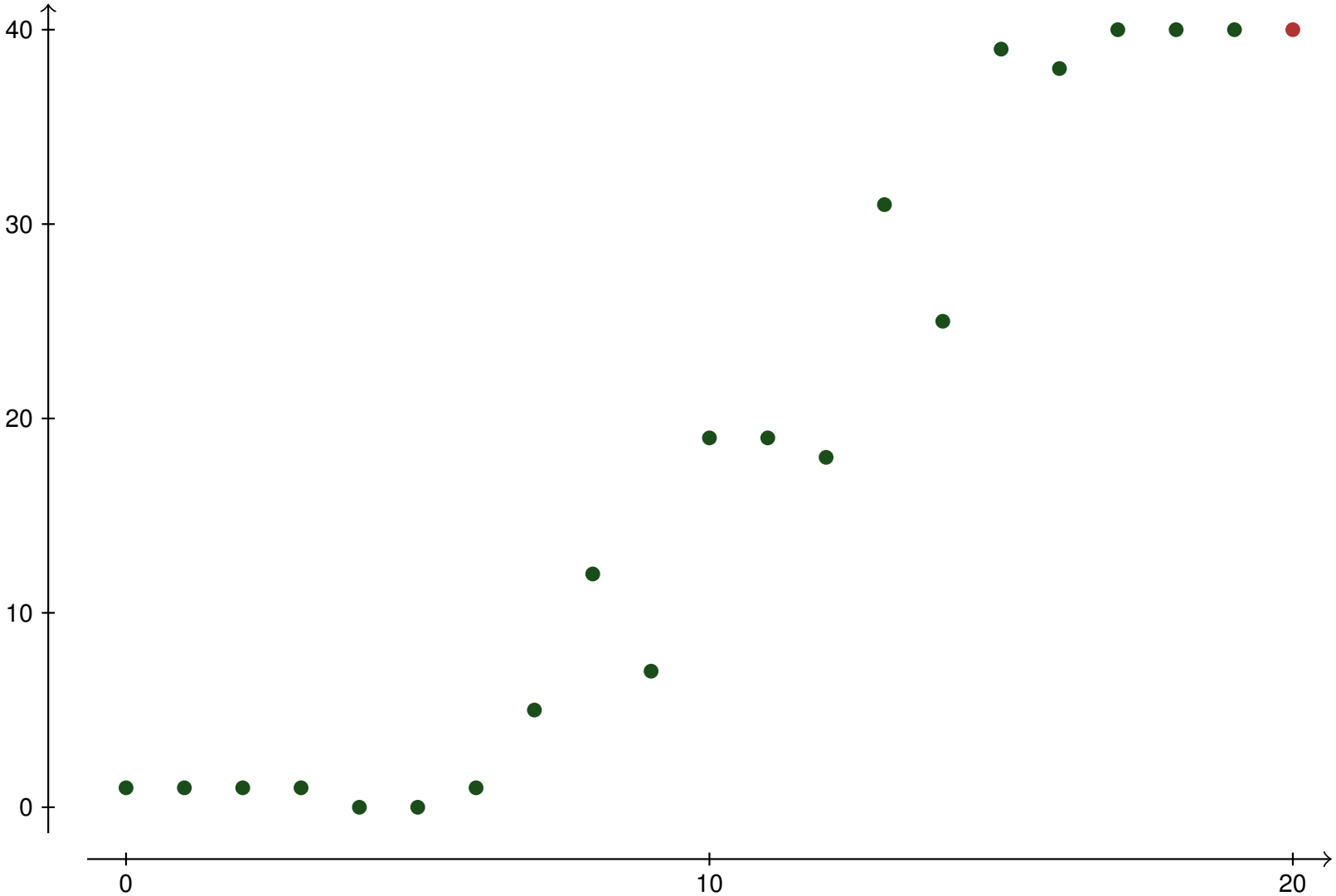
Pertes de précision

$p = 2$, $d = 20$



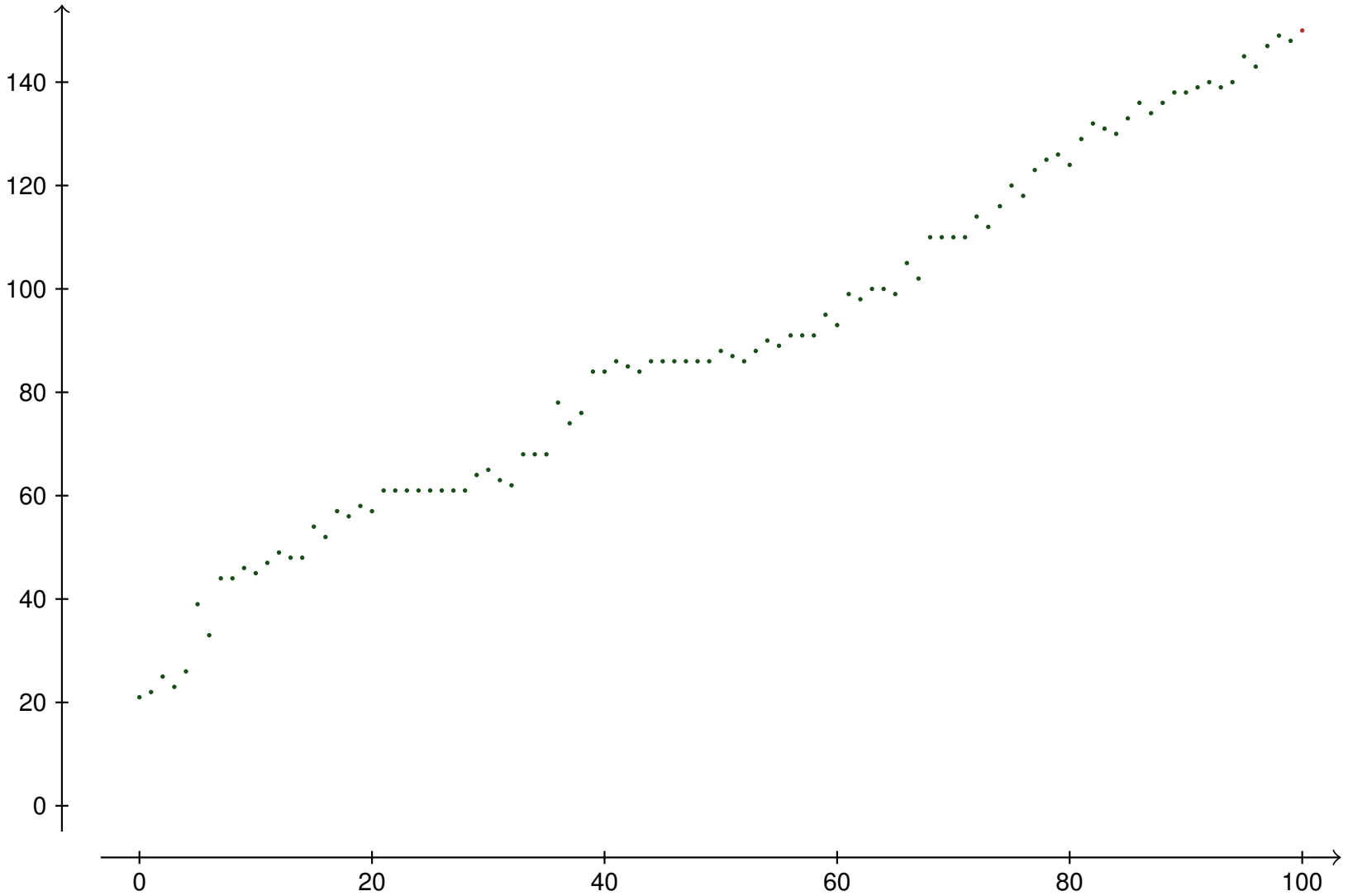
Pertes de précision

$p = 2$, $d = 20$



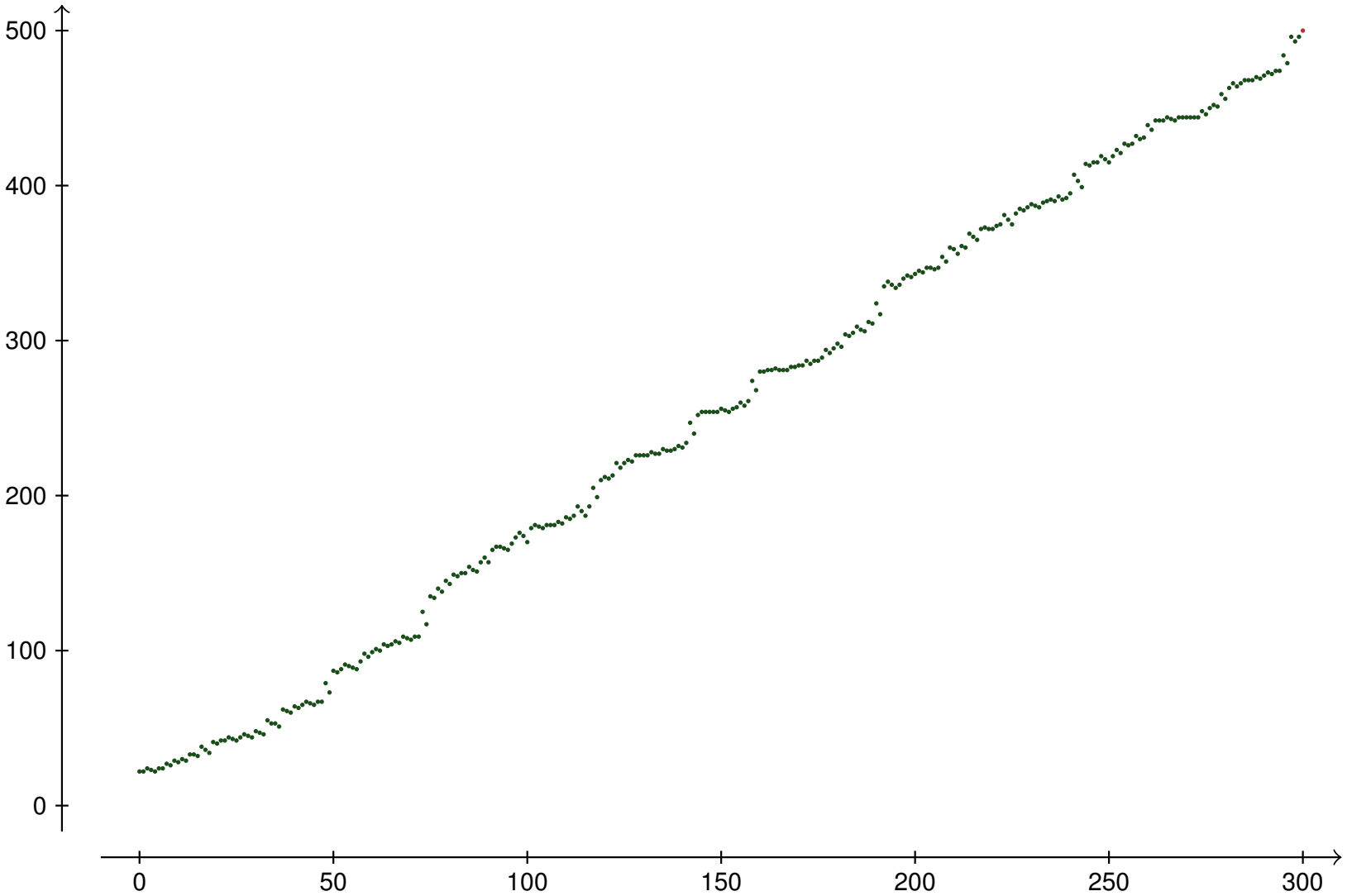
Pertes de précision

$p = 2$, $d = 100$



Pertes de précision

$p = 2$, $d = 300$



Pertes de précision

$p = 2$, $d = 300$

Analyse de la perte de précision

Analyse de la perte de précision

Hypothèses

Analyse de la perte de précision

Hypothèses

On suppose que, dans l'algorithme d'Euclide, les degrés des restes décroissent de 1 à chaque étape.

Analyse de la perte de précision

Hypothèses

On suppose que, dans l'algorithme d'Euclide, les degrés des restes décroissent de 1 à chaque étape.

On utilise un modèle de précision « plat ».

Analyse de la perte de précision

Hypothèses

On suppose que, dans l'algorithme d'Euclide, les degrés des restes décroissent de 1 à chaque étape.

On utilise un modèle de précision « plat ».

Notations

Analyse de la perte de précision

Hypothèses

On suppose que, dans l'algorithme d'Euclide, les degrés des restes décroissent de 1 à chaque étape.

On utilise un modèle de précision « plat ».

Notations

r_j = le reste de degré j dans l'algorithme d'Euclide

Analyse de la perte de précision

Hypothèses

On suppose que, dans l'algorithme d'Euclide, les degrés des restes décroissent de 1 à chaque étape.

On utilise un modèle de précision « plat ».

Notations

r_j = le reste de degré j dans l'algorithme d'Euclide

$\mathrm{lc}(r_j)$ = le coefficient dominant de r_j

Analyse de la perte de précision

Hypothèses

On suppose que, dans l'algorithme d'Euclide, les degrés des restes décroissent de 1 à chaque étape.

On utilise un modèle de précision « plat ».

Notations

r_j = le reste de degré j dans l'algorithme d'Euclide

$\mathrm{lc}(r_j)$ = le coefficient dominant de r_j

N_j = la précision de r_j

Analyse de la perte de précision

Hypothèses

On suppose que, dans l'algorithme d'Euclide, les degrés des restes décroissent de 1 à chaque étape.

On utilise un modèle de précision « plat ».

Notations

$r_j =$ le reste de degré j dans l'algorithme d'Euclide

$\mathrm{lc}(r_j) =$ le coefficient dominant de r_j

$N_j =$ la précision de r_j

$v_j =$ la valuation de $\mathrm{lc}(r_j)$

Analyse de la perte de précision

Hypothèses

On suppose que, dans l'algorithme d'Euclide, les degrés des restes décroissent de 1 à chaque étape.

On utilise un modèle de précision « plat ».

Notations

$r_j =$ le reste de degré j dans l'algorithme d'Euclide

$\mathrm{lc}(r_j) =$ le coefficient dominant de r_j

$N_j =$ la précision de r_j

$v_j =$ la valuation de $\mathrm{lc}(r_j)$

$w_j =$ la plus petite valuation d'un coefficient de r_j

Analyse de la perte de précision

Hypothèses

On suppose que, dans l'algorithme d'Euclide, les degrés des restes décroissent de 1 à chaque étape.

On utilise un modèle de précision « plat ».

Notations

$r_j =$ le reste de degré j dans l'algorithme d'Euclide

$\mathrm{lc}(r_j) =$ le coefficient dominant de r_j

$N_j =$ la précision de r_j

$v_j =$ la valuation de $\mathrm{lc}(r_j)$

$w_j =$ la plus petite valuation d'un coefficient de r_j

$\delta_j = v_j - w_j$

Analyse de la perte de précision

Hypothèses

On suppose que, dans l'algorithme d'Euclide, les degrés des restes décroissent de 1 à chaque étape.

On utilise un modèle de précision « plat ».

Notations

$r_j =$ le reste de degré j dans l'algorithme d'Euclide

$\mathrm{lc}(r_j) =$ le coefficient dominant de r_j

$N_j =$ la précision de r_j

$v_j =$ la valuation de $\mathrm{lc}(r_j)$

$w_j =$ la plus petite valuation d'un coefficient de r_j

$\delta_j = v_j - w_j \geqslant 0$

Analyse de la perte de précision

Analyse de la perte de précision

Perte de précision dans la division euclidienne

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision relative de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision relative de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$$N_{j+1} - v_{j+1}$$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision relative de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$$N_{j+1} - v_{j+1} \quad N_j - v_j$$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision relative de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$N_{j+1} - v_{j+1}$ $N_j - v_j$ $N_j - w_j$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision relative de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$$\min(\ N_{j+1} - v_{j+1},\ N_j - v_j,\ N_j - w_j\ )$$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision relative de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$\min(\ N_{j+1} - v_{j+1},\ N_j - v_j,\ \cancel{N_j - w_j}\ )$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision absolue de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$$\min(\ N_{j+1} - v_{j+1},\ N_j - v_j,\ \cancel{N_j - w_j}\ ) + v_{j+1} - v_j + w_j$$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision absolue de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$$\begin{aligned} &\min(\ N_{j+1} - v_{j+1},\ N_j - v_j,\ \cancel{N_j - w_j}\ ) + v_{j+1} - v_j + w_j \\ &\qquad = \min(\ N_{j+1} - \delta_j,\ N_j - \delta_j + v_{j+1} - v_j\ ) \end{aligned}$$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision absolue de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$$\begin{aligned} &\min(\ N_{j+1} - v_{j+1},\ N_j - v_j,\ \cancel{N_j - w_j}\ ) + v_{j+1} - v_j + w_j \\ &\qquad = \min(\ N_{j+1} - \delta_j,\ N_j - \delta_j + v_{j+1} - v_j\ ) \end{aligned}$$

Précision absolue de $\tilde{r}_{j-1}$:

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision absolue de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$$\begin{aligned} &\min(\ N_{j+1} - v_{j+1},\ N_j - v_j,\ \cancel{N_j - w_j}\ ) + v_{j+1} - v_j + w_j \\ &\qquad = \min(\ N_{j+1} - \delta_j,\ N_j - \delta_j + v_{j+1} - v_j\ ) \end{aligned}$$

Précision absolue de $\tilde{r}_{j-1}$:

$$\tilde{N}_{j-1} = \min(\ N_{j+1} - \delta_j,\ N_j - \delta_j + v_{j+1} - v_j\ )$$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision absolue de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$$\begin{aligned} &\min(\ N_{j+1} - v_{j+1},\ N_j - v_j,\ \cancel{N_j - w_j}\ ) + v_{j+1} - v_j + w_j \\ &\qquad = \min(\ N_{j+1} - \delta_j,\ N_j - \delta_j + v_{j+1} - v_j\ ) \end{aligned}$$

Précision absolue de $\tilde{r}_{j-1}$:

$$\tilde{N}_{j-1} = \min(\ N_{j+1} - \delta_j,\ N_j - \delta_j + v_{j+1} - v_j\ )$$

Précision absolue de r_{j-1} :

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision absolue de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$$\begin{aligned} &\min(\ N_{j+1} - v_{j+1},\ N_j - v_j,\ \cancel{N_j - w_j}\ ) + v_{j+1} - v_j + w_j \\ &\qquad = \min(\ N_{j+1} - \delta_j,\ N_j - \delta_j + v_{j+1} - v_j\ ) \end{aligned}$$

Précision absolue de $\tilde{r}_{j-1}$:

$$\tilde{N}_{j-1} = \min(\ N_{j+1} - \delta_j,\ N_j - \delta_j + v_{j+1} - v_j\ )$$

Précision absolue de r_{j-1} :

$$N_{j-1} = \min(\ \tilde{N}_{j-1} - \delta_j,\ N_j - \delta_j + \tilde{v}_{j-1} - v_j\ )$$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision absolue de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$$\begin{aligned} &\min(\ N_{j+1} - v_{j+1},\ N_j - v_j,\ \cancel{N_j - w_j}\ ) + v_{j+1} - v_j + w_j \\ &\qquad = \min(\ N_{j+1} - \delta_j,\ N_j - \delta_j + v_{j+1} - v_j\ ) \end{aligned}$$

Précision absolue de $\tilde{r}_{j-1}$:

$$\tilde{N}_{j-1} = \min(\ N_{j+1} - \delta_j,\ N_j - \delta_j + v_{j+1} - v_j\ )$$

Précision absolue de r_{j-1} :

$$N_{j-1} \leqslant \qquad \tilde{N}_{j-1} - \delta_j$$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

Précision absolue de $\frac{lc(r_{j+1})}{lc(r_j)} \cdot r_j$:

$$\begin{aligned} &\min(\ N_{j+1} - v_{j+1},\ N_j - v_j,\ \cancel{N_j - w_j}\ ) + v_{j+1} - v_j + w_j \\ &\qquad = \min(\ N_{j+1} - \delta_j,\ N_j - \delta_j + v_{j+1} - v_j\ ) \end{aligned}$$

Précision absolue de $\tilde{r}_{j-1}$:

$$\tilde{N}_{j-1} = \min(\ N_{j+1} - \delta_j,\ N_j - \delta_j + v_{j+1} - v_j\ )$$

Précision absolue de r_{j-1} :

$$N_{j-1} \leqslant \quad \tilde{N}_{j-1} - \delta_j \quad \leqslant N_j - 2 \cdot \delta_j + v_{j+1} - v_j$$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

D'où on déduit :

$$N_{j-1} \leqslant N_j - 2 \cdot \delta_j + (v_{j+1} - v_j)$$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

D'où on déduit :

$$N_{j-1} \leqslant N_j - 2 \cdot \delta_j + (v_{j+1} - v_j)$$

Perte de précision dans l'algorithme d'Euclide

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

D'où on déduit :

$$N_{j-1} \leqslant N_j - 2 \cdot \delta_j + (v_{j+1} - v_j)$$

Perte de précision dans l'algorithme d'Euclide

En sommant on trouve une minoration des pertes de précision :

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

D'où on déduit :

$$N_{j-1} \leqslant N_j - 2 \cdot \delta_j + (v_{j+1} - v_j)$$

Perte de précision dans l'algorithme d'Euclide

En sommant on trouve une minoration des pertes de précision :

$$N - (N_j - v_j)$$

$$[\, N = N_d \,]$$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

D'où on déduit :

$$N_{j-1} \leqslant N_j - 2 \cdot \delta_j + (v_{j+1} - v_j)$$

Perte de précision dans l'algorithme d'Euclide

En sommant on trouve une minoration des pertes de précision :

$$N - (N_j - v_j) \geqslant v_j + v_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k.$$

$[\, N = N_d \,]$

Analyse de la perte de précision

Perte de précision dans la division euclidienne

D'après les conditions sur les degrés, on a :

$$\tilde{r}_{j-1} = r_{j+1} - \frac{\mathrm{lc}(r_{j+1})}{\mathrm{lc}(r_j)} \cdot r_j \quad ; \quad r_{j-1} = \tilde{r}_{j-1} - \frac{\mathrm{lc}(\tilde{r}_{j-1})}{\mathrm{lc}(r_j)} \cdot r_j$$

D'où on déduit :

$$N_{j-1} \leqslant N_j - 2 \cdot \delta_j + (v_{j+1} - v_j)$$

Perte de précision dans l'algorithme d'Euclide

En sommant on trouve une minoration des pertes de précision :

$$N - (N_j - v_j) \geqslant v_j + v_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k.$$

$[\, N = N_d \,]$

Une formule analogue existe pour les coefficients de Bézout.

Estimation des pertes de précision pour des polynômes aléatoires

Résultants et sous-résultants

Résultants

Résultants

Soient $A, B \in R[X]$

Résultants

Soient $A, B \in R[X]$ (où R est un anneau intègre).

Résultants

Soient $A, B \in R[X]$ (où R est un anneau intègre).

On suppose que A et B sont unitaires de même degré d.

Résultants

Soient $A, B \in R[X]$ (où R est un anneau intègre).

On suppose que A et B sont unitaires de même degré d.

La matrice de Sylvester est la matrice de l'application

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

dans les bases canoniques.

Résultants

Soient $A, B \in R[X]$ (où R est un anneau intègre).

On suppose que A et B sont unitaires de même degré d.

La matrice de Sylvester est la matrice de l'application

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

dans les bases canoniques.

Le résultant de A et B, noté $\mathrm{Rés}(A, B)$, est son déterminant.

Résultants

Soient $A, B \in R[X]$ (où R est un anneau intègre).

On suppose que A et B sont unitaires de même degré d.

La matrice de Sylvester est la matrice de l'application

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

dans les bases canoniques.

Le résultant de A et B, noté $\mathrm{Rés}(A, B)$, est son déterminant.

C'est un élément de l'anneau R.

Résultants

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

Propriétés

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

Résultants

Propriétés

Si R est un corps,

$$\text{Rés}(A, B) \neq 0$$
ssi $\text{PGCD}(A, B) = 1$.

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

Propriétés

Si R est un corps,

$$\text{Rés}(A, B) \neq 0$$

ssi $\text{PGCD}(A, B) = 1$.

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

Il existe des polynômes $\mathcal{U}_0, \mathcal{V}_0 \in R_{<d}[X]$

- dont les coefficients sont, au signe près, des mineurs de la matrice de Sylvester, et
- tels que $A\,\mathcal{U}_0 + B\,\mathcal{V}_0 = \text{Rés}(A, B)$.

Résultants

Propriétés

Si R est un corps,

$$\text{Rés}(A, B) \neq 0$$
ssi $\text{PGCD}(A, B) = 1$.

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

Il existe des polynômes $\mathcal{U}_0, \mathcal{V}_0 \in R_{<d}[X]$

- dont les coefficients sont, au signe près, des mineurs de la matrice de Sylvester, et
- tels que $A\,\mathcal{U}_0 + B\,\mathcal{V}_0 = \text{Rés}(A, B)$.

Remarque en passant

En calculant $\frac{\mathcal{U}_0}{\text{Rés}(A,B)}$ et $\frac{\mathcal{V}_0}{\text{Rés}(A,B)}$, on obtient les coefficients de Bézout avec une perte de précision de $2 \cdot v_p(\text{Rés}(A, B))$ chiffres.

Sous-résultants

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

Sous-résultants

Théorème

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

Sous-résultants

Théorème

Pour $j \in \{0, \ldots, d-1\}$, il existe des polynômes $R_j, \mathcal{U}_j, \mathcal{V}_j \in R[X]$ avec :

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

Sous-résultants

Théorème

Pour $j \in \{0, \dots, d-1\}$,
il existe des polynômes
$R_j, \mathcal{U}_j, \mathcal{V}_j \in R[X]$ avec :

- $\deg R_j \leqslant j$, $\deg \mathcal{U}_j < d-j$, $\deg \mathcal{V}_j < d-j$

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

Sous-résultants

Théorème

Pour $j \in \{0, \dots, d-1\}$, il existe des polynômes $R_j, \mathcal{U}_j, \mathcal{V}_j \in R[X]$ avec :

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

- $\deg R_j \leqslant j$, $\deg \mathcal{U}_j < d - j$, $\deg \mathcal{V}_j < d - j$,
- les coefficients de R_j, $\mathcal{U}_j$ et $\mathcal{V}_j$ sont tous, au signe près, des mineurs de la matrice de Sylvester

Sous-résultants

Théorème

Pour $j \in \{0, \dots, d-1\}$, il existe des polynômes $R_j, \mathcal{U}_j, \mathcal{V}_j \in R[X]$ avec :

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

- $\deg R_j \leqslant j$, $\deg \mathcal{U}_j < d-j$, $\deg \mathcal{V}_j < d-j$,
- les coefficients de R_j, $\mathcal{U}_j$ et $\mathcal{V}_j$ sont tous, au signe près, des mineurs de la matrice de Sylvester, et
- $A\,\mathcal{U}_j + B\,\mathcal{V}_j = R_j$.

Sous-résultants

Théorème

Pour $j \in \{0, \dots, d-1\}$, il existe des polynômes $R_j, \mathcal{U}_j, \mathcal{V}_j \in R[X]$ avec :

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

- $\deg R_j \leqslant j$, $\deg \mathcal{U}_j < d-j$, $\deg \mathcal{V}_j < d-j$,
- les coefficients de R_j, $\mathcal{U}_j$ et $\mathcal{V}_j$ sont tous, au signe près, des mineurs de la matrice de Sylvester, et
- $A\,\mathcal{U}_j + B\,\mathcal{V}_j = R_j$.

Le polynôme R_j est appelé le *j*-ième sous-résultant de A et B.

Sous-résultants

Théorème

Pour $j \in \{0, \dots, d-1\}$,
il existe des polynômes
$R_j, \mathcal{U}_j, \mathcal{V}_j \in R[X]$ avec :

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

- $\deg R_j \leqslant j$, $\deg \mathcal{U}_j < d-j$, $\deg \mathcal{V}_j < d-j$,
- les coefficients de R_j, $\mathcal{U}_j$ et $\mathcal{V}_j$ sont tous, au signe près, des mineurs de la matrice de Sylvester, et
- $A\,\mathcal{U}_j + B\,\mathcal{V}_j = R_j$.

Le polynôme R_j est appelé le *j*-ième sous-résultant de A et B.

Propriété

Sous-résultants

Théorème

Pour $j \in \{0, \dots, d-1\}$,
il existe des polynômes
$R_j, \mathcal{U}_j, \mathcal{V}_j \in R[X]$ avec :

Application de Sylvester :

$$\begin{array}{rcl} R_{<d}[X] \times R_{<d}[X] & \to & R_{<2d}[X] \\ (U, V) & \mapsto & A\,U + B\,V \end{array}$$

- $\deg R_j \leqslant j$, $\deg \mathcal{U}_j < d - j$, $\deg \mathcal{V}_j < d - j$,
- les coefficients de R_j, $\mathcal{U}_j$ et $\mathcal{V}_j$ sont tous, au signe près, des mineurs de la matrice de Sylvester, et
- $A\,\mathcal{U}_j + B\,\mathcal{V}_j = R_j$.

Le polynôme R_j est appelé le *j*-ième sous-résultant de A et B.

Propriété

Si R est un corps et si j est le plus petit indice tel que $R_j \neq 0$, alors $\deg R_j = j$ et $\mathrm{PGCD}(A, B) \sim R_j$.

Calcul des sous-résultants

Calcul des sous-résultants

On suppose, pour simplifier, que $\deg R_j = j$ pour tout j.

Calcul des sous-résultants

On suppose, pour simplifier, que $\deg R_j = j$ pour tout j.

Algorithme des pseudo-restes

Calcul des sous-résultants

On suppose, pour simplifier, que $\deg R_j = j$ pour tout j.

Algorithme des pseudo-restes

En posant $R_{d+1} = A$ et $R_d = B$, on a :

$$R_{j-1} = \frac{\mathrm{lc}(R_j)^2}{\mathrm{lc}(R_{j+1})^2} \cdot R_{j+1} \% R_j.$$

Calcul des sous-résultants

On suppose, pour simplifier, que $\deg R_j = j$ pour tout j.

Algorithme des pseudo-restes

En posant $R_{d+1} = A$ et $R_d = B$, on a :

$$R_{j-1} = \frac{\mathrm{lc}(R_j)^2}{\mathrm{lc}(R_{j+1})^2} \cdot R_{j+1} \% R_j.$$

Corollaire

Calcul des sous-résultants

On suppose, pour simplifier, que $\deg R_j = j$ pour tout j.

Algorithme des pseudo-restes

En posant $R_{d+1} = A$ et $R_d = B$, on a :

$$R_{j-1} = \frac{\mathrm{lc}(R_j)^2}{\mathrm{lc}(R_{j+1})^2} \cdot R_{j+1} \,\%\, R_j.$$

Corollaire

Pour tout j, on a :

$$r_j = \lambda_j \cdot R_j \qquad \text{avec} \quad \lambda_j \in \mathrm{Frac}(R)$$

Calcul des sous-résultants

On suppose, pour simplifier, que $\deg R_j = j$ pour tout j.

Algorithme des pseudo-restes

En posant $R_{d+1} = A$ et $R_d = B$, on a :

$$R_{j-1} = \frac{\mathrm{lc}(R_j)^2}{\mathrm{lc}(R_{j+1})^2} \cdot R_{j+1} \,\%\, R_j.$$

Corollaire

Pour tout j, on a :

$$r_j = \lambda_j \cdot R_j \qquad \text{avec} \quad \lambda_j \in \mathrm{Frac}(R)$$

ainsi que la relation $\lambda_{j-1} \cdot \lambda_j = \mathrm{lc}(R_j)^2$.

Calcul des sous-résultants

On suppose, pour simplifier, que $\deg R_j = j$ pour tout j.

Algorithme des pseudo-restes

En posant $R_{d+1} = A$ et $R_d = B$, on a :

$$R_{j-1} = \frac{\mathrm{lc}(R_j)^2}{\mathrm{lc}(R_{j+1})^2} \cdot R_{j+1} \% R_j.$$

Corollaire

Pour tout j, on a :

$$r_j = \lambda_j \cdot R_j \qquad \text{avec} \quad \lambda_j \in \mathrm{Frac}(R)$$

ainsi que la relation $\lambda_{j-1} \cdot \lambda_j = \mathrm{lc}(R_j)^2$.

Preuve : Récurrence descendante sur j à partir de $r_{j-1} = r_{j+1} \% r_j$.

Retour sur les pertes de précision

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant v_j + v_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant v_j + v_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

Notations

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant v_j + v_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

Notations

$V_j =$ la valuation de $\mathrm{lc}(R_j)$

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant v_j + v_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

Notations

$V_j =$ la valuation de $\mathrm{lc}(R_j)$

$W_j =$ la plus petite valuation d'un coefficient de R_j

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant v_j + v_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

Notations

$V_j =$ la valuation de $\mathrm{lc}(R_j)$

$W_j =$ la plus petite valuation d'un coefficient de R_j

Relations

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant v_j + v_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

Notations

$V_j =$ la valuation de $\mathrm{lc}(R_j)$

$W_j =$ la plus petite valuation d'un coefficient de R_j

Relations

- $\delta_j = v_j - w_j = V_j - W_j$

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant v_j + v_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

Notations

$V_j =$ la valuation de $\mathrm{lc}(R_j)$

$W_j =$ la plus petite valuation d'un coefficient de R_j

Relations

- $\delta_j = v_j - w_j = V_j - W_j$
  provient de $r_j = \lambda_j \cdot R_j$

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant v_j + v_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

Notations

V_j = la valuation de $\mathrm{lc}(R_j)$

W_j = la plus petite valuation d'un coefficient de R_j

Relations

- $\delta_j = v_j - w_j = V_j - W_j$
  provient de $r_j = \lambda_j \cdot R_j$
- $v_j + v_{j+1} = V_j - V_{j+1}$

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant v_j + v_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

Notations

$V_j =$ la valuation de $\mathrm{lc}(R_j)$

$W_j =$ la plus petite valuation d'un coefficient de R_j

Relations

- $\delta_j = v_j - w_j = V_j - W_j$
  provient de $r_j = \lambda_j \cdot R_j$
- $v_j + v_{j+1} = V_j - V_{j+1}$
  provient de $\lambda_j \cdot \lambda_{j+1} = \mathrm{lc}(R_{j+1})^2$

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

Notations

V_j = la valuation de $\mathrm{lc}(R_j)$

W_j = la plus petite valuation d'un coefficient de R_j

Relations

- $\delta_j = v_j - w_j = V_j - W_j$
  provient de $r_j = \lambda_j \cdot R_j$
- $v_j + v_{j+1} = V_j - V_{j+1}$
  provient de $\lambda_j \cdot \lambda_{j+1} = \mathrm{lc}(R_{j+1})^2$

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

On considère V_j, W_j et δ_j comme des variables aléatoires.

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

On considère V_j, W_j et δ_j comme des variables aléatoires.

Théorème

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

On considère V_j, W_j et δ_j comme des variables aléatoires.

Théorème

- $\frac{1}{p-1} \leqslant \mathbb{E}[V_j] \leqslant \frac{p}{(p-1)^2}$

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

On considère V_j, W_j et δ_j comme des variables aléatoires.

Théorème

- $\frac{1}{p-1} \leqslant \mathbb{E}[V_j] \leqslant \frac{p}{(p-1)^2}$
- $\mathbb{E}[\delta_j] \geqslant \frac{1}{p} - \frac{1}{p^{j+1}}$

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2\sum_{k=j+1}^{d} \delta_k$$

On considère V_j, W_j et δ_j comme des variables aléatoires.

Théorème

- $\frac{1}{p-1} \leqslant \mathbb{E}[V_j] \leqslant \frac{p}{(p-1)^2}$
- $\mathbb{E}[\delta_j] \geqslant \frac{1}{p} - \frac{1}{p^{j+1}}$

Corollaire

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

On considère V_j, W_j et δ_j comme des variables aléatoires.

Théorème

- $\frac{1}{p-1} \leqslant \mathbb{E}[V_j] \leqslant \frac{p}{(p-1)^2}$
- $\mathbb{E}[\delta_j] \geqslant \frac{1}{p} - \frac{1}{p^{j+1}}$

Corollaire

Les pertes de précision dans l'algorithme d'Euclide sont en moyenne en $\Omega(\frac{d-j}{p})$.

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2\sum_{k=j+1}^{d} \delta_k$$

On considère V_j, W_j et δ_j comme des variables aléatoires.

Théorème

- $\frac{1}{p-1} \leqslant \mathbb{E}[V_j] \leqslant \frac{p}{(p-1)^2}$
- $\mathbb{E}[\delta_j] \geqslant \frac{1}{p} - \frac{1}{p^{j+1}}$

Remarque en passant :

En calculant $\mathcal{U}_0/R_0$ et $\mathcal{V}_0/R_0$, on obtient les coefficients de Bézout avec une perte de précision de $2V_0$ chiffres.

Corollaire

Les pertes de précision dans l'algorithme d'Euclide sont en moyenne en $\Omega(\frac{d-j}{p})$.

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

On considère V_j, W_j et δ_j comme des variables aléatoires.

Théorème amélioré pour V_j

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

On considère V_j, W_j et δ_j comme des variables aléatoires.

Théorème amélioré pour V_j

Soient $X_0, \ldots, X_{d-1}$ des variables aléatoires deux à deux indépendantes avec $\mathbb{P}[X_i = k] = (1 - p^{-1}) \cdot p^{-k}$.

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2 \sum_{k=j+1}^{d} \delta_k$$

On considère V_j, W_j et δ_j comme des variables aléatoires.

Théorème amélioré pour V_j

Soient $X_0, \ldots, X_{d-1}$ des variables aléatoires deux à deux indépendantes avec $\mathbb{P}[X_i = k] = (1 - p^{-1}) \cdot p^{-k}$.

[loi géométrique discrète de paramètre $(1 - p^{-1})$]

Retour sur les pertes de précision

Pertes de précision dans l'algorithme d'Euclide :

$$N - (N_j - v_j) \geqslant V_j - V_{j+1} + 2\sum_{k=j+1}^{d} \delta_k$$

On considère V_j, W_j et δ_j comme des variables aléatoires.

Théorème amélioré pour V_j

Soient $X_0, \ldots, X_{d-1}$ des variables aléatoires deux à deux indépendantes avec $\mathbb{P}[X_i = k] = (1 - p^{-1}) \cdot p^{-k}$.

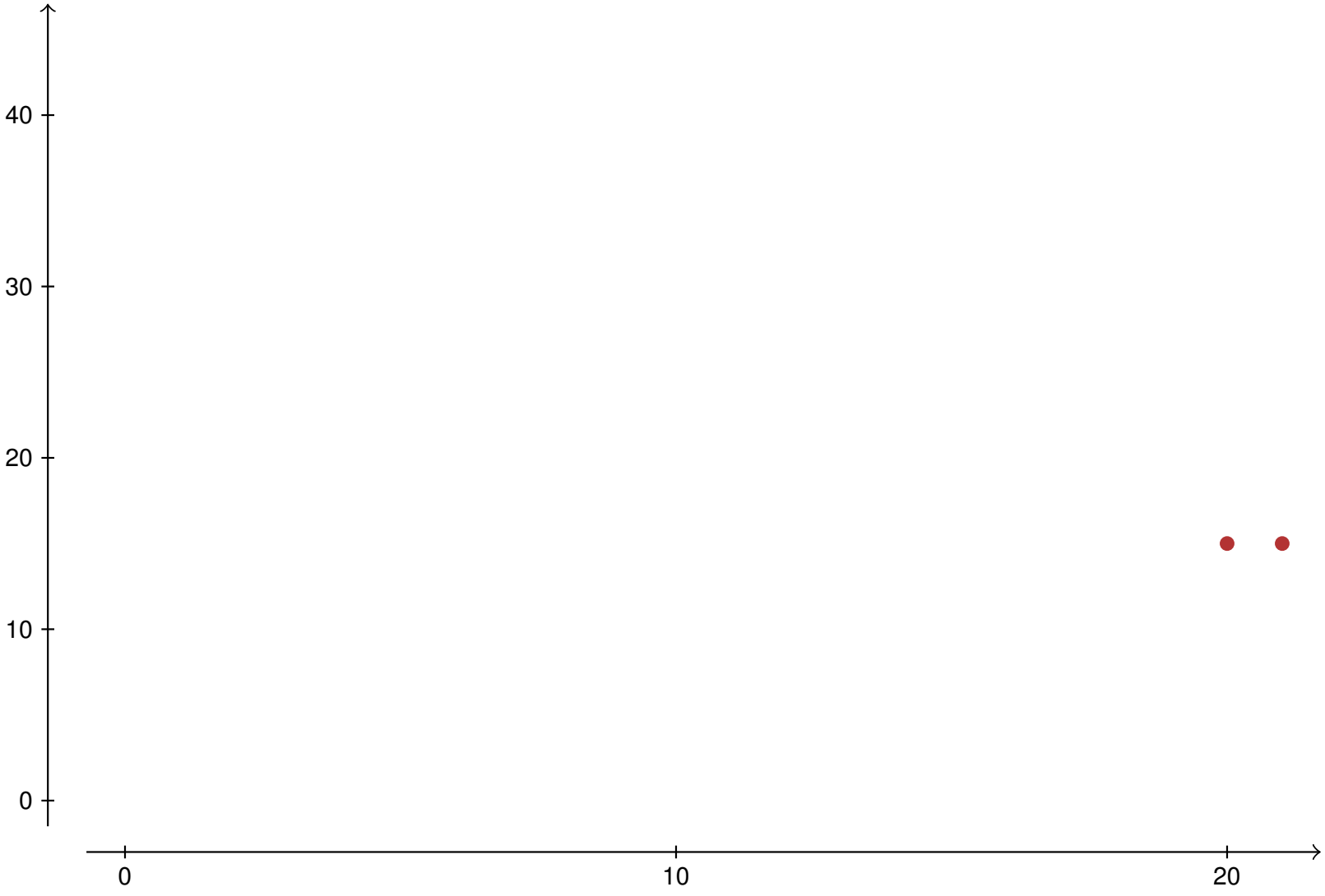
[loi géométrique discrète de paramètre $(1 - p^{-1})$]

Alors V_i suit la même loi que : $\displaystyle\sum_{k=0}^{d} \min(X_{j-k}, X_{j-k+1}, \ldots, X_{j+k})$

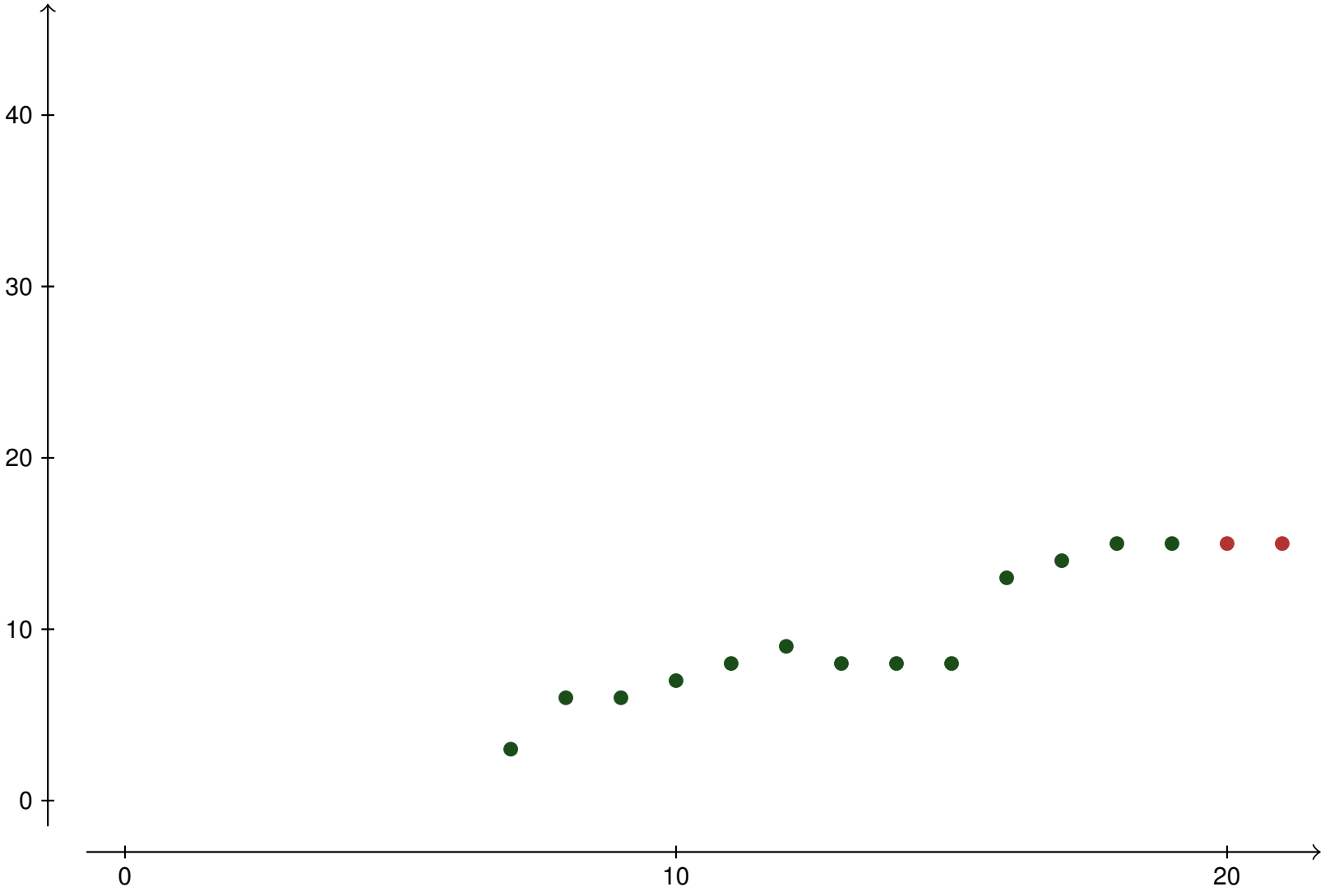
où par convention $X_i = +\infty$ pour $i < 0$ et $X_i = 0$ pour $i \geqslant d$.

Une version stable de l'algorithme d'Euclide

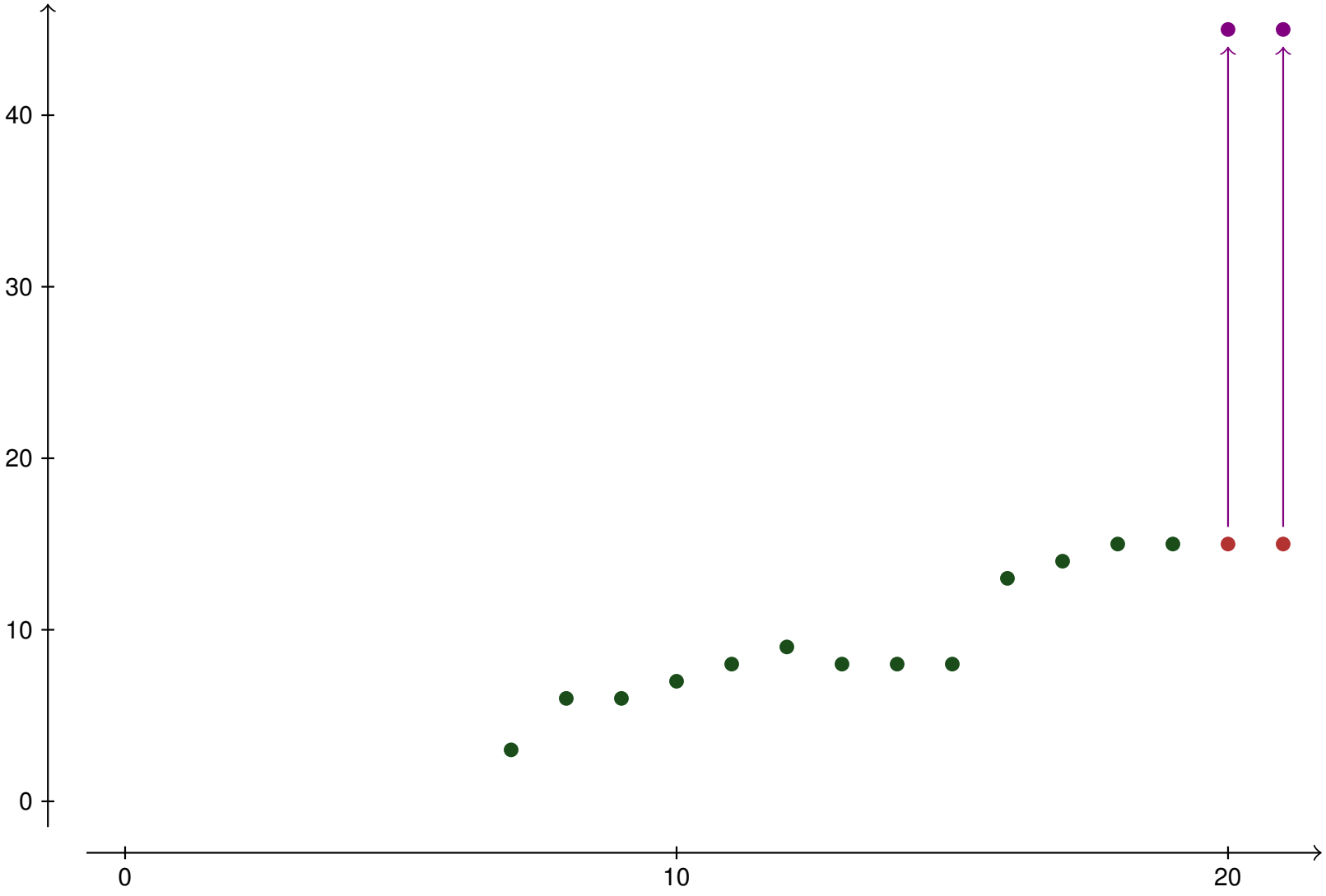
Une méthode naïve



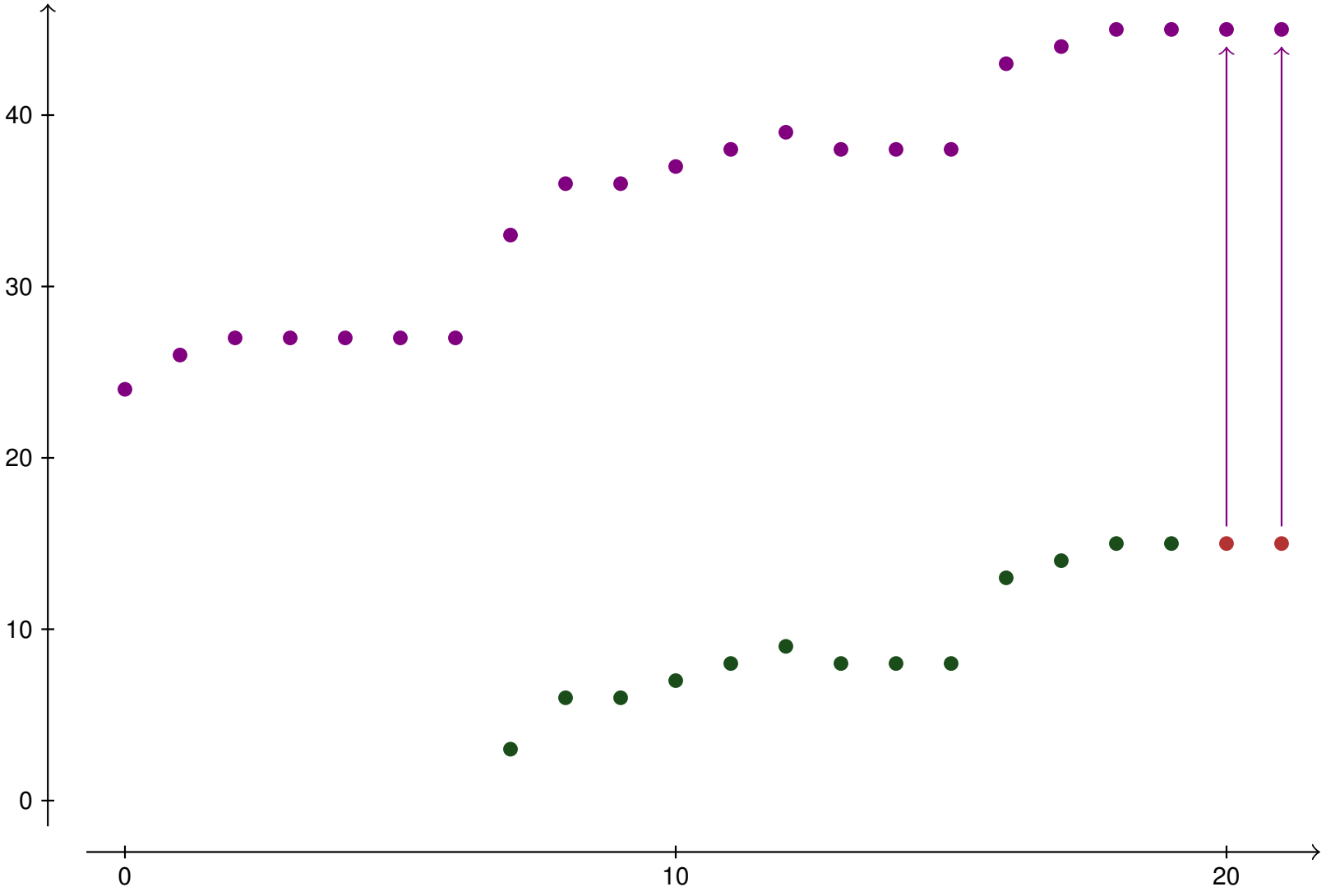
Une méthode naïve



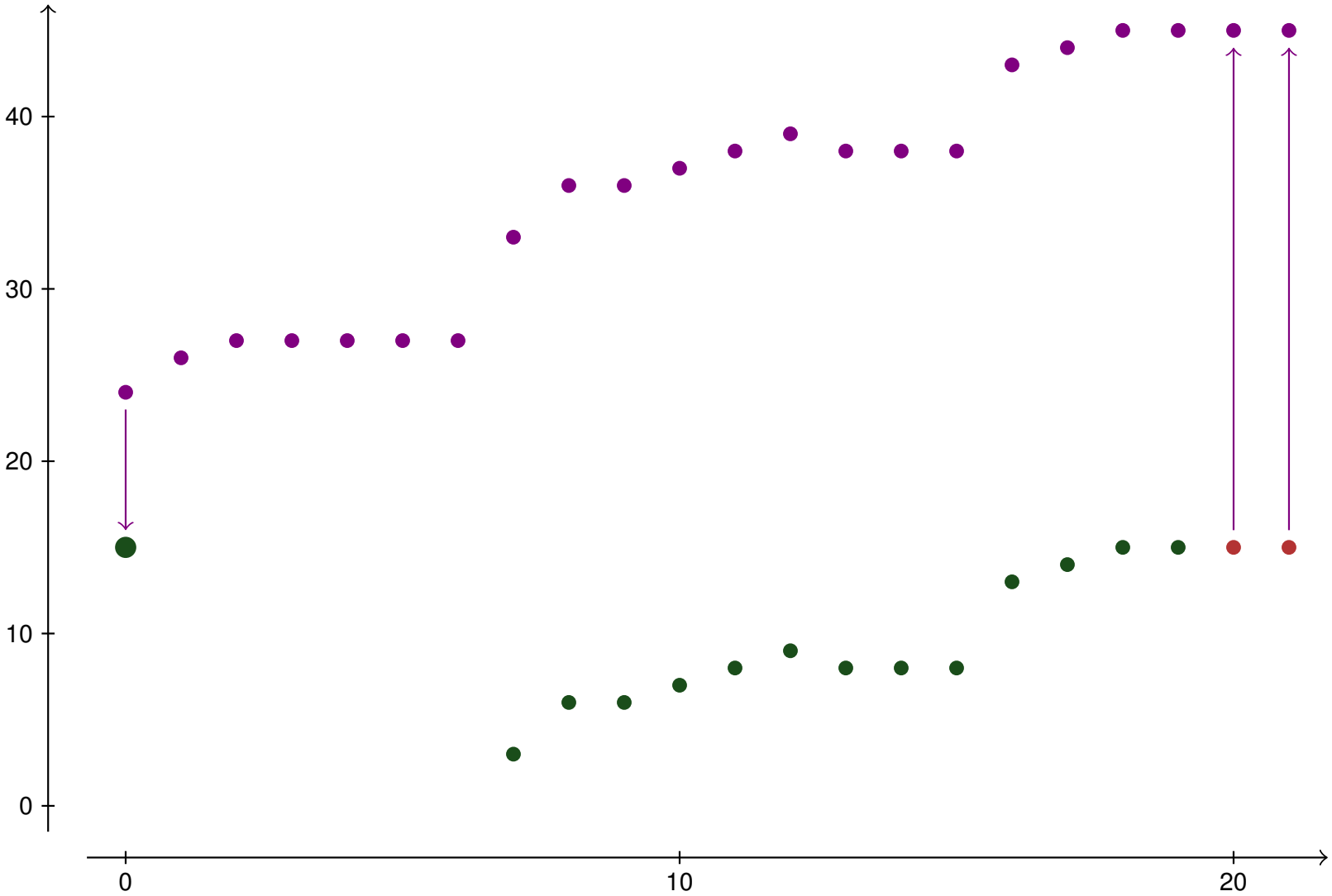
Une méthode naïve



Une méthode naïve



Une méthode naïve



Une méthode adaptative

Une méthode adaptative

Lemme clé

Une méthode adaptative

Lemme clé

On suppose $2V_{j+1} < N$.

Toute perturbation de (R_{j+1}, R_j) par un $O(p^{N+2V_{j+1}})$ est induite par une perturbation de (A, B) par un $O(p^N)$.

Une méthode adaptative

Lemme clé

On suppose $2V_{j+1} < N$.

Toute perturbation de (R_{j+1}, R_j) par un $O(p^{N+2V_{j+1}})$ est induite par une perturbation de (A, B) par un $O(p^N)$.

Démonstration par le calcul différentiel

Une méthode adaptative

Lemme clé

On suppose $2V_{j+1} < N$.

Toute perturbation de (R_{j+1}, R_j) par un $O(p^{N+2V_{j+1}})$ est induite par une perturbation de (A, B) par un $O(p^N)$.

Démonstration par le calcul différentiel

Une itération dans l'algorithme

Une méthode adaptative

Lemme clé

On suppose $2V_{j+1} < N$.

Toute perturbation de (R_{j+1}, R_j) par un $O(p^{N+2V_{j+1}})$ est induite par une perturbation de (A, B) par un $O(p^N)$.

Démonstration par le calcul différentiel

Une itération dans l'algorithme

Entrée : le couple (R_{j+1}, R_j) à précision $O(p^{N+2V_{j+1}})$

Sortie : le couple (R_j, R_{j-1}) à précision $O(p^{N+2V_j})$

Une méthode adaptative

Lemme clé

On suppose $2V_{j+1} < N$.

Toute perturbation de (R_{j+1}, R_j) par un $O(p^{N+2V_{j+1}})$ est induite par une perturbation de (A, B) par un $O(p^N)$.

Démonstration par le calcul différentiel

Une itération dans l'algorithme

Entrée : le couple (R_{j+1}, R_j) à précision $O(p^{N+2V_{j+1}})$

Sortie : le couple (R_j, R_{j-1}) à précision $O(p^{N+2V_j})$

1. relever (R_{j+1}, R_j) à précision $O(p^{N+2V_j+2V_{j+1}})$

Une méthode adaptative

Lemme clé

On suppose $2V_{j+1} < N$.

Toute perturbation de (R_{j+1}, R_j) par un $O(p^{N+2V_{j+1}})$ est induite par une perturbation de (A, B) par un $O(p^N)$.

Démonstration par le calcul différentiel

Une itération dans l'algorithme

Entrée : le couple (R_{j+1}, R_j) à précision $O(p^{N+2V_{j+1}})$

Sortie : le couple (R_j, R_{j-1}) à précision $O(p^{N+2V_j})$

1. relever (R_{j+1}, R_j) à précision $O(p^{N+2V_j+2V_{j+1}})$
2. calculer R_{j-1} à précision $O(p^{N+2V_j})$

Une méthode adaptative

Lemme clé

On suppose $2V_{j+1} < N$.

Toute perturbation de (R_{j+1}, R_j) par un $O(p^{N+2V_{j+1}})$ est induite par une perturbation de (A, B) par un $O(p^N)$.

Démonstration par le calcul différentiel

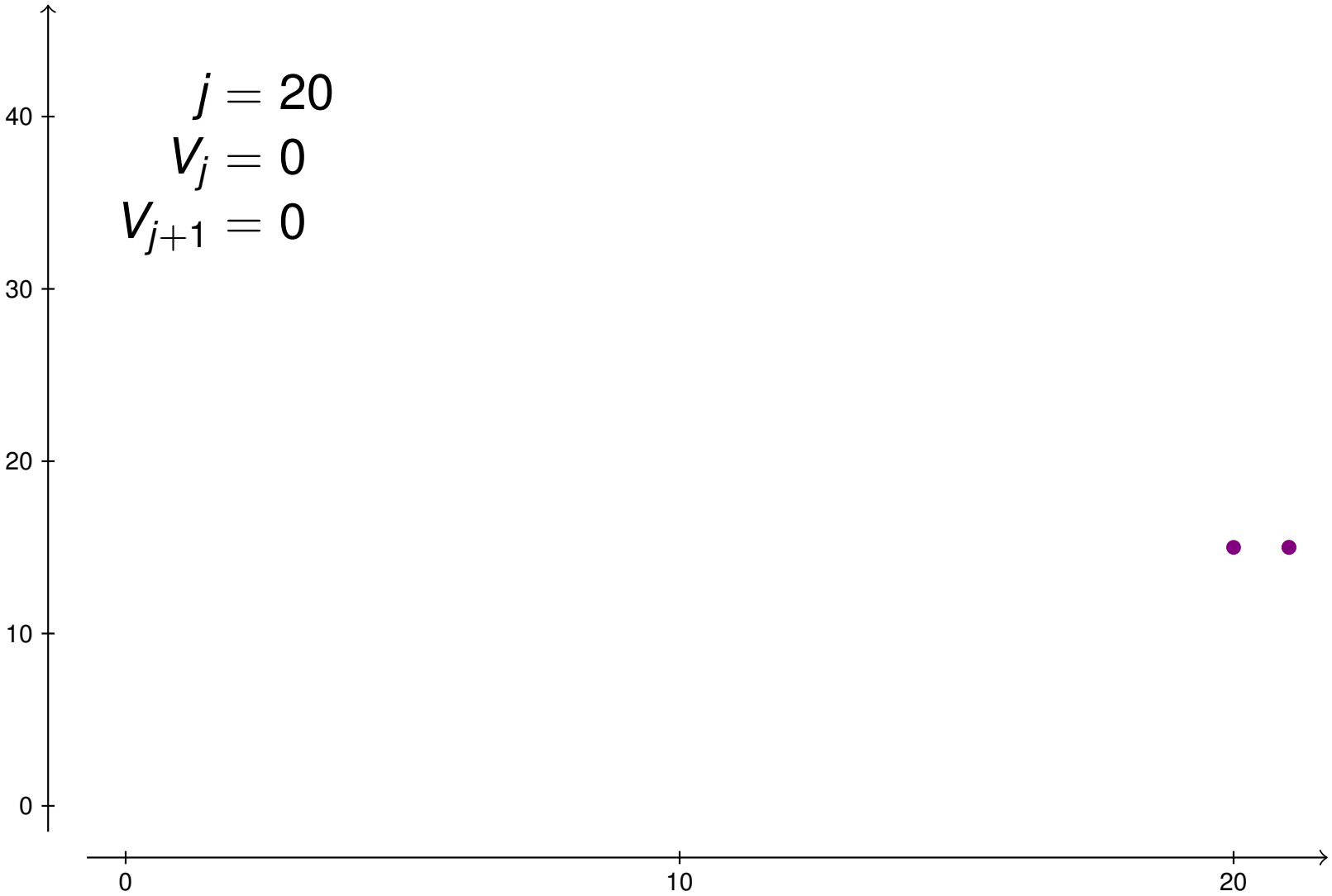
Une itération dans l'algorithme

Entrée : le couple (R_{j+1}, R_j) à précision $O(p^{N+2V_{j+1}})$

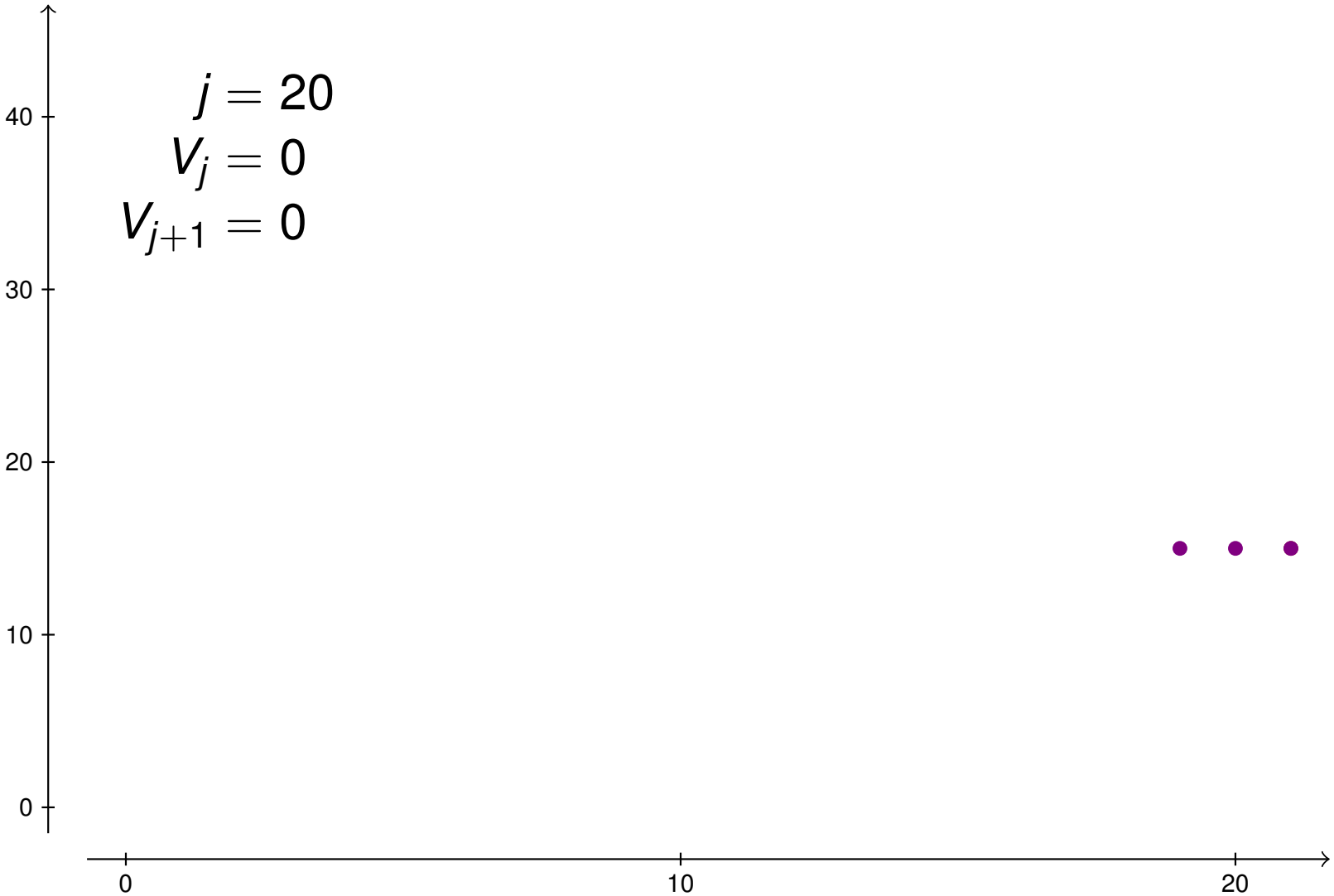
Sortie : le couple (R_j, R_{j-1}) à précision $O(p^{N+2V_j})$

1. relever (R_{j+1}, R_j) à précision $O(p^{N+2V_j+2V_{j+1}})$
2. calculer R_{j-1} à précision $O(p^{N+2V_j})$
3. renvoyer (R_j, R_{j-1}) à précision $O(p^{N+2V_j})$

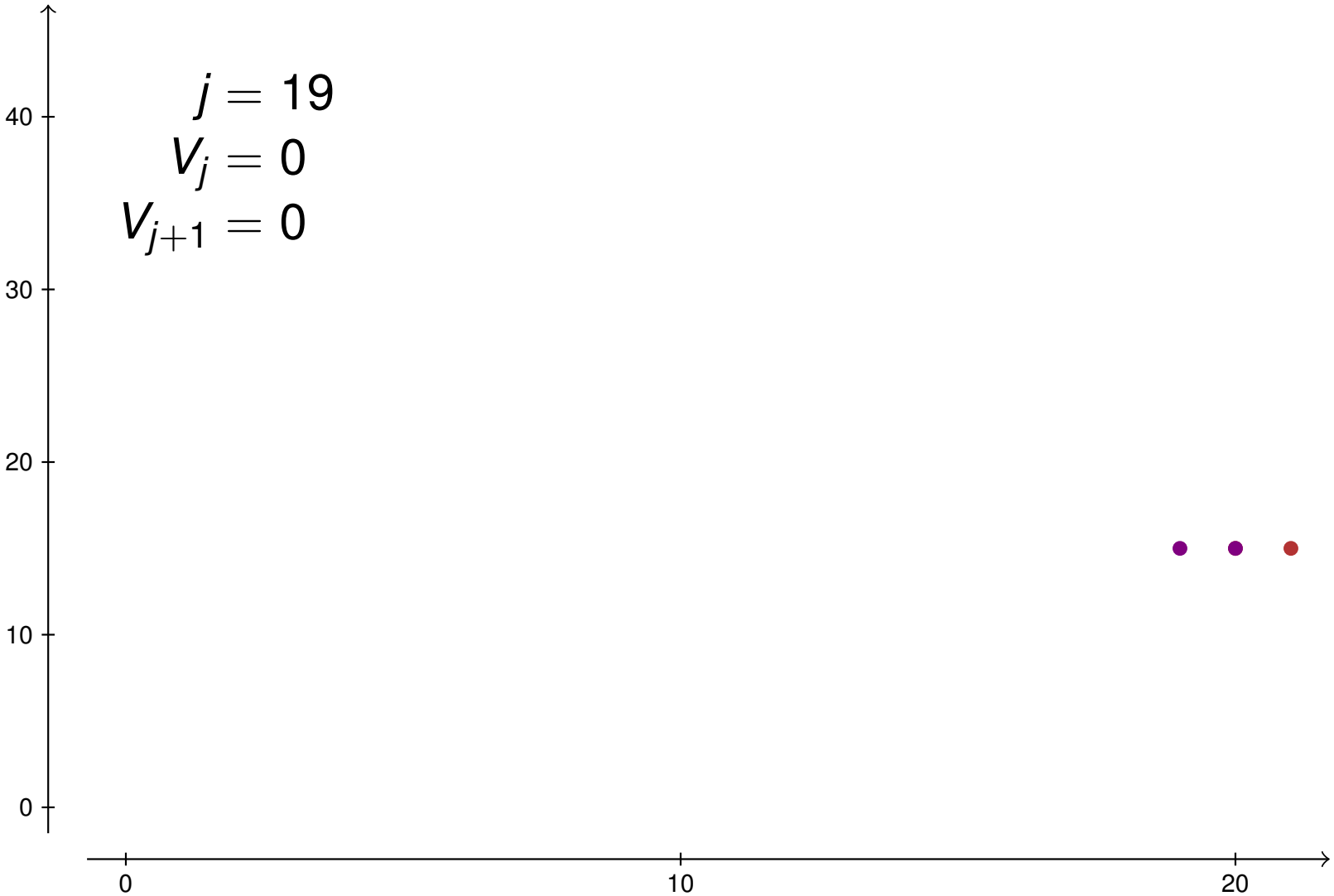
Une méthode adaptative



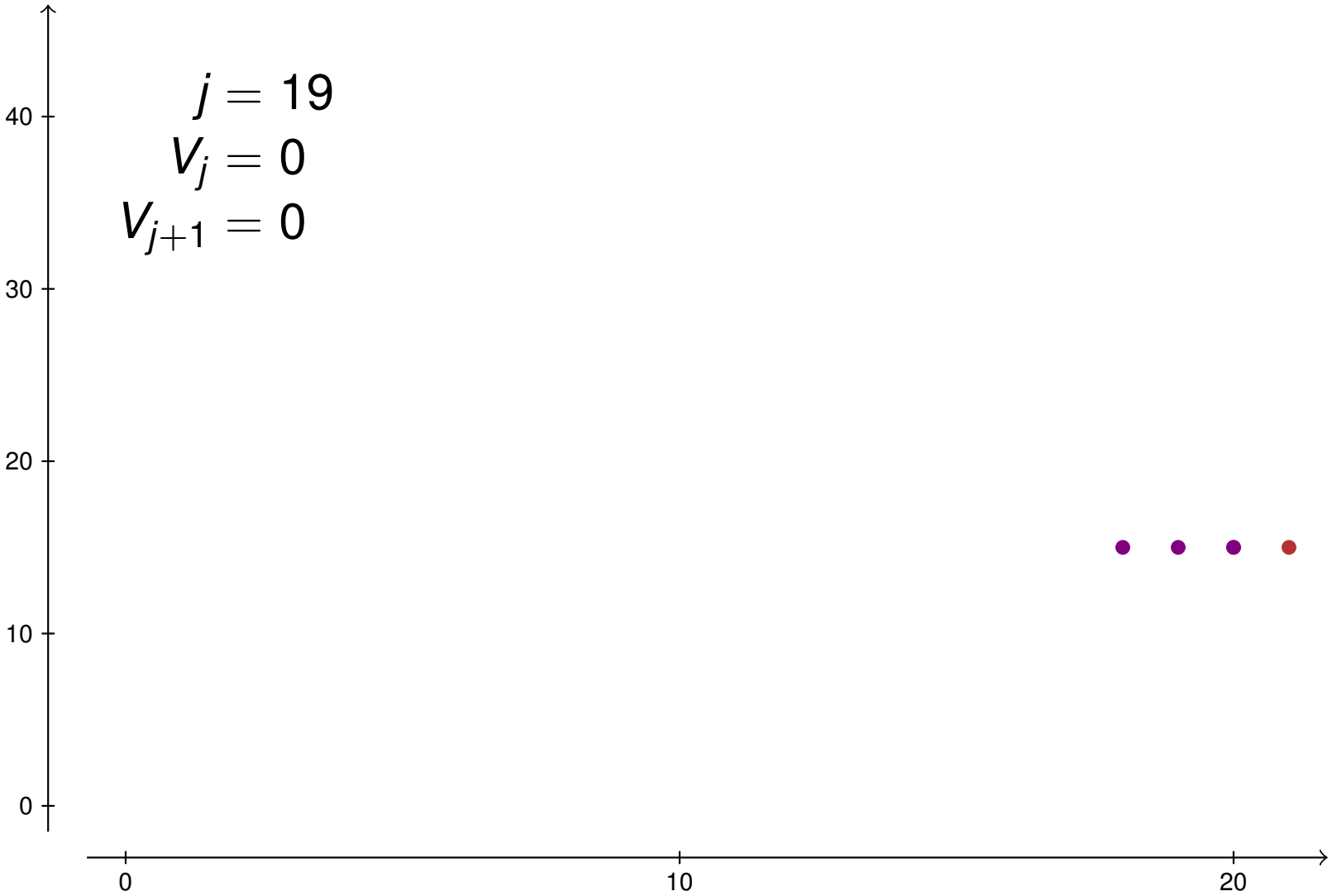
Une méthode adaptative



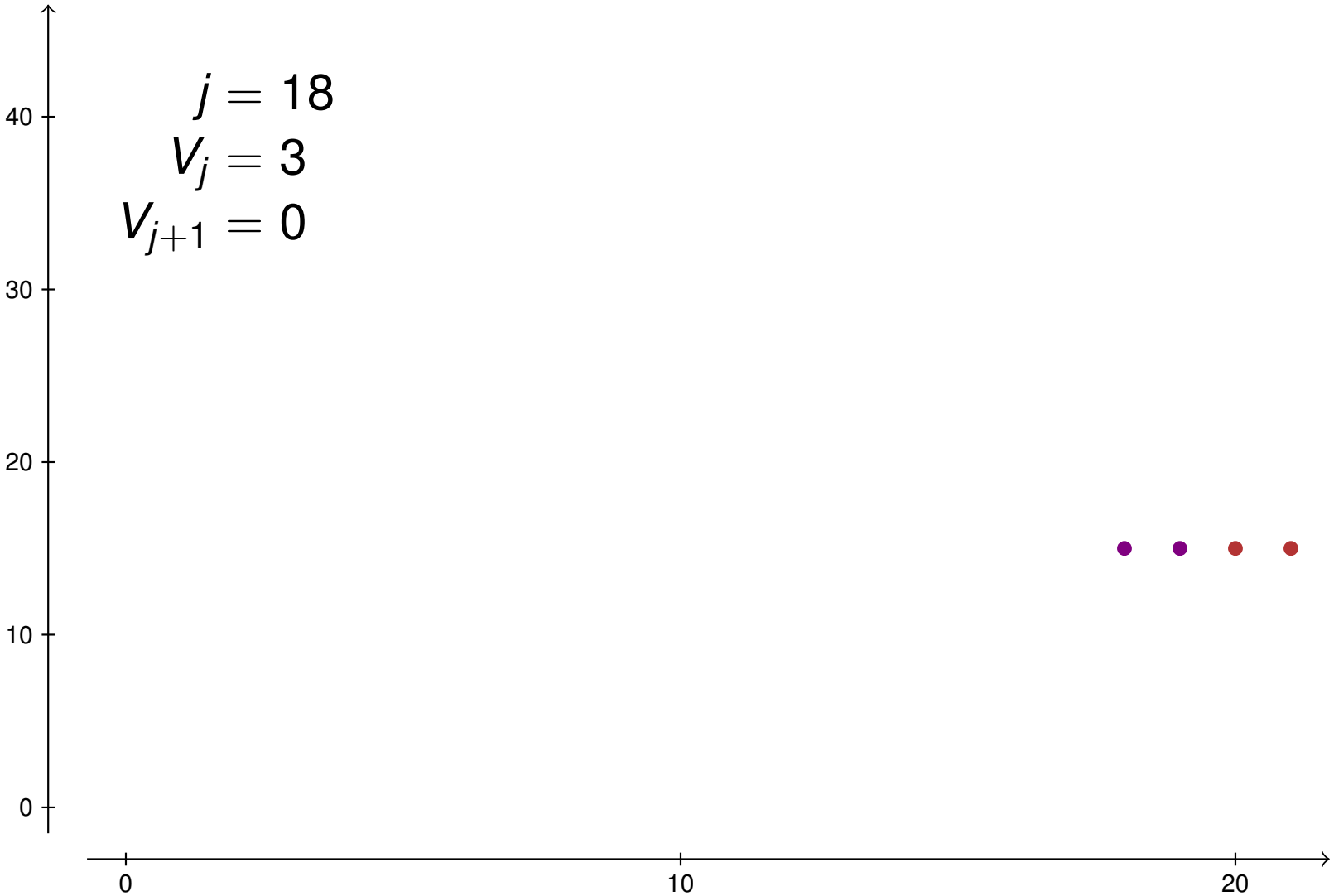
Une méthode adaptative



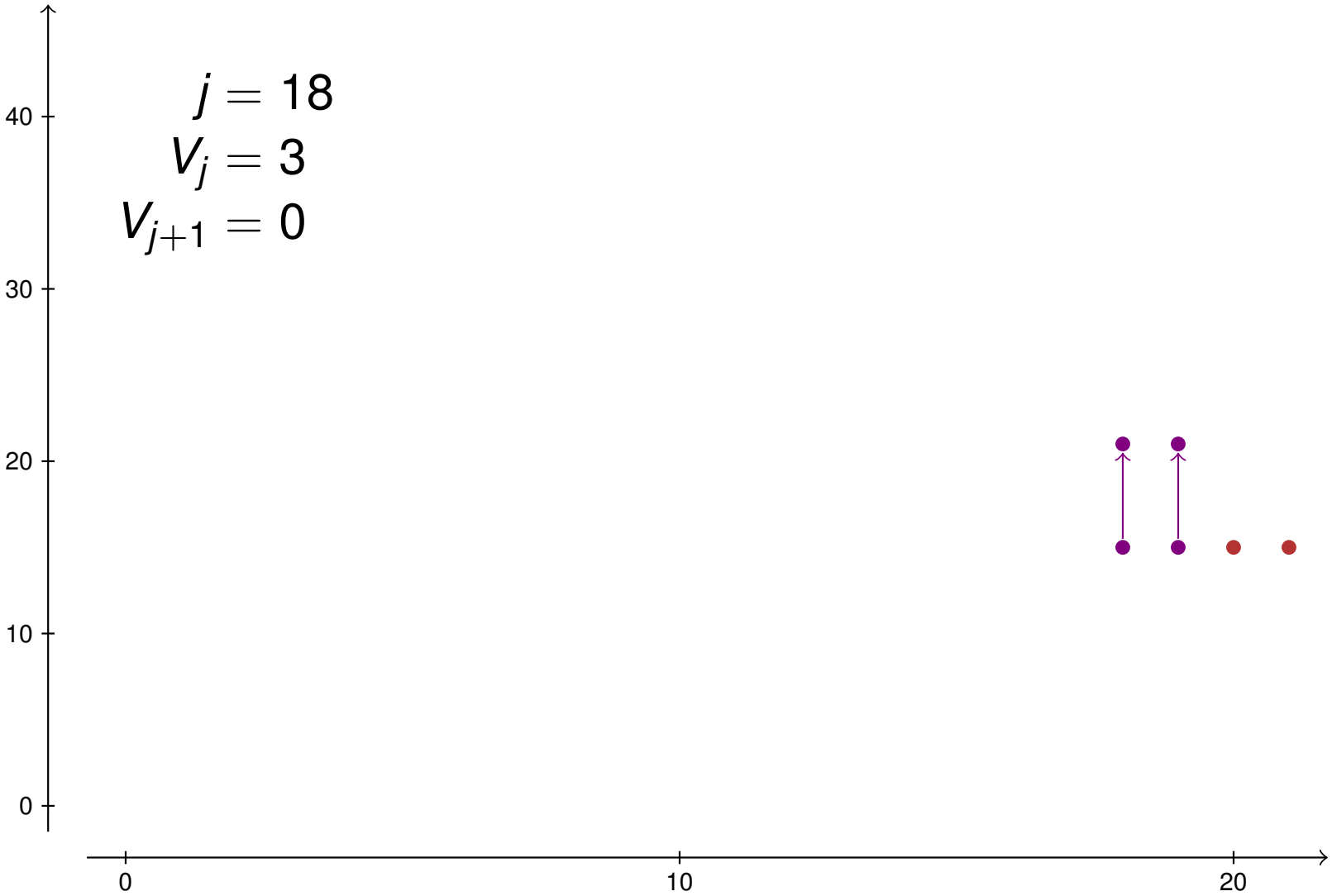
Une méthode adaptative



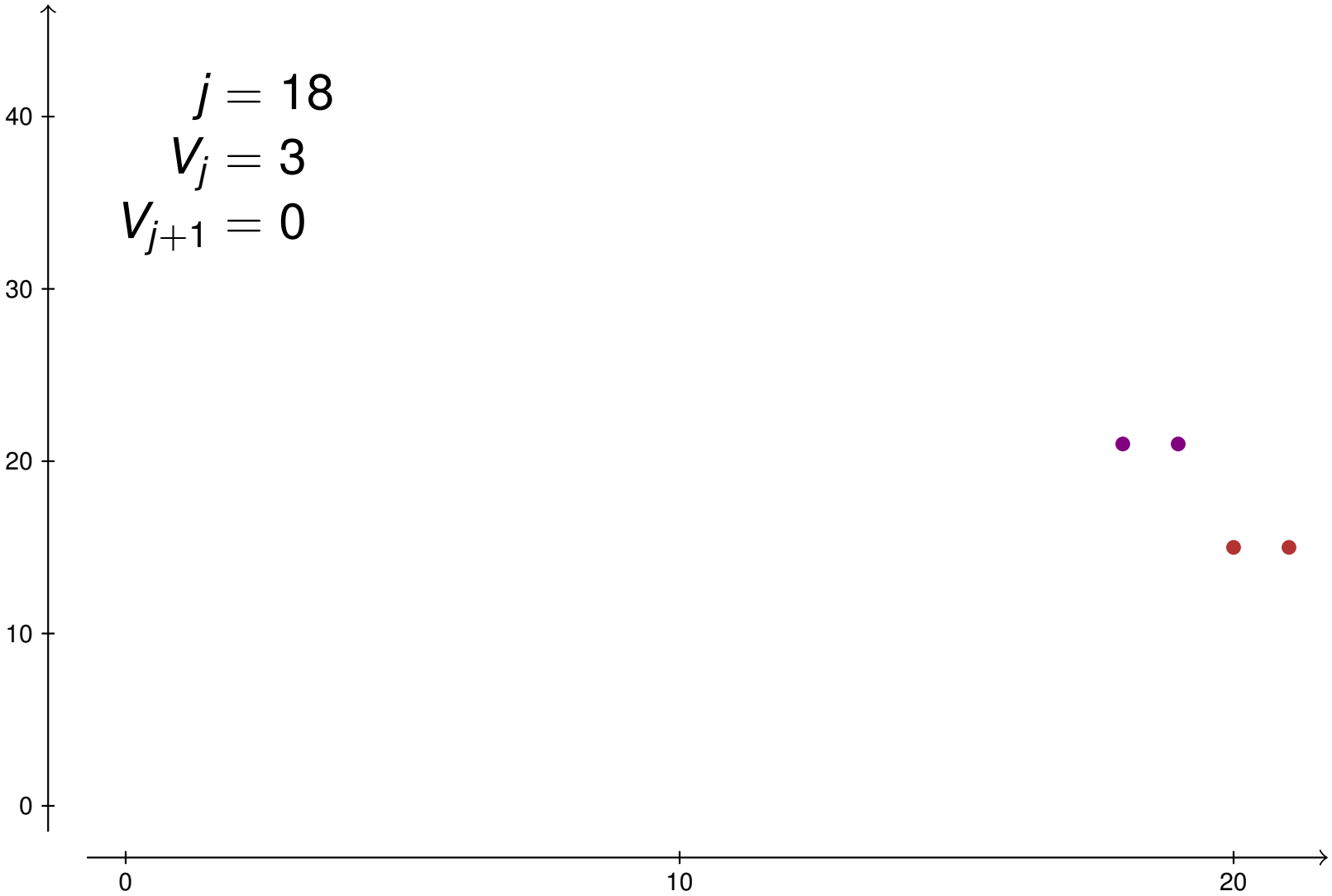
Une méthode adaptative



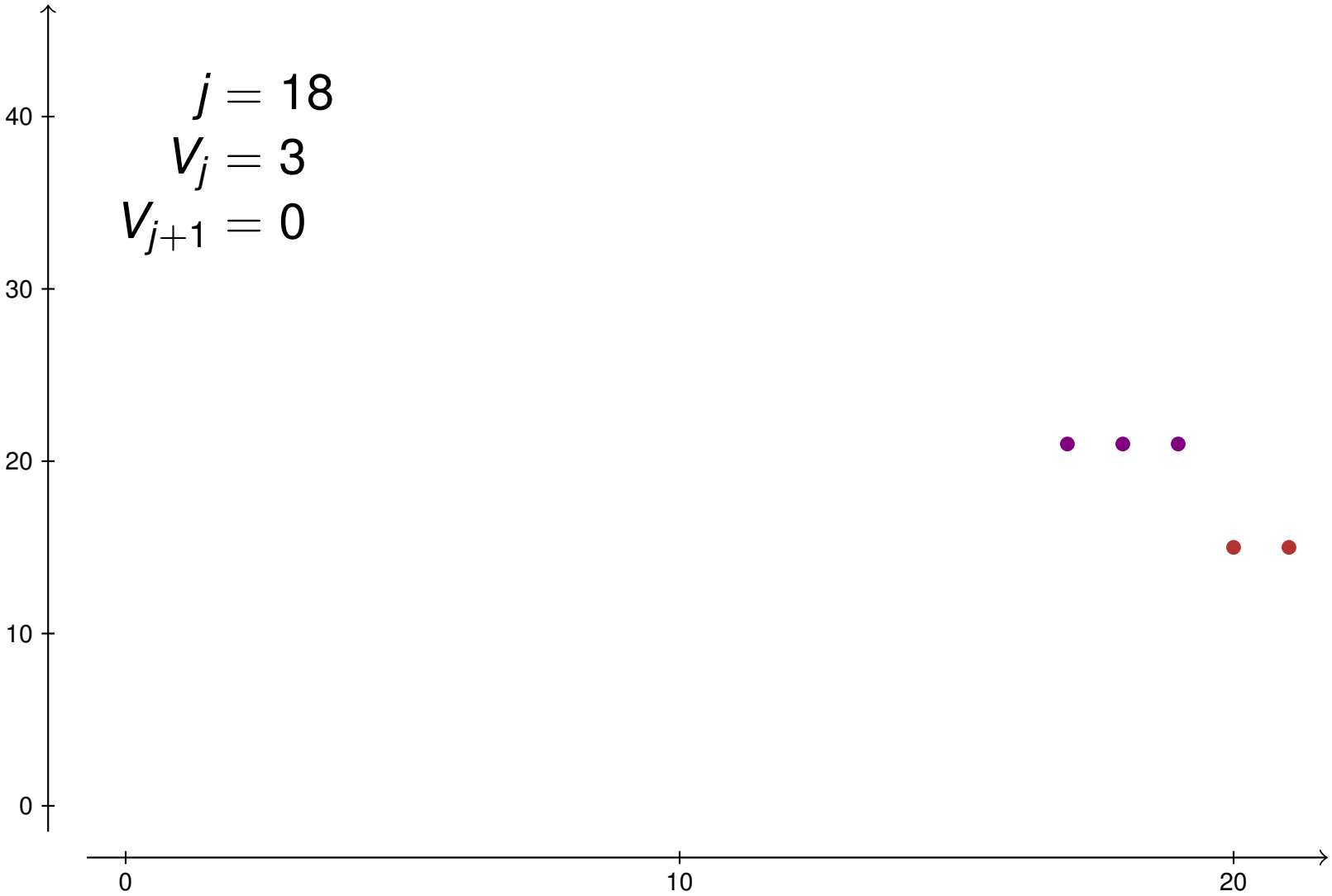
Une méthode adaptative



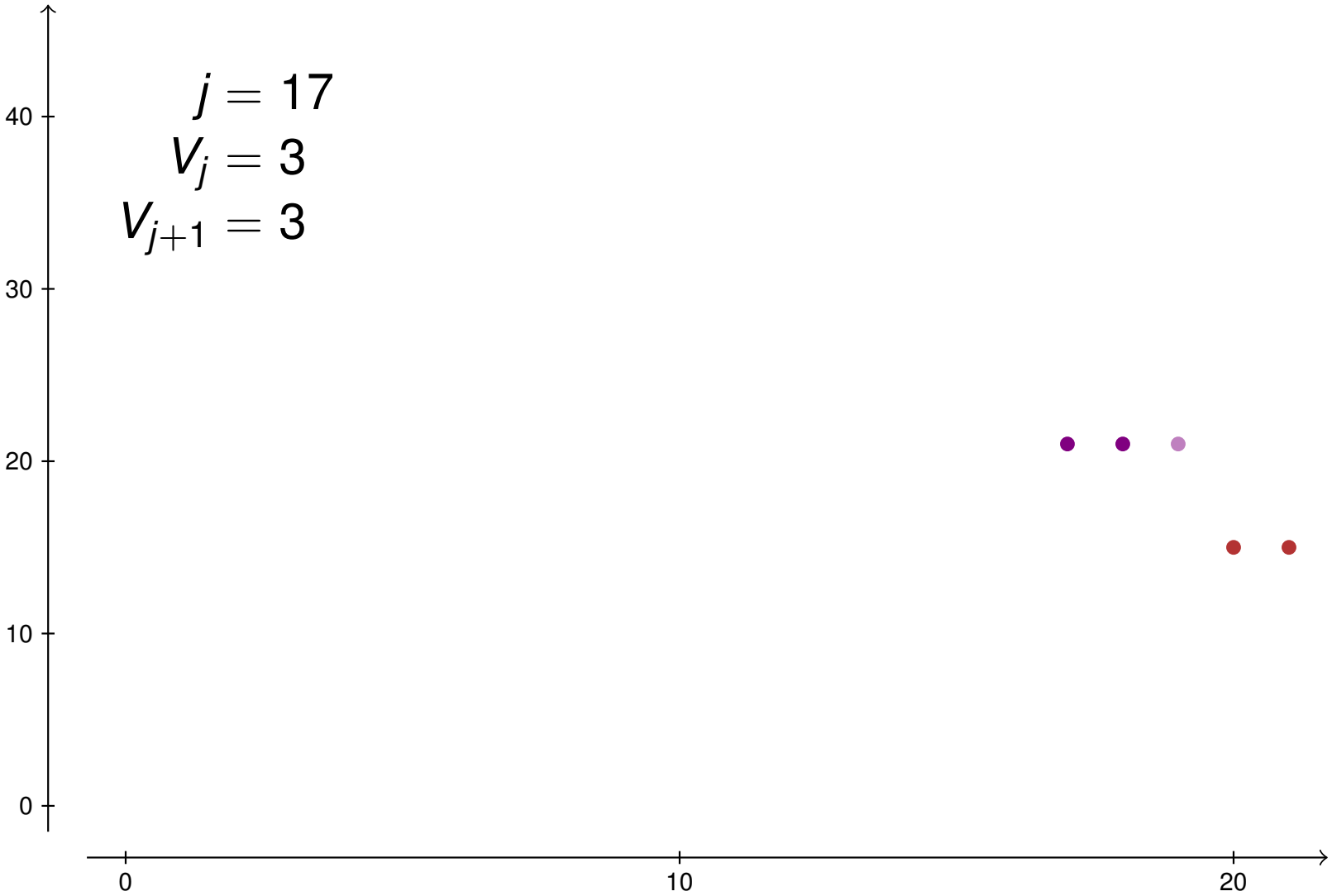
Une méthode adaptative



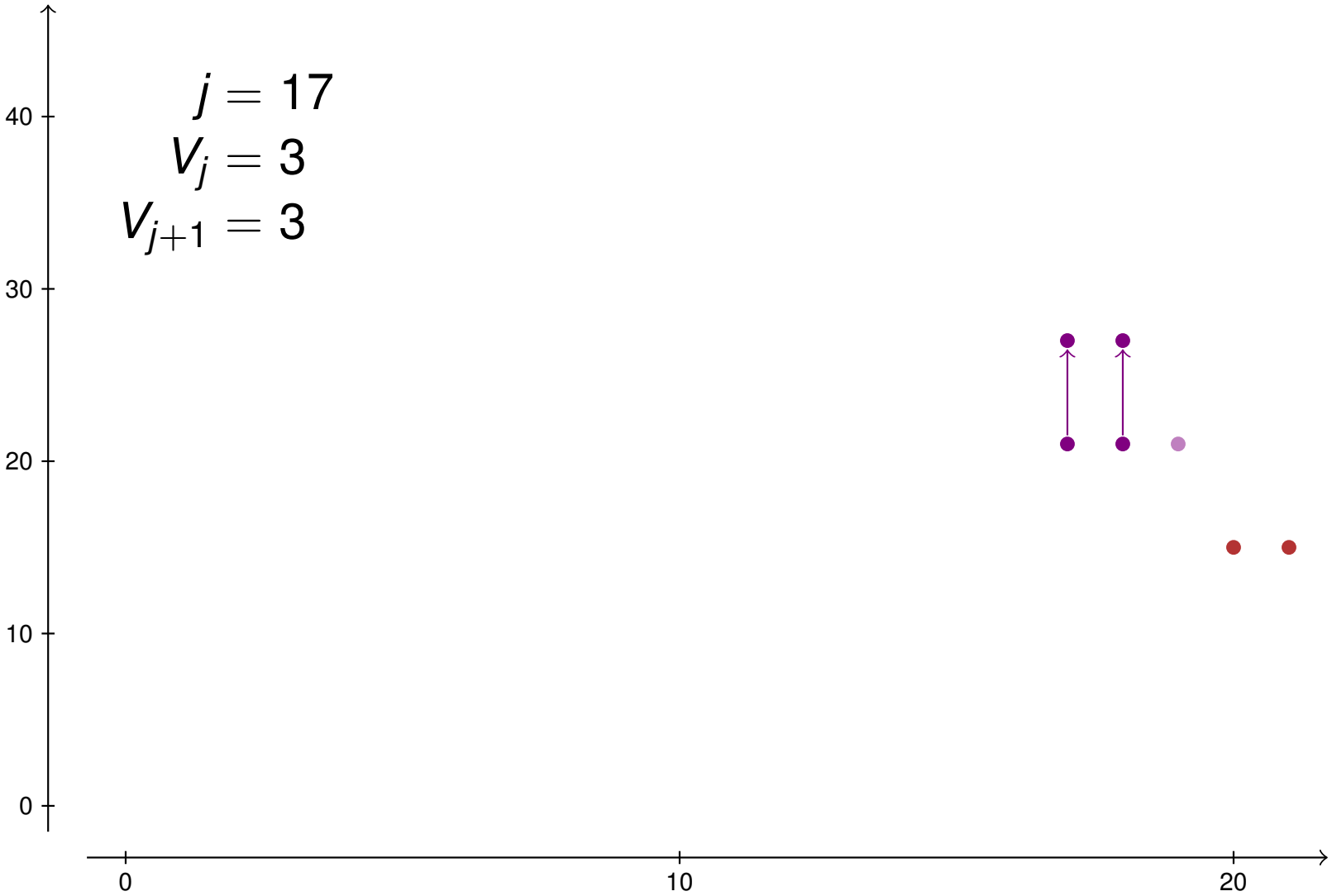
Une méthode adaptative



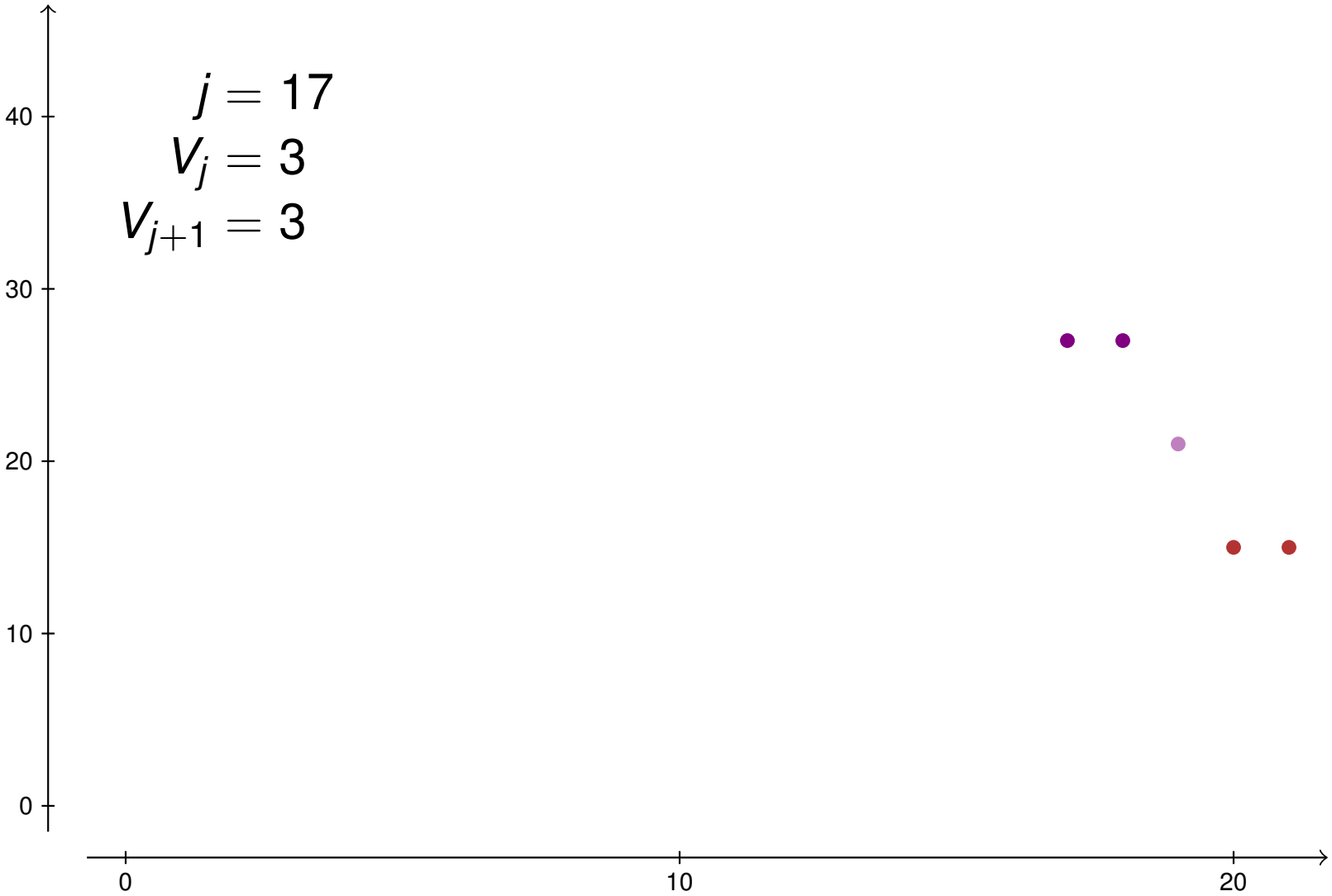
Une méthode adaptative



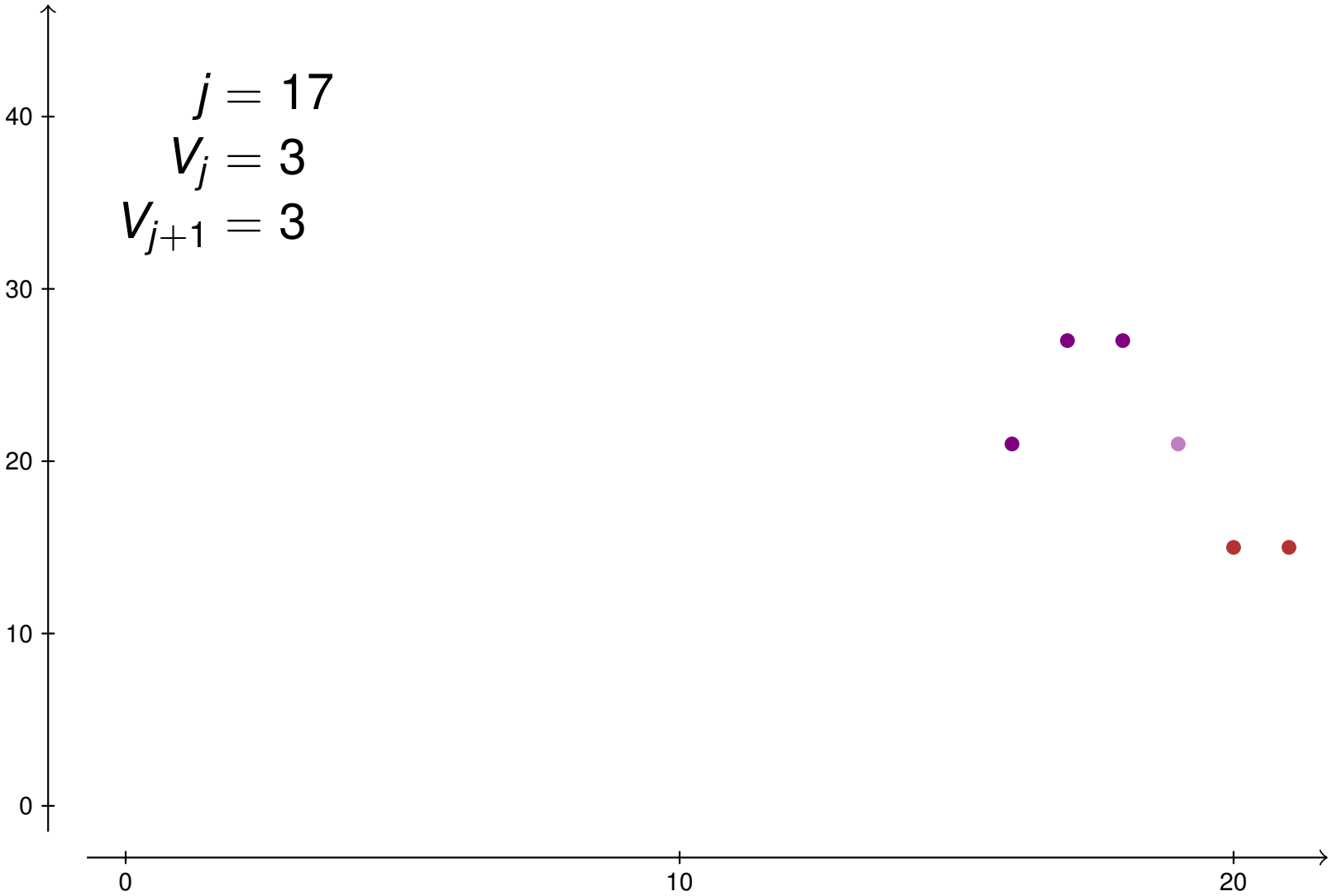
Une méthode adaptative



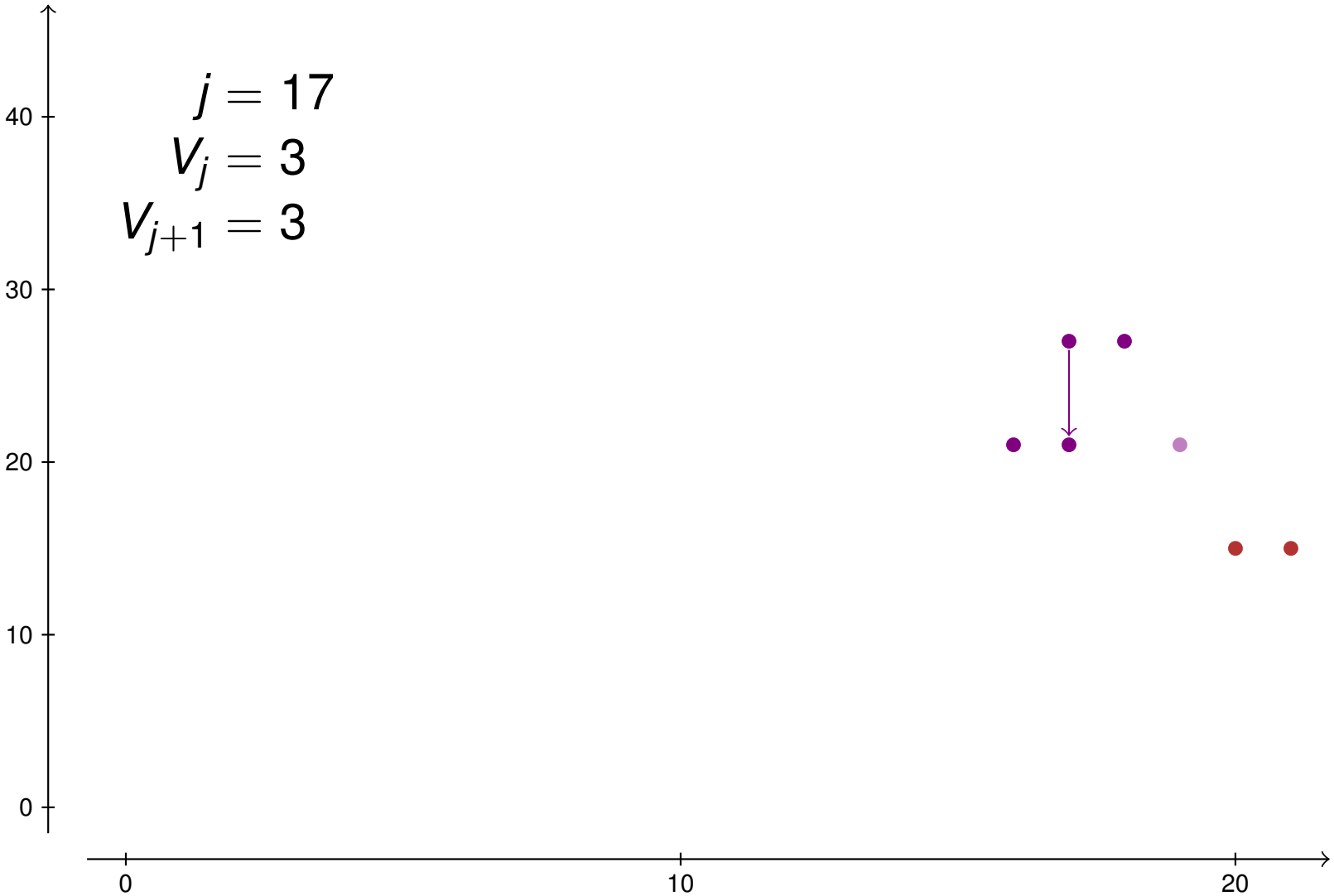
Une méthode adaptative



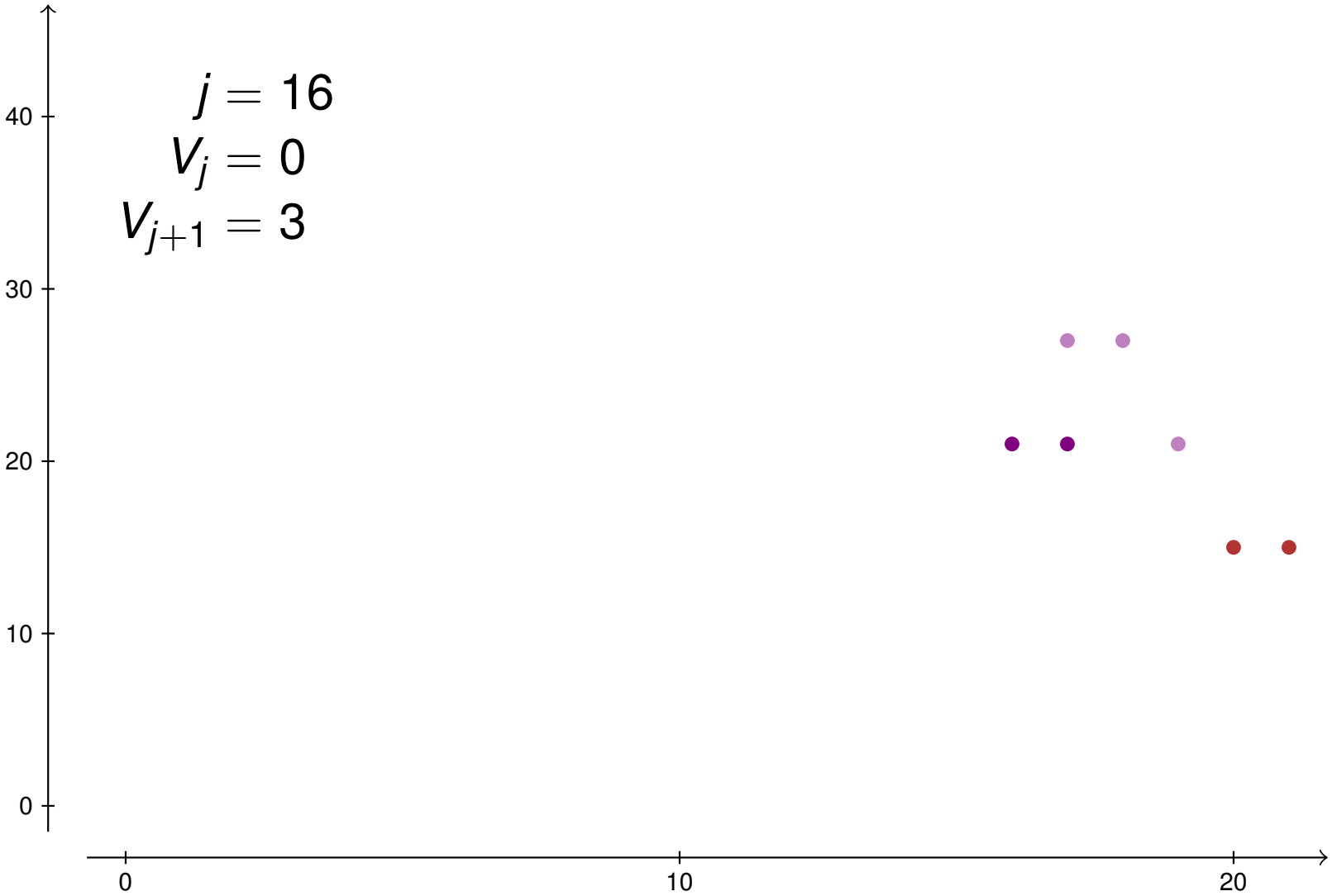
Une méthode adaptative



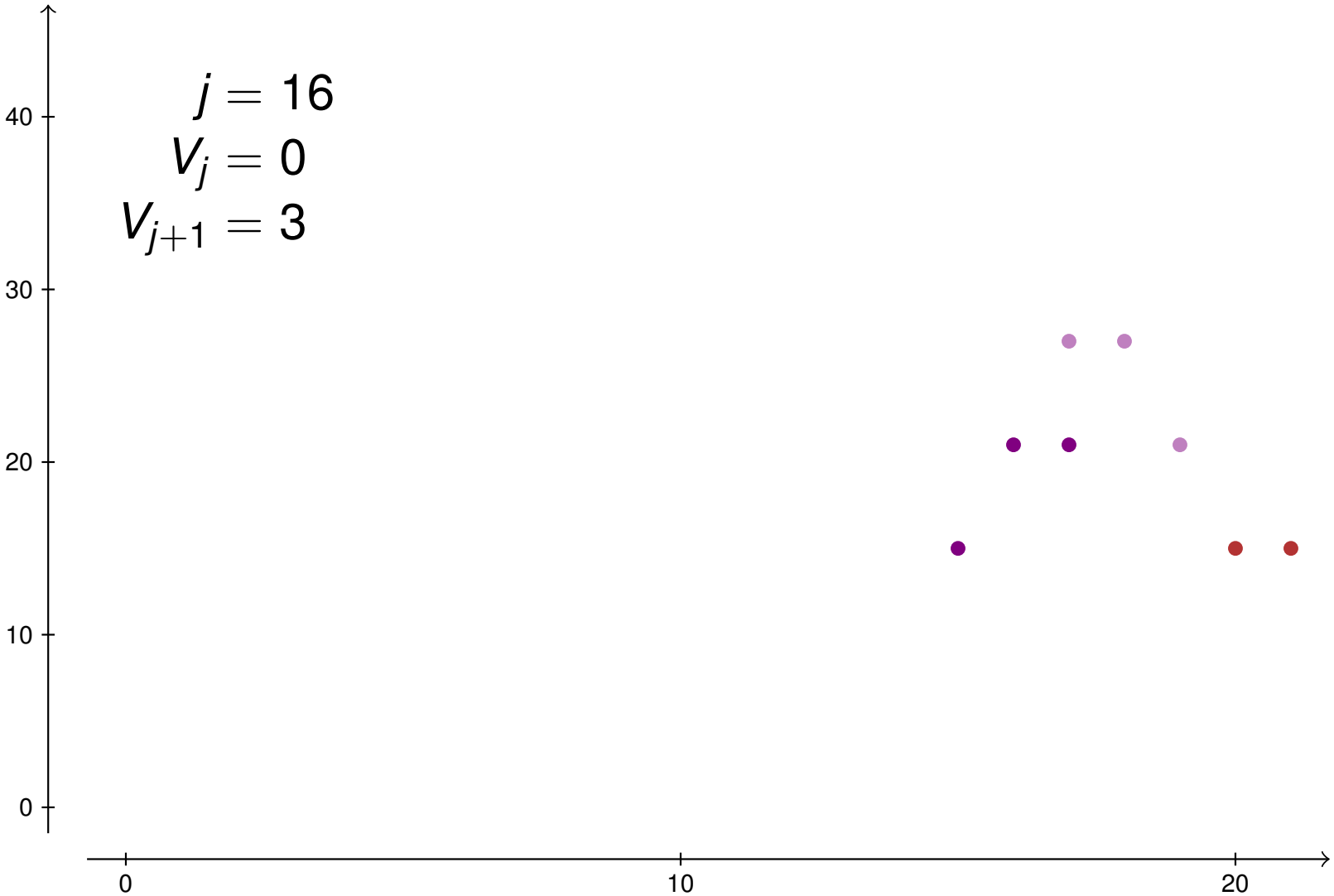
Une méthode adaptative



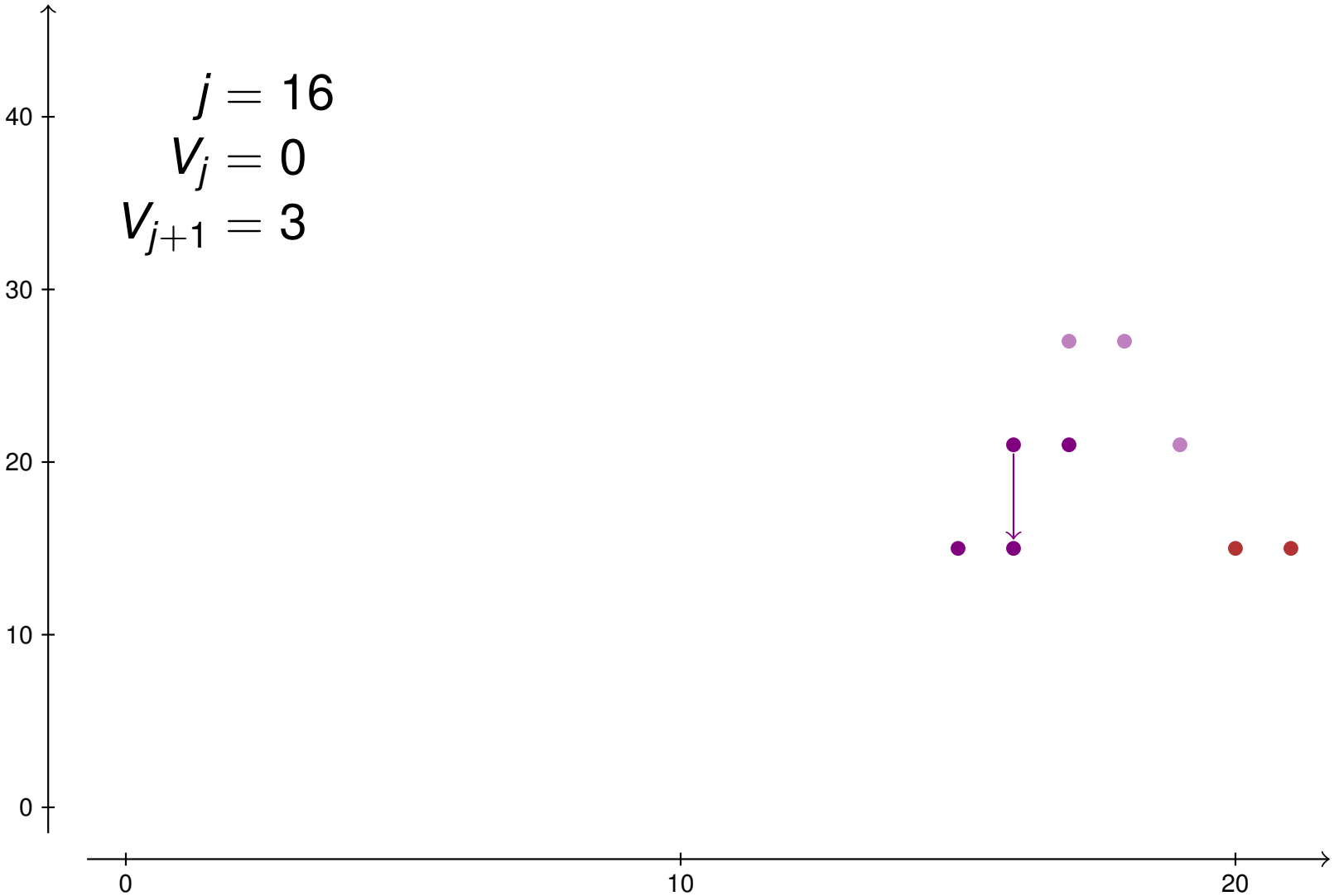
Une méthode adaptative



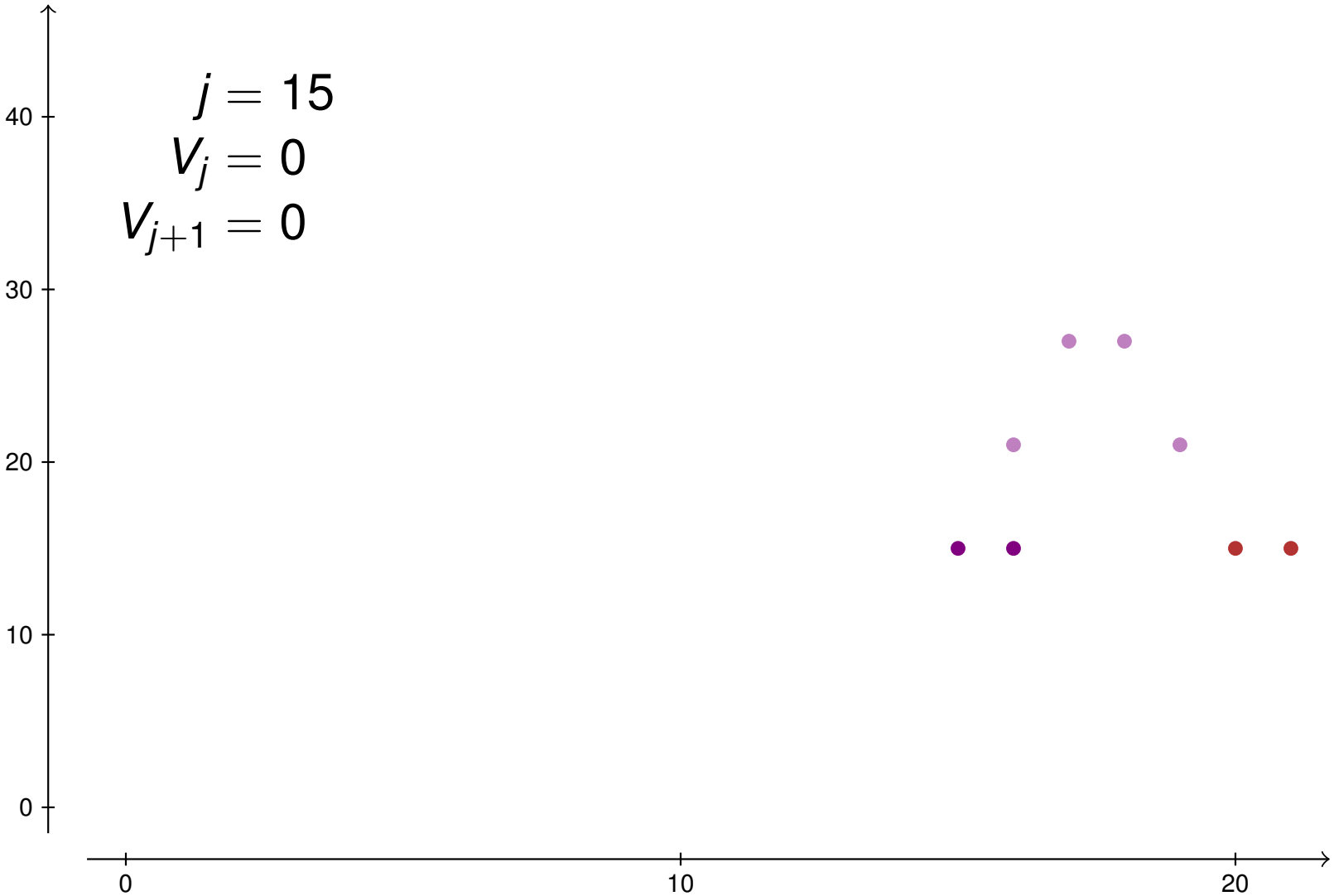
Une méthode adaptative



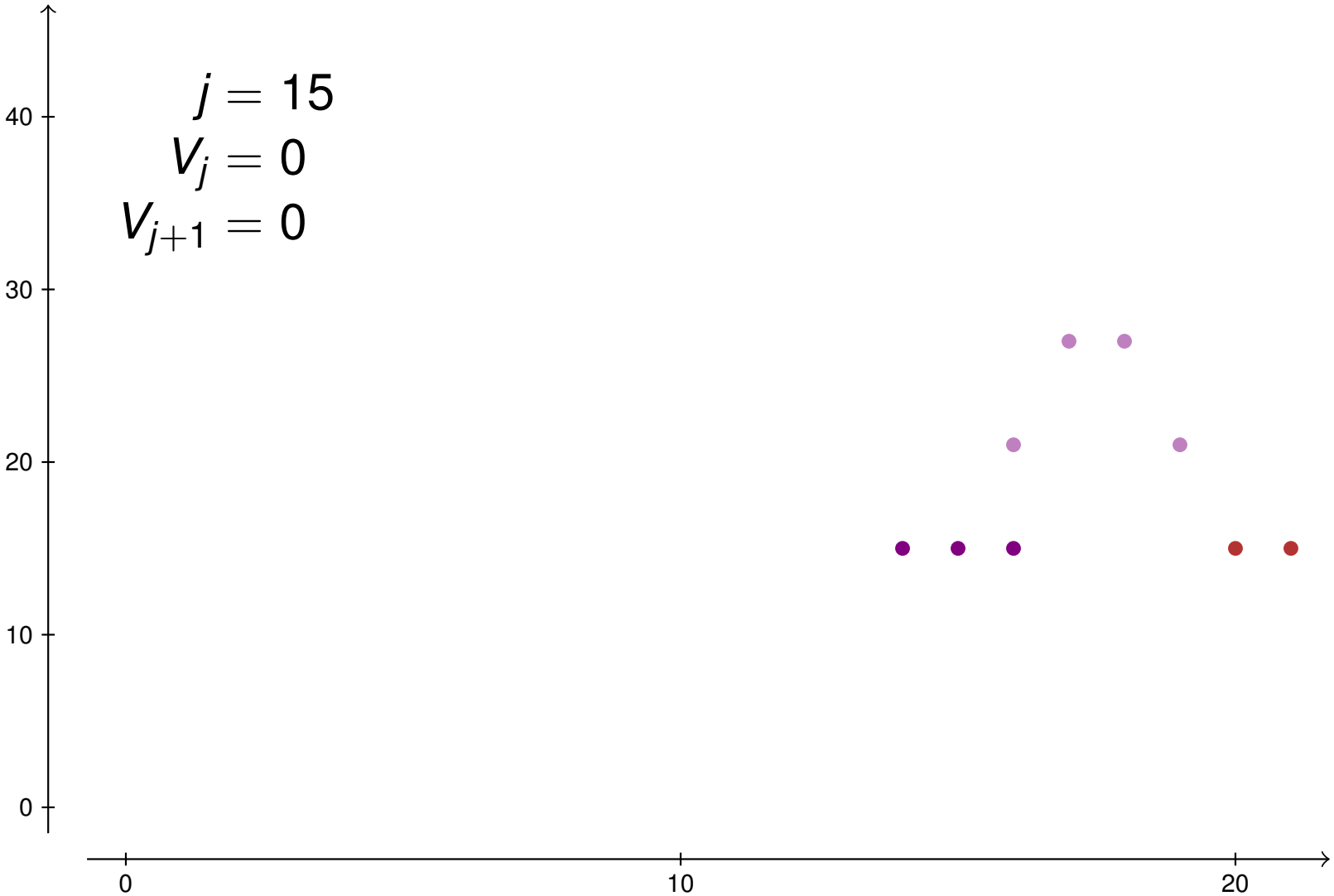
Une méthode adaptative



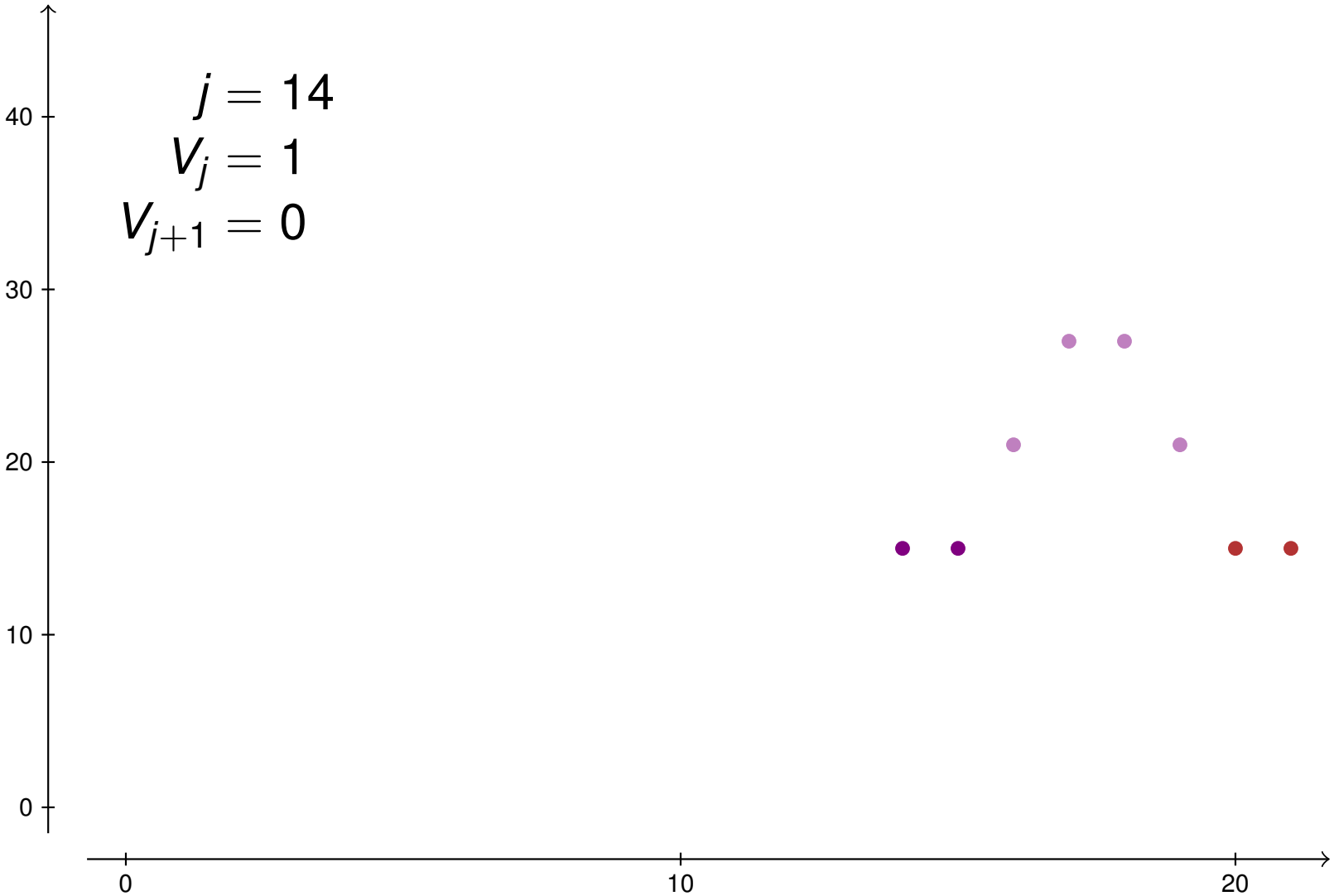
Une méthode adaptative



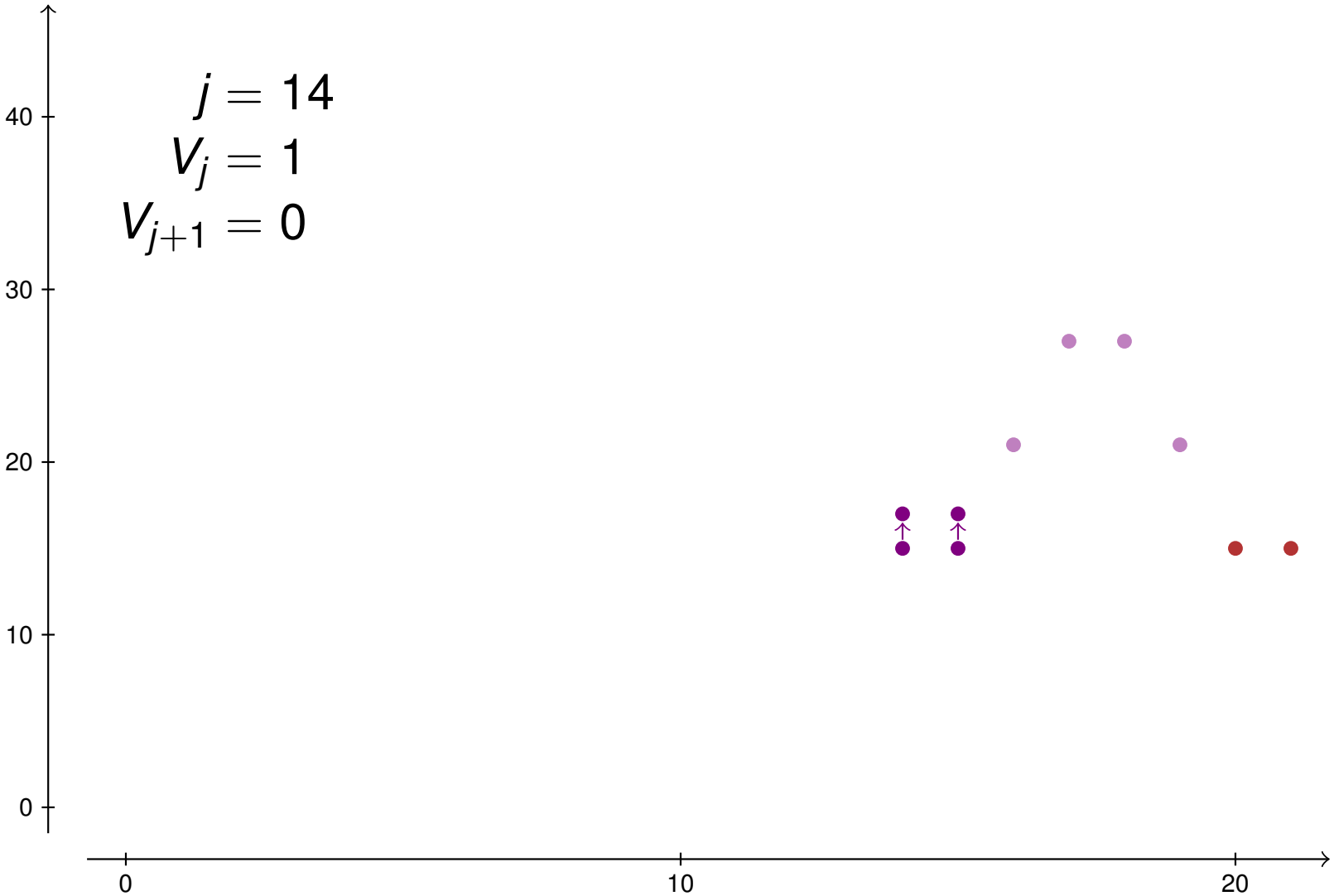
Une méthode adaptative



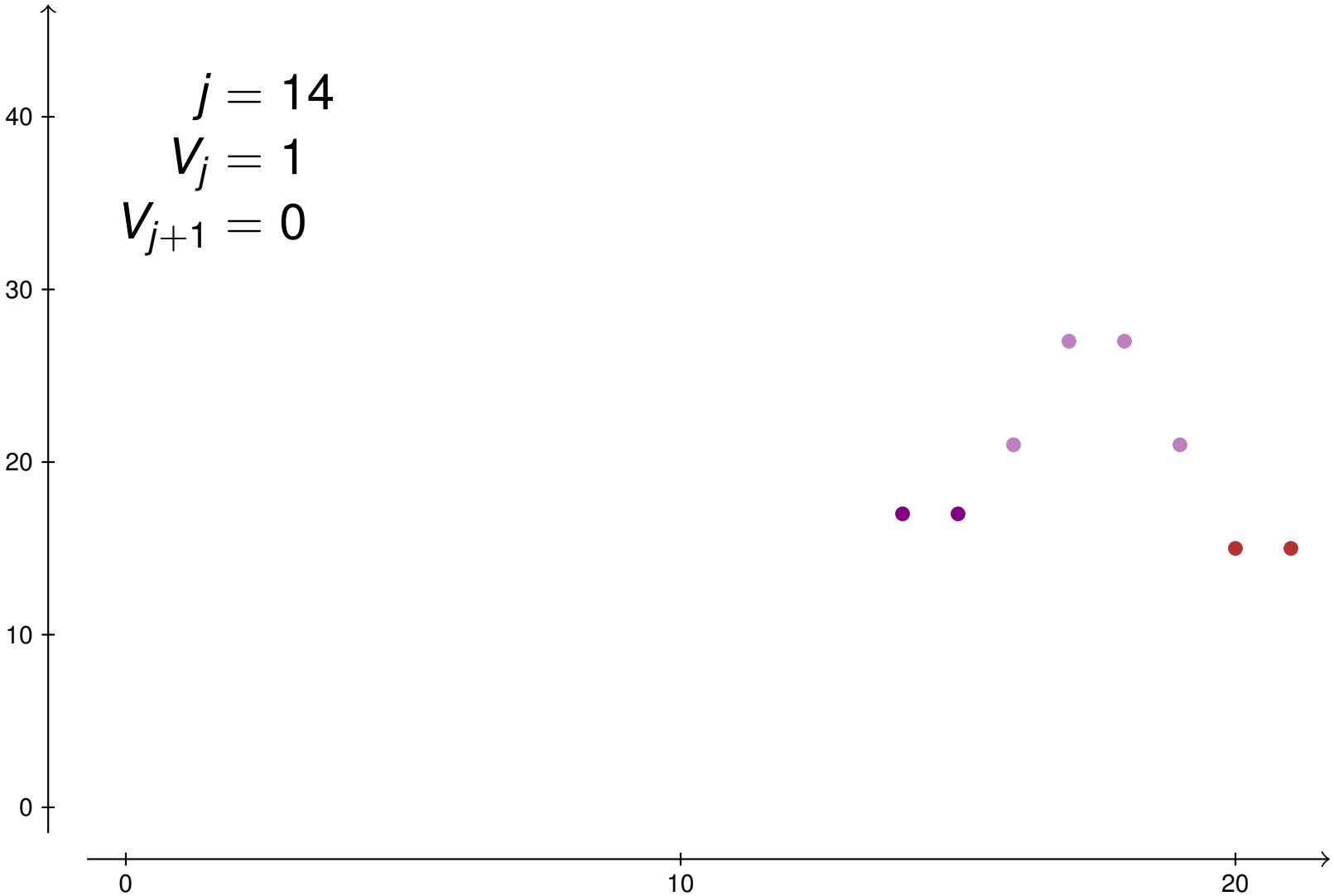
Une méthode adaptative



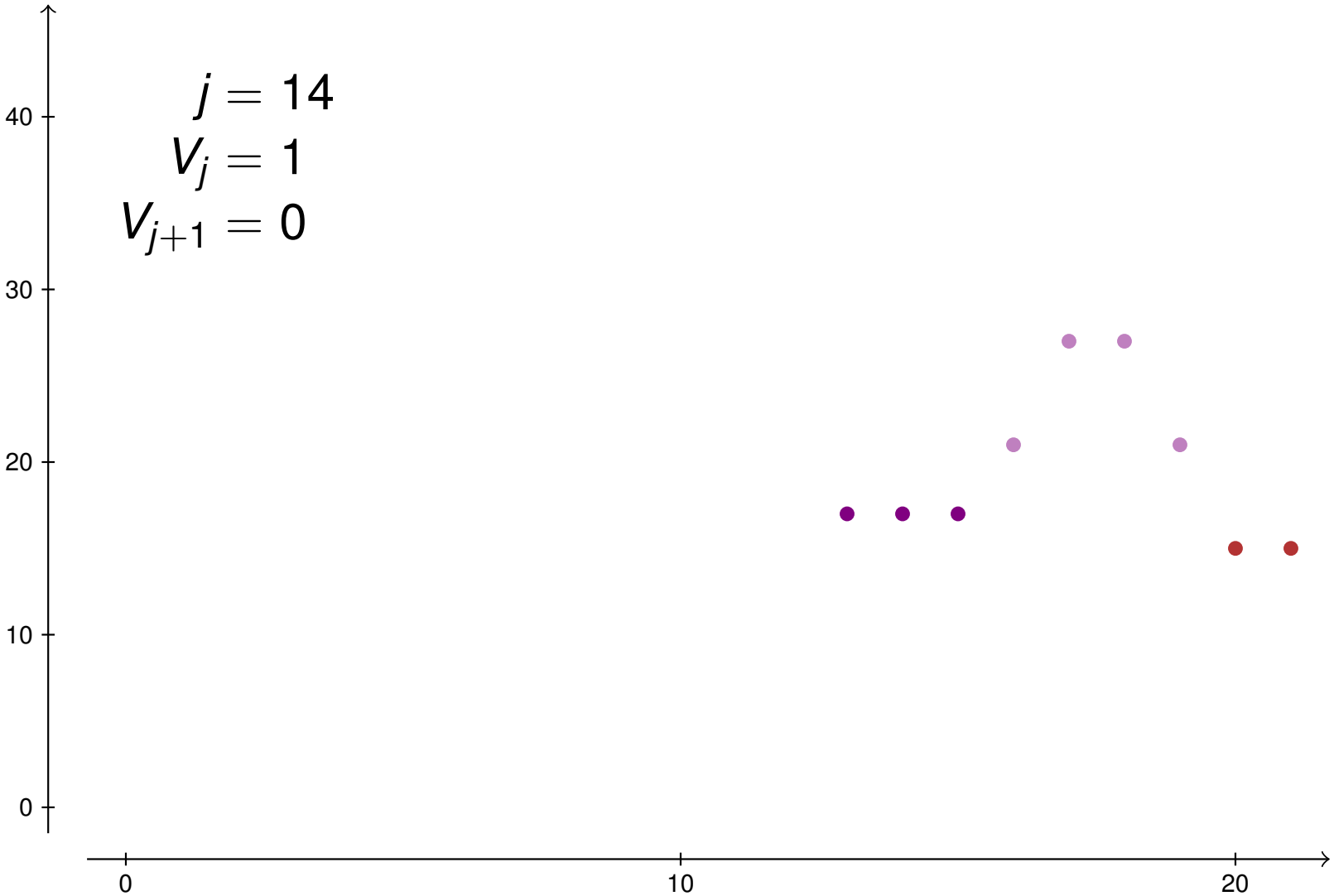
Une méthode adaptative



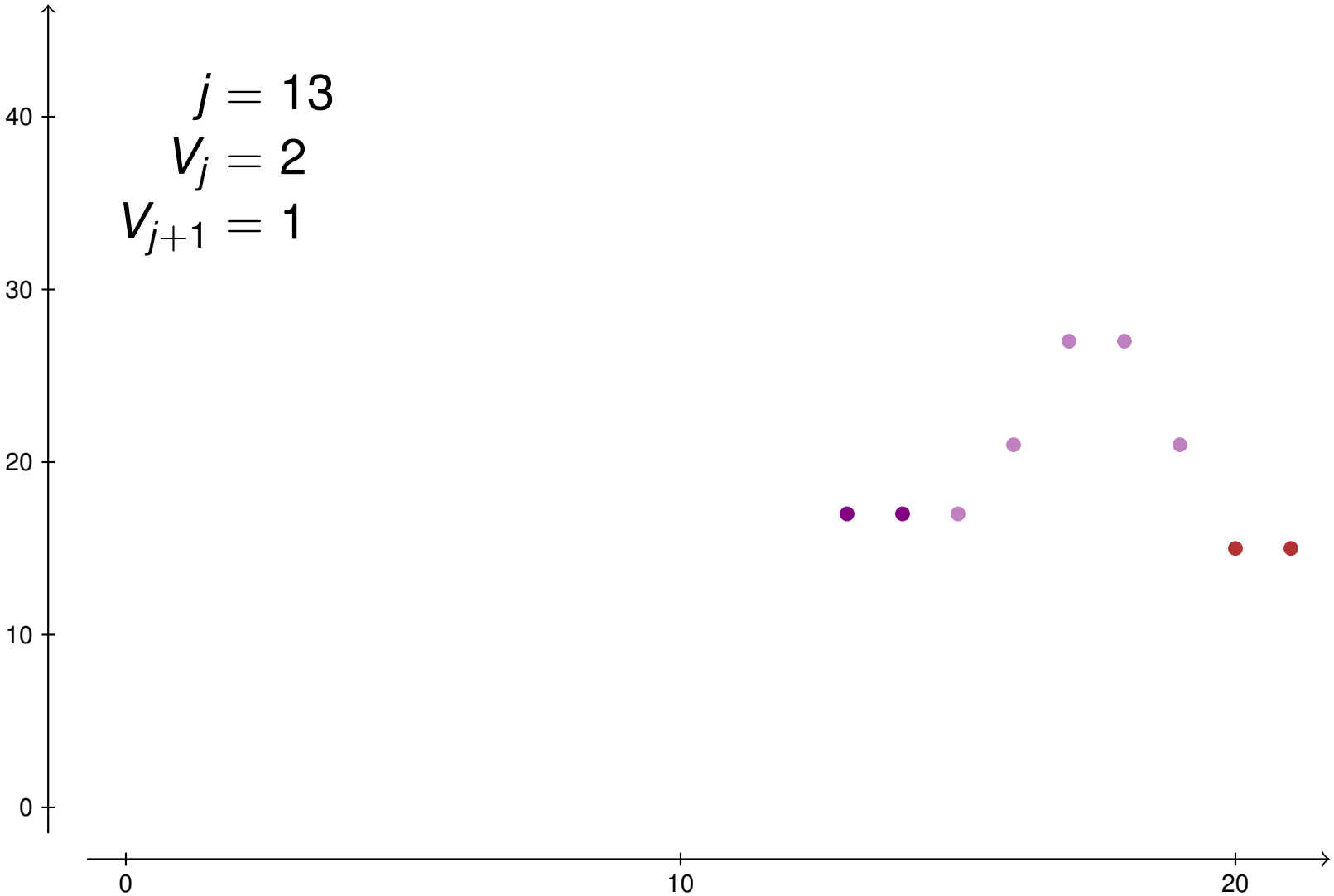
Une méthode adaptative



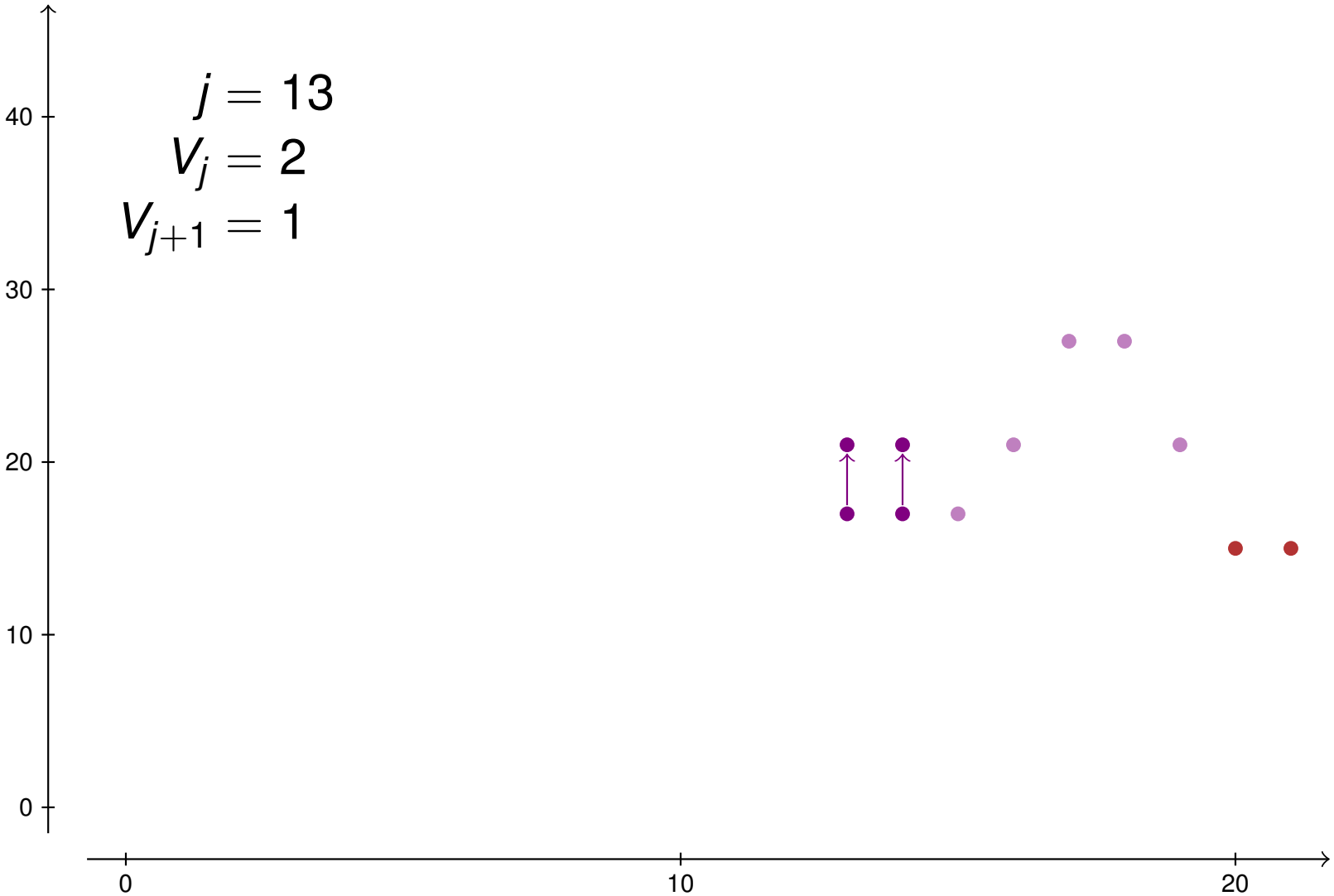
Une méthode adaptative



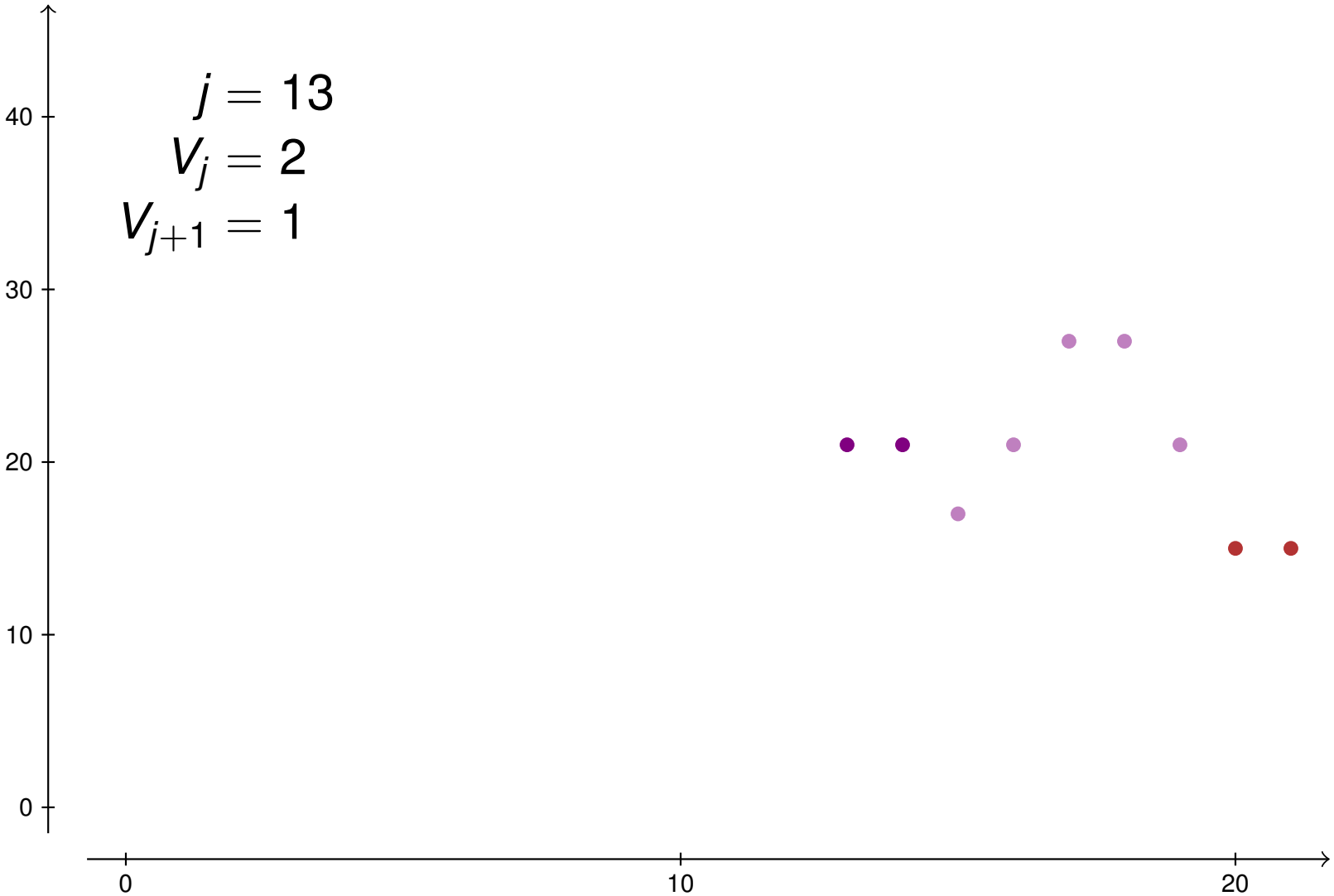
Une méthode adaptative



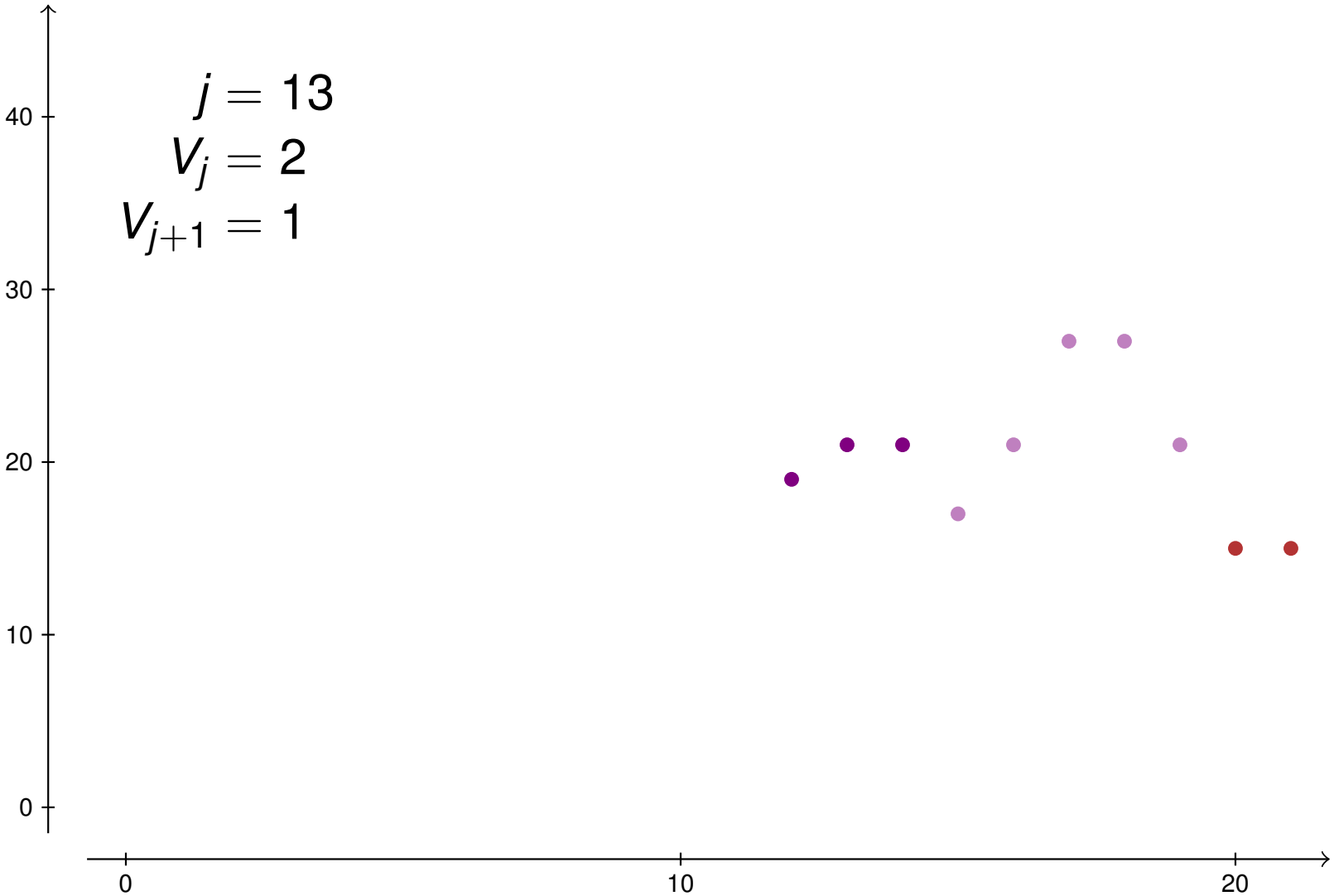
Une méthode adaptative



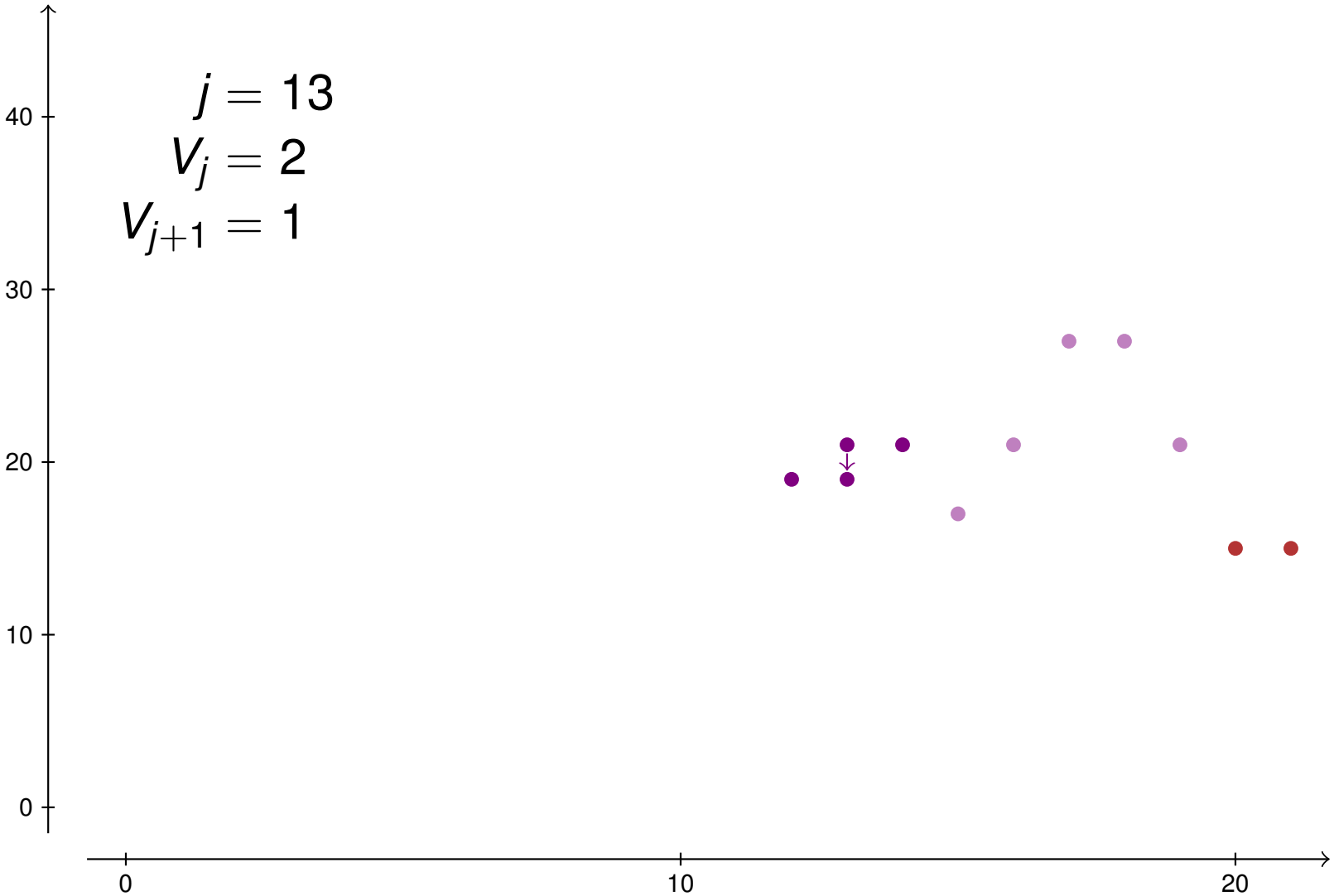
Une méthode adaptative



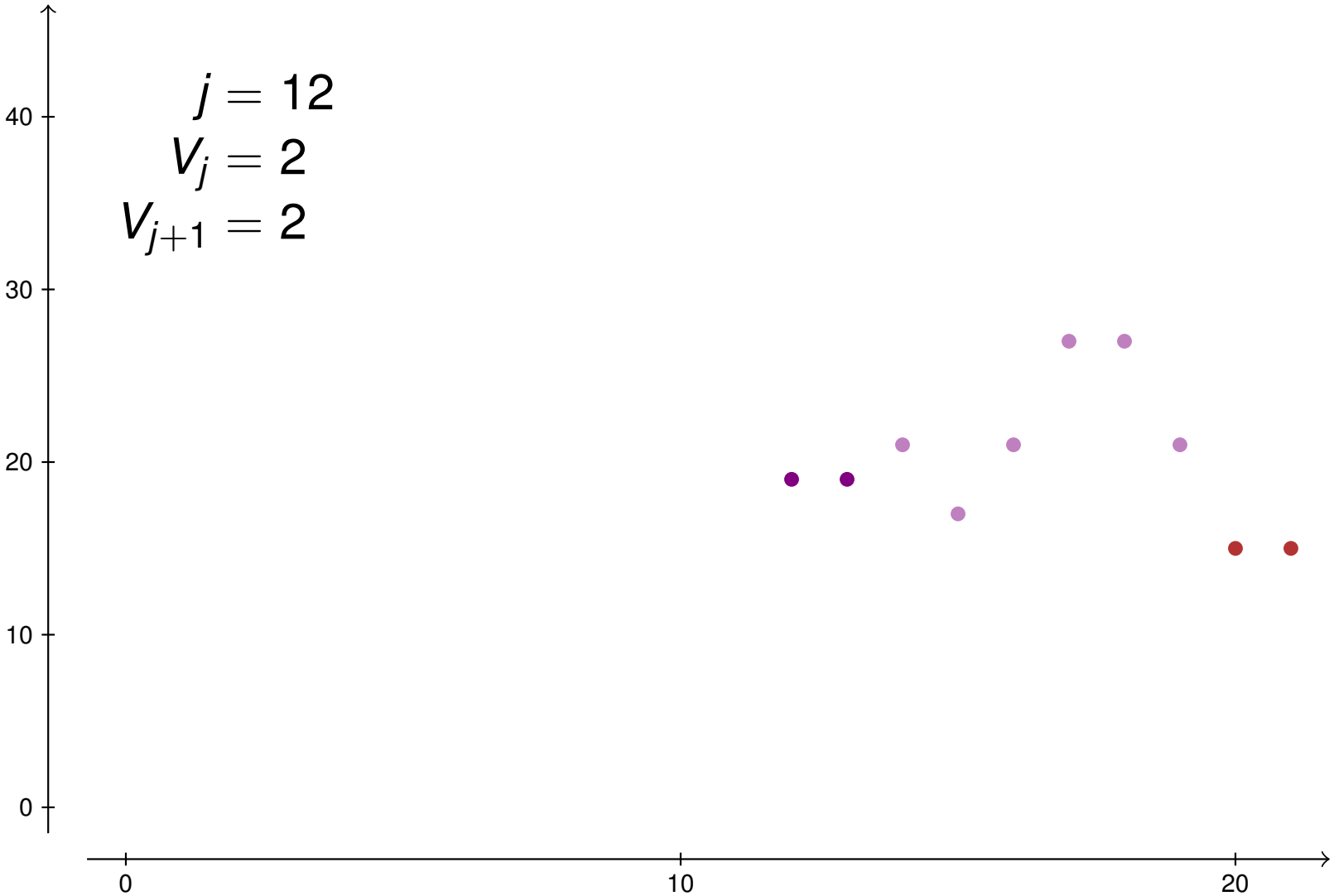
Une méthode adaptative



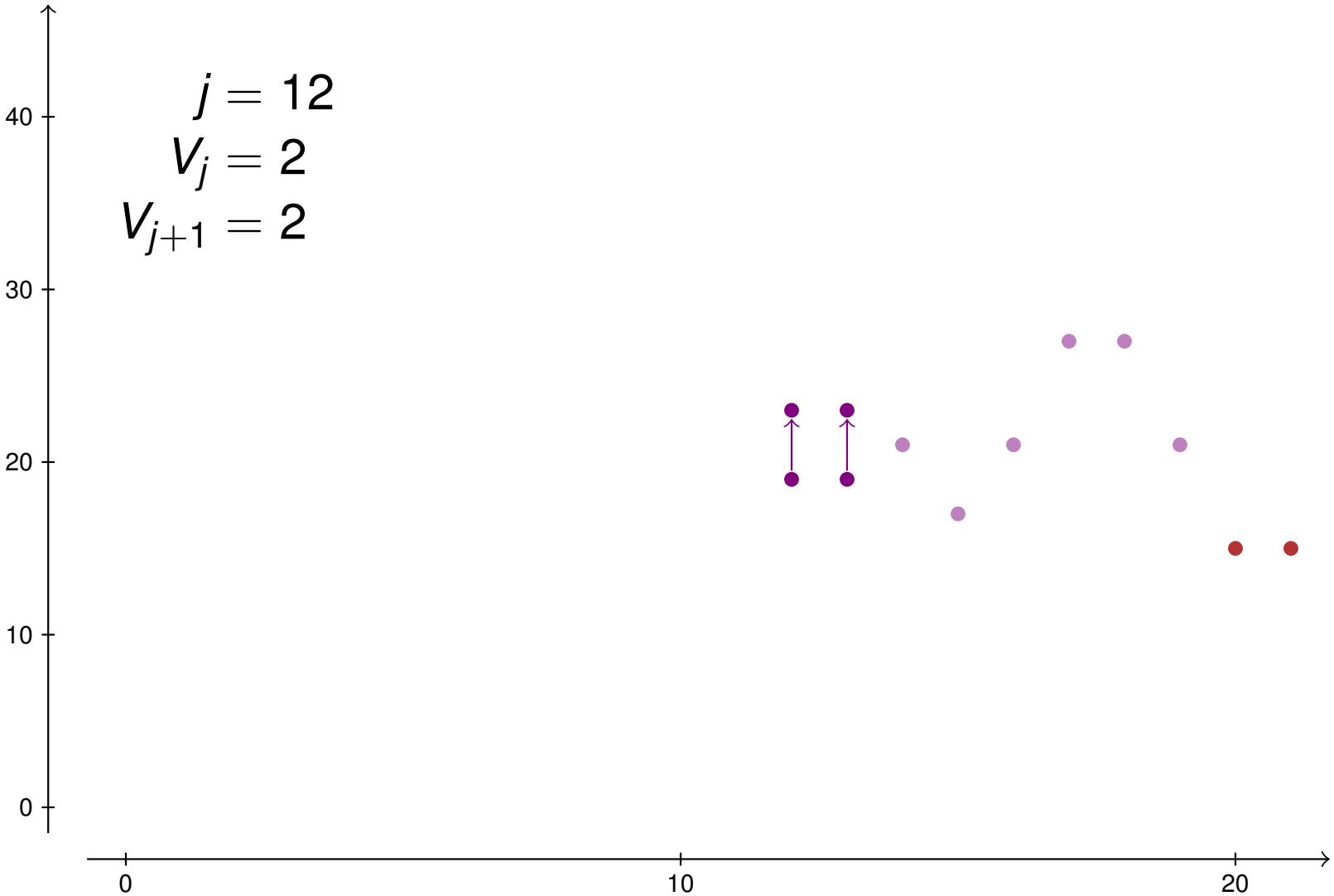
Une méthode adaptative



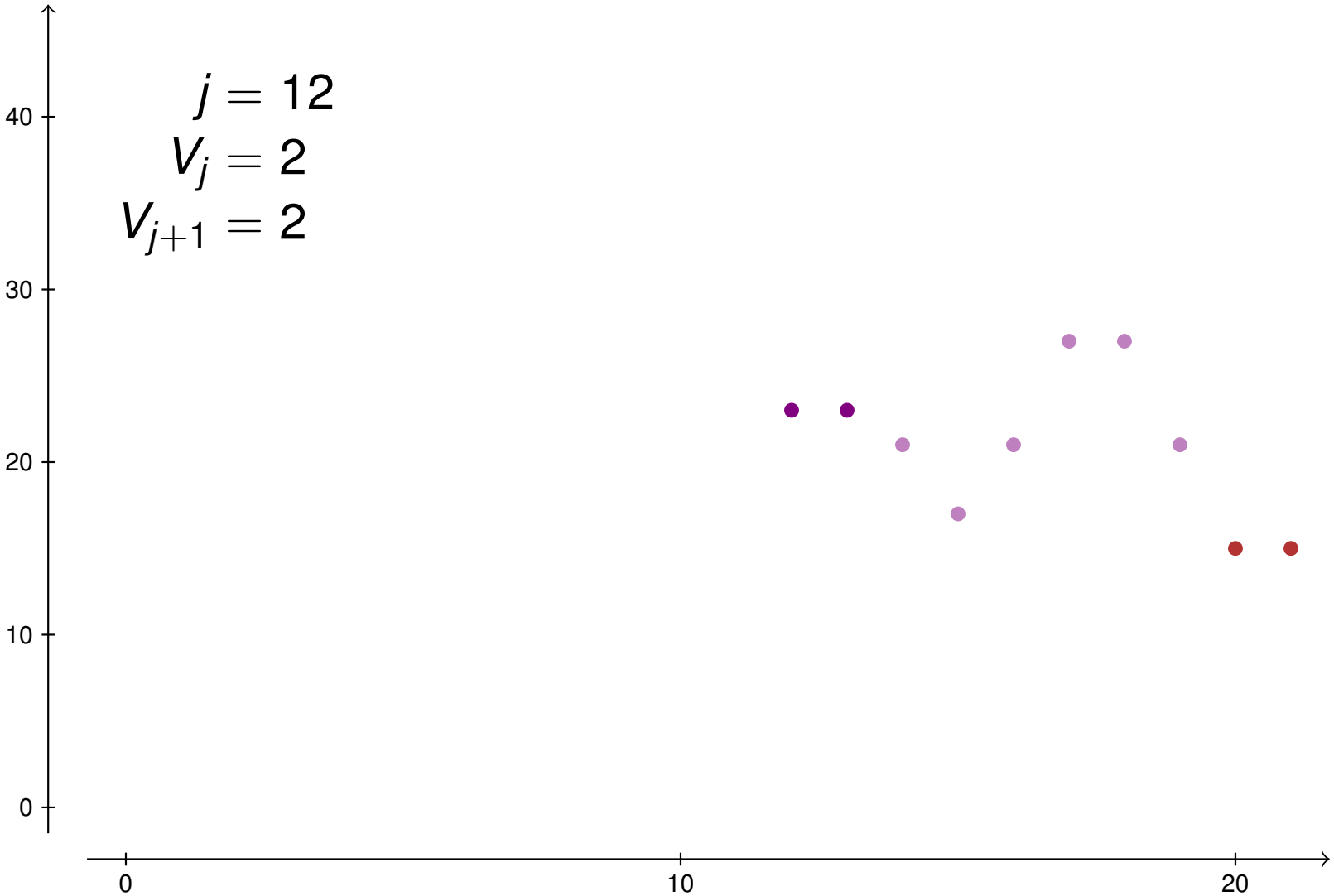
Une méthode adaptative



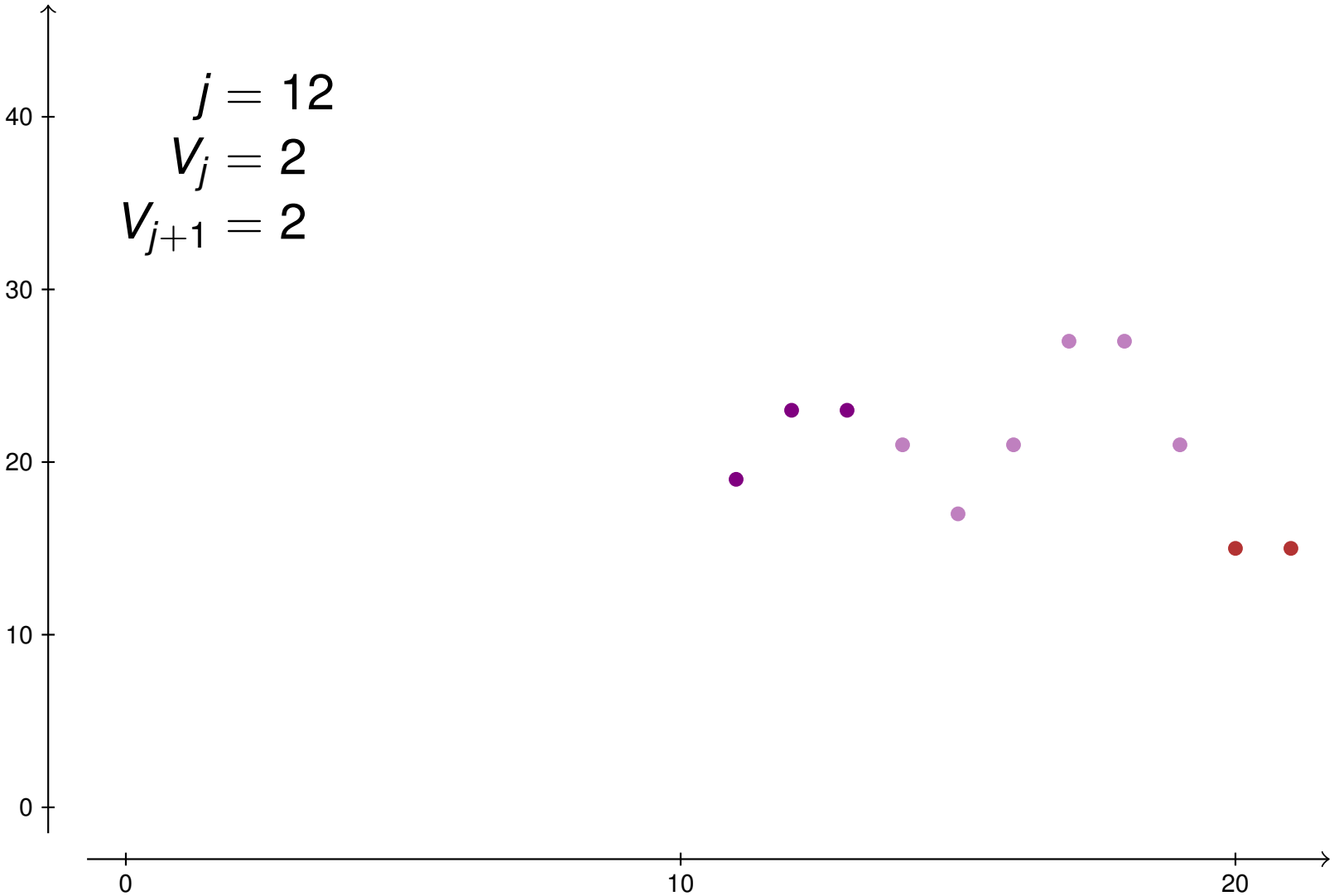
Une méthode adaptative



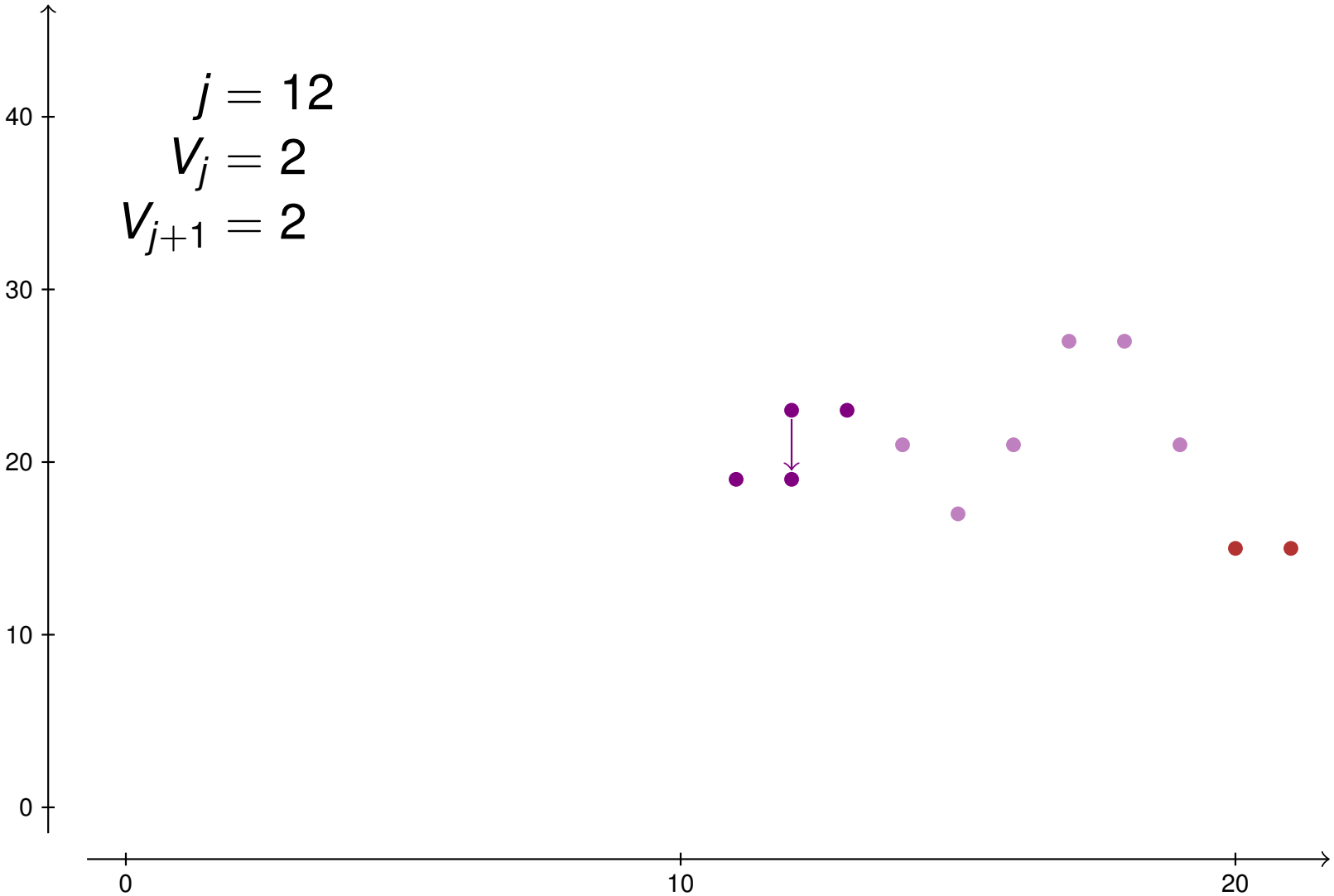
Une méthode adaptative



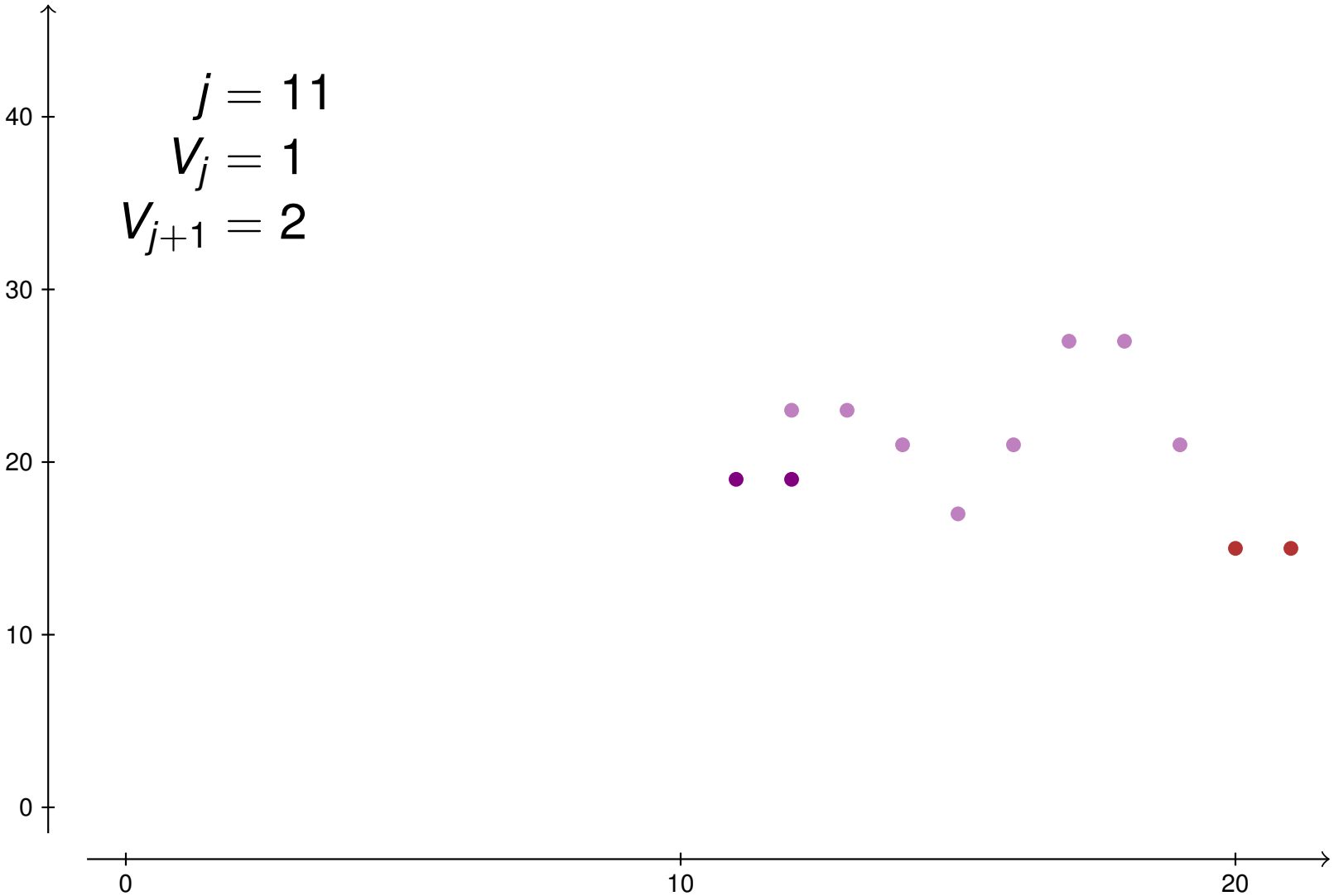
Une méthode adaptative



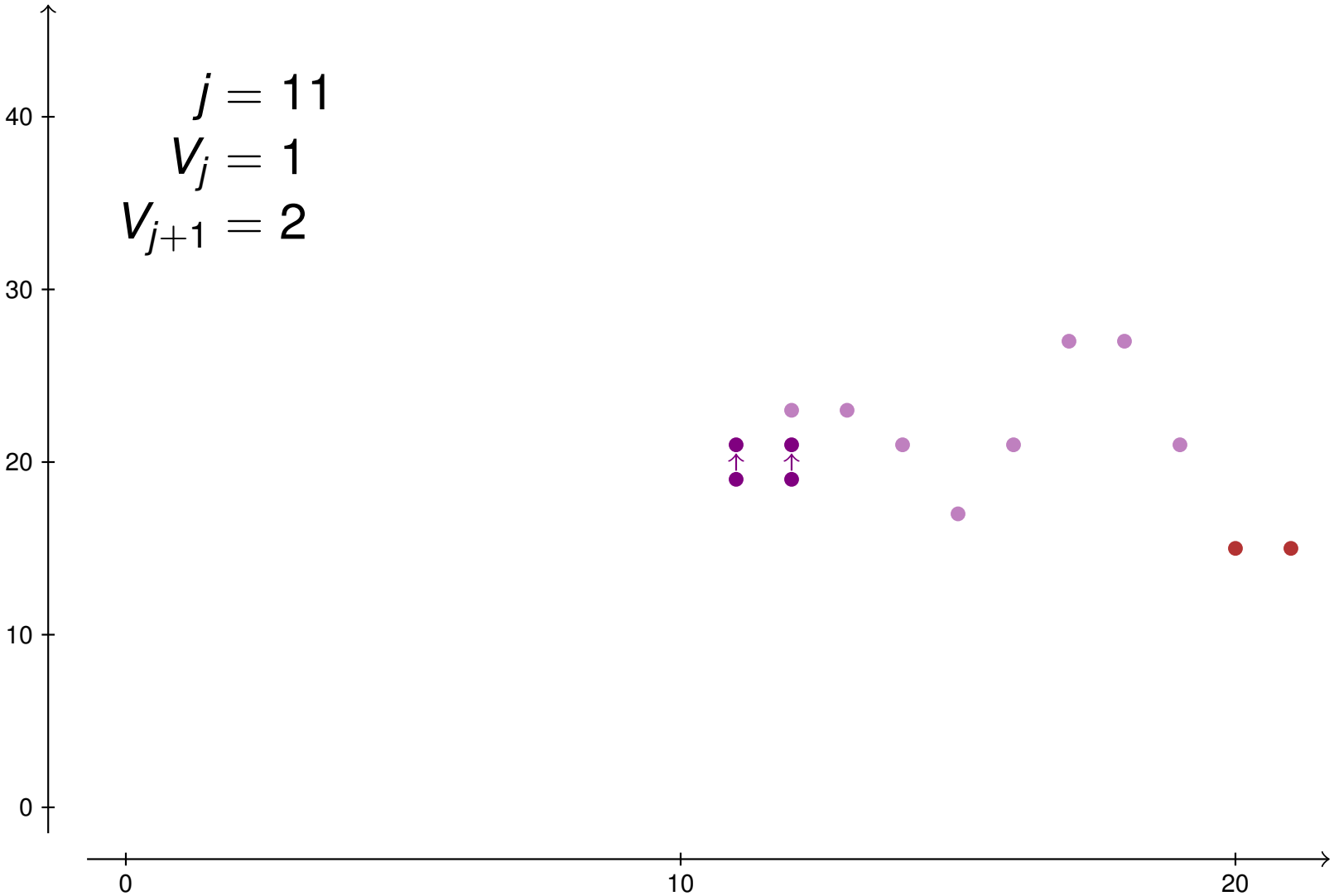
Une méthode adaptative



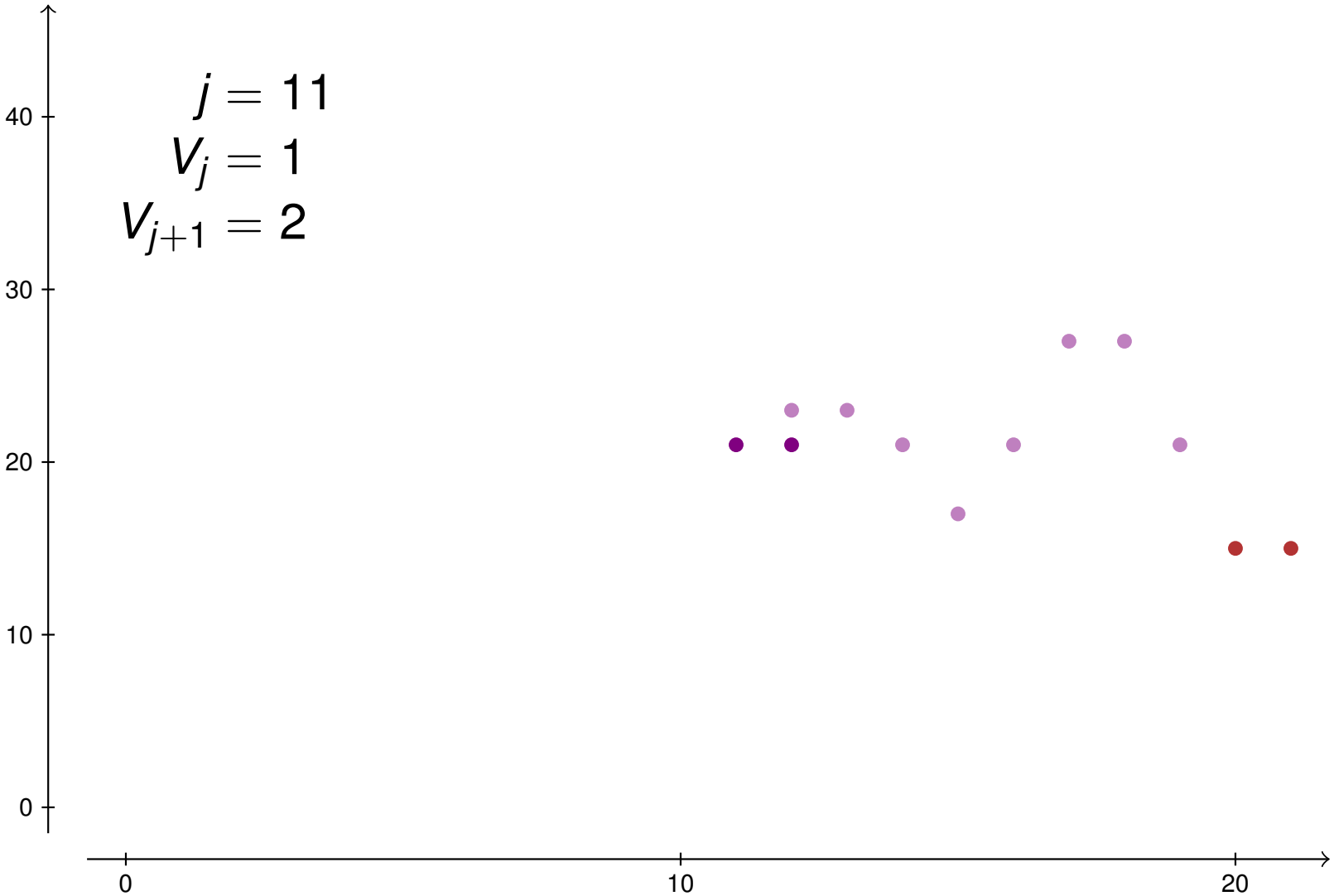
Une méthode adaptative



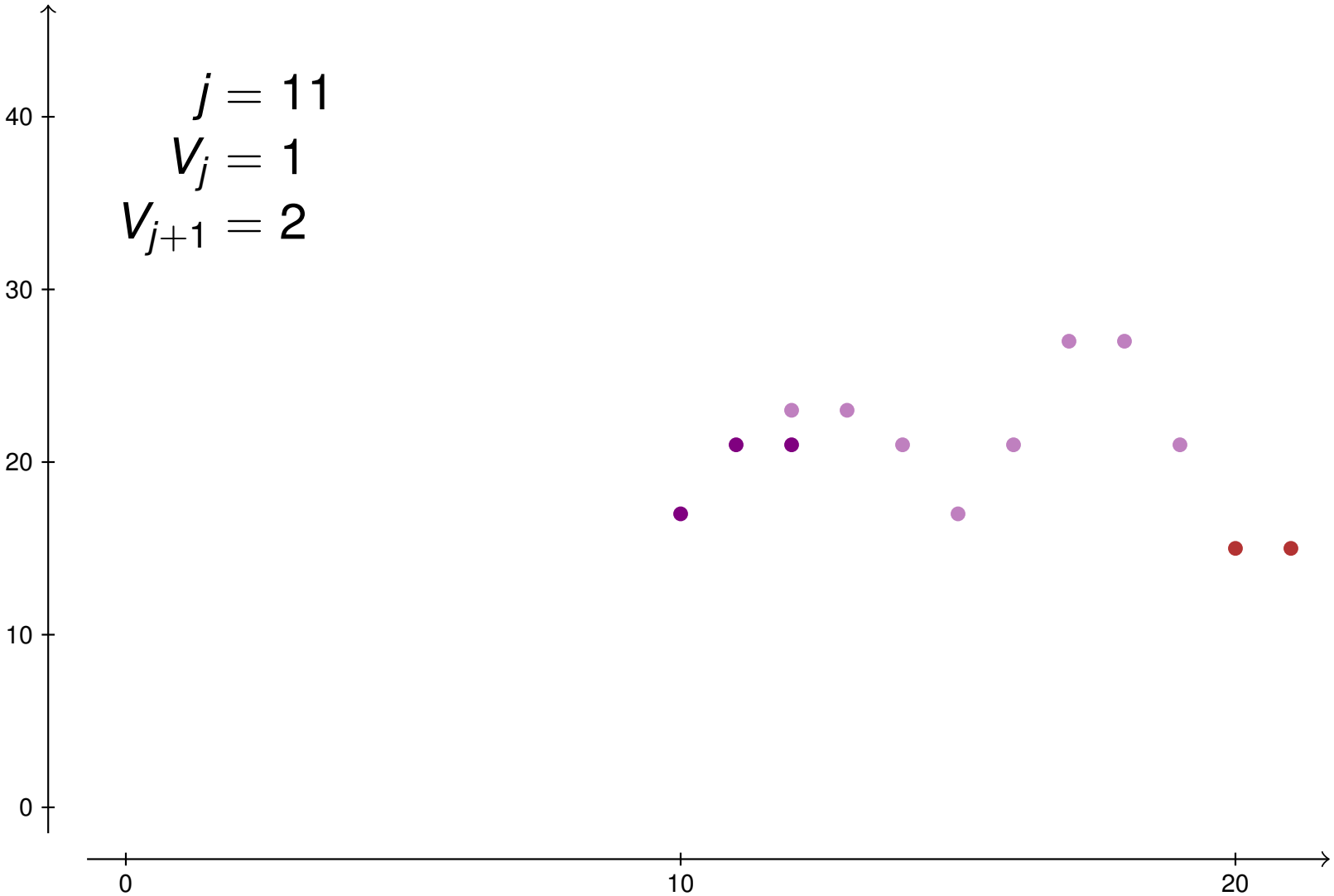
Une méthode adaptative



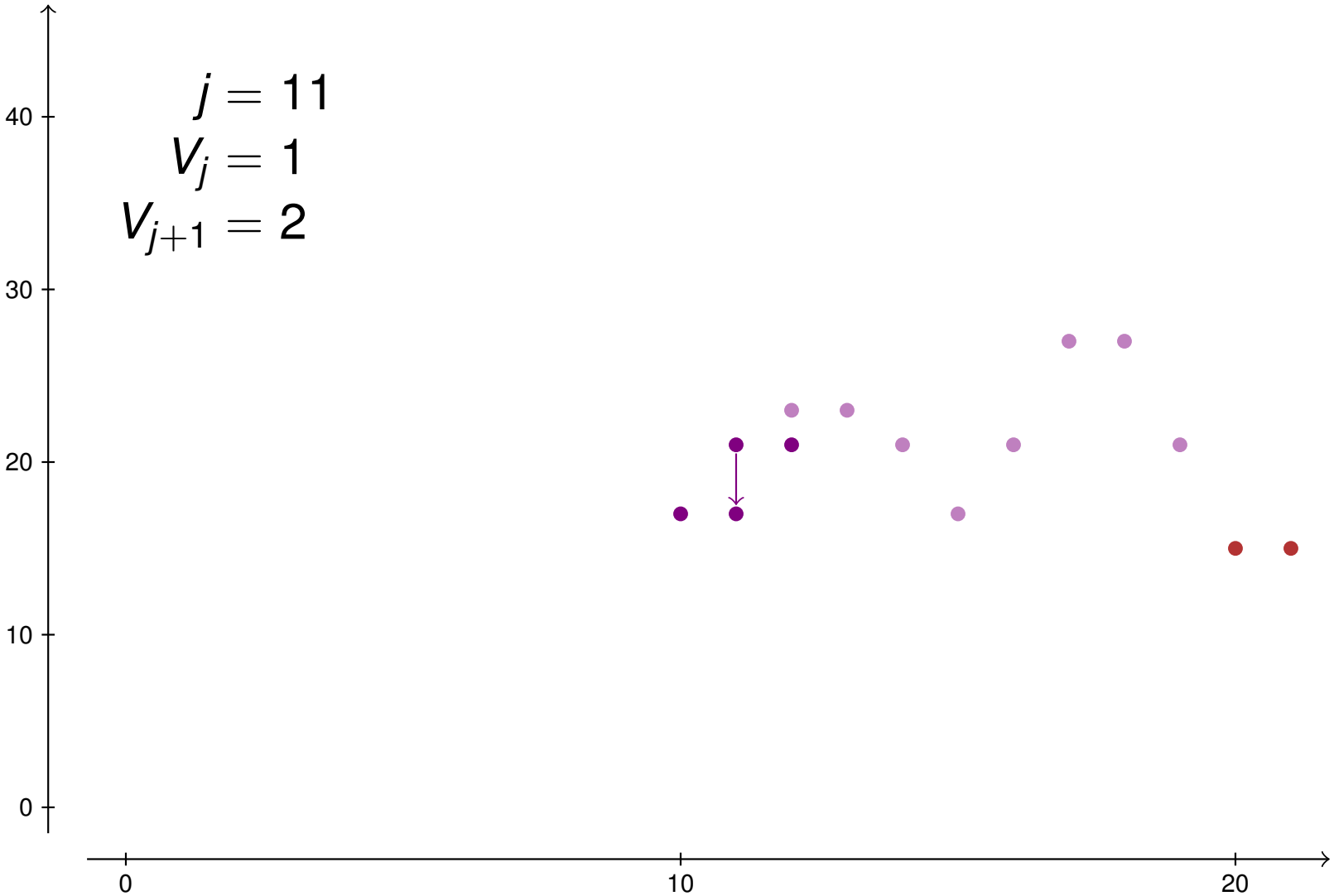
Une méthode adaptative



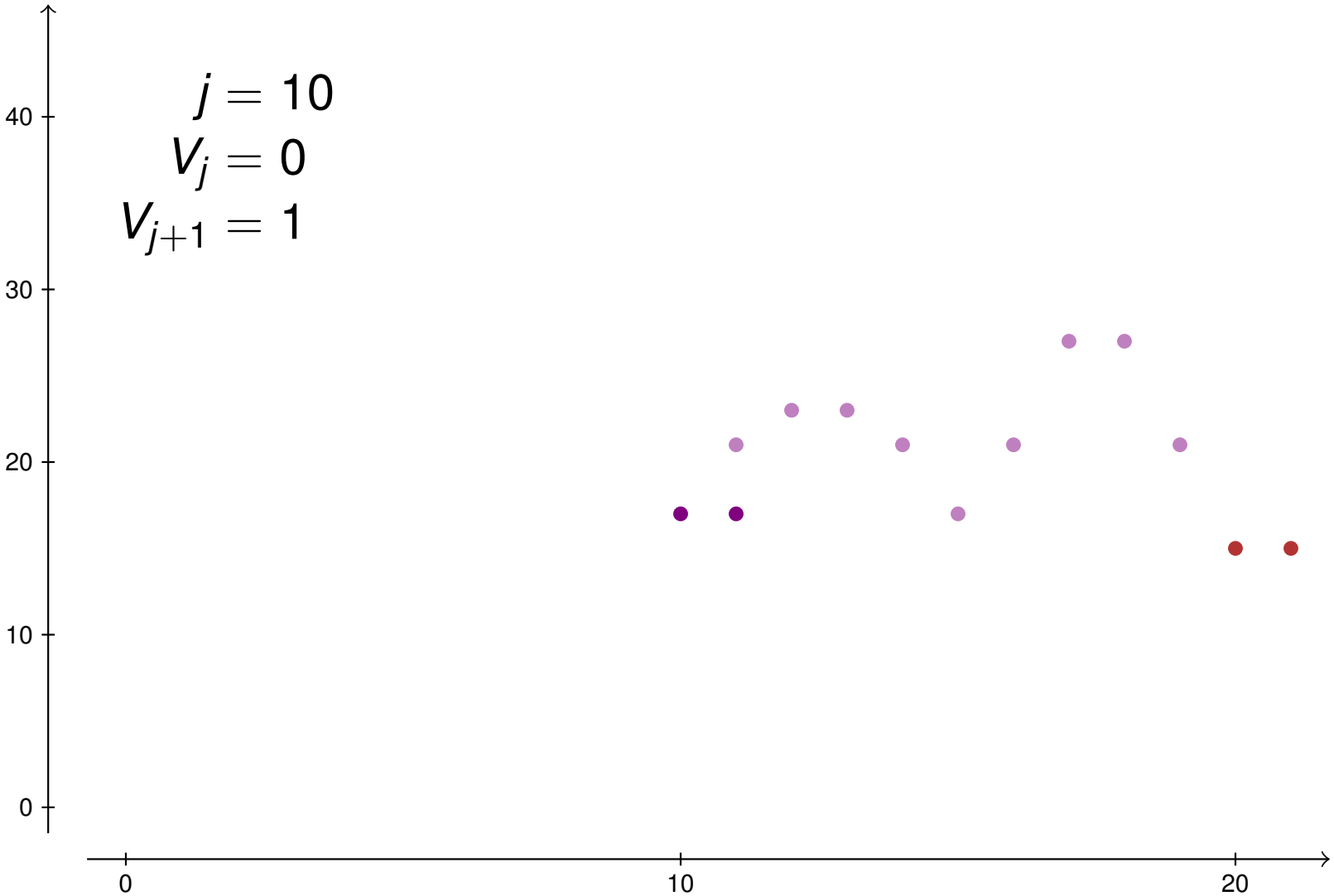
Une méthode adaptative



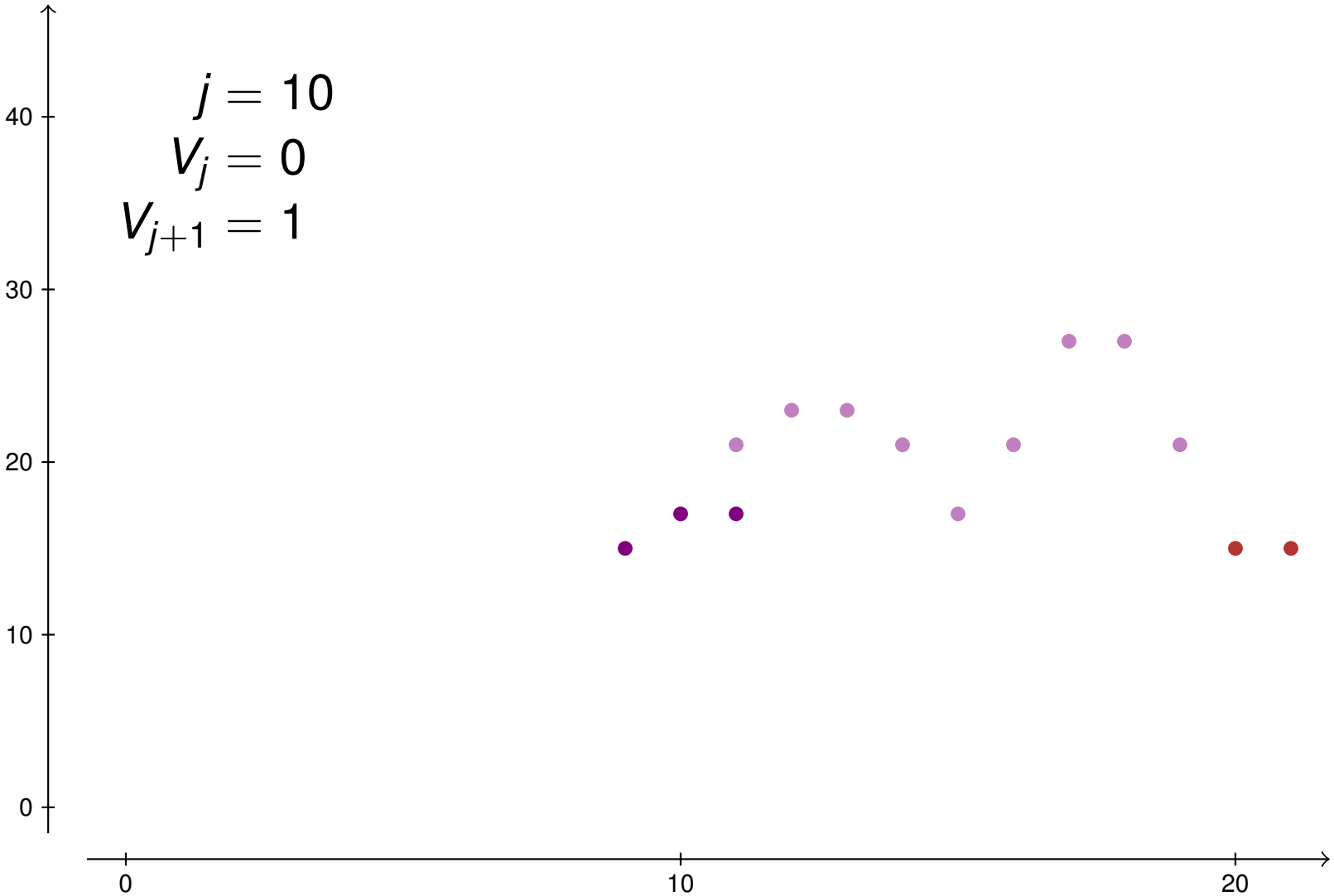
Une méthode adaptative



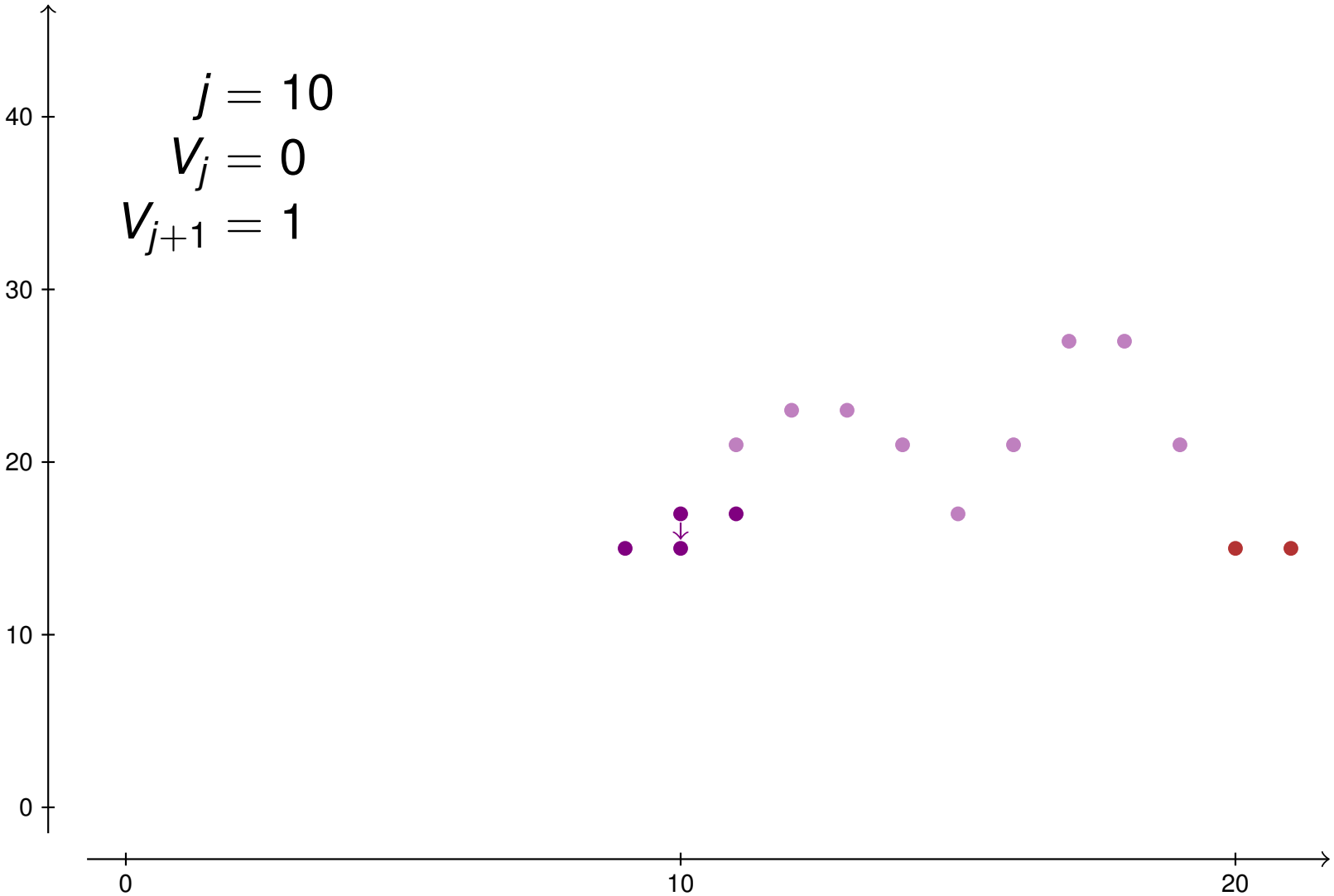
Une méthode adaptative



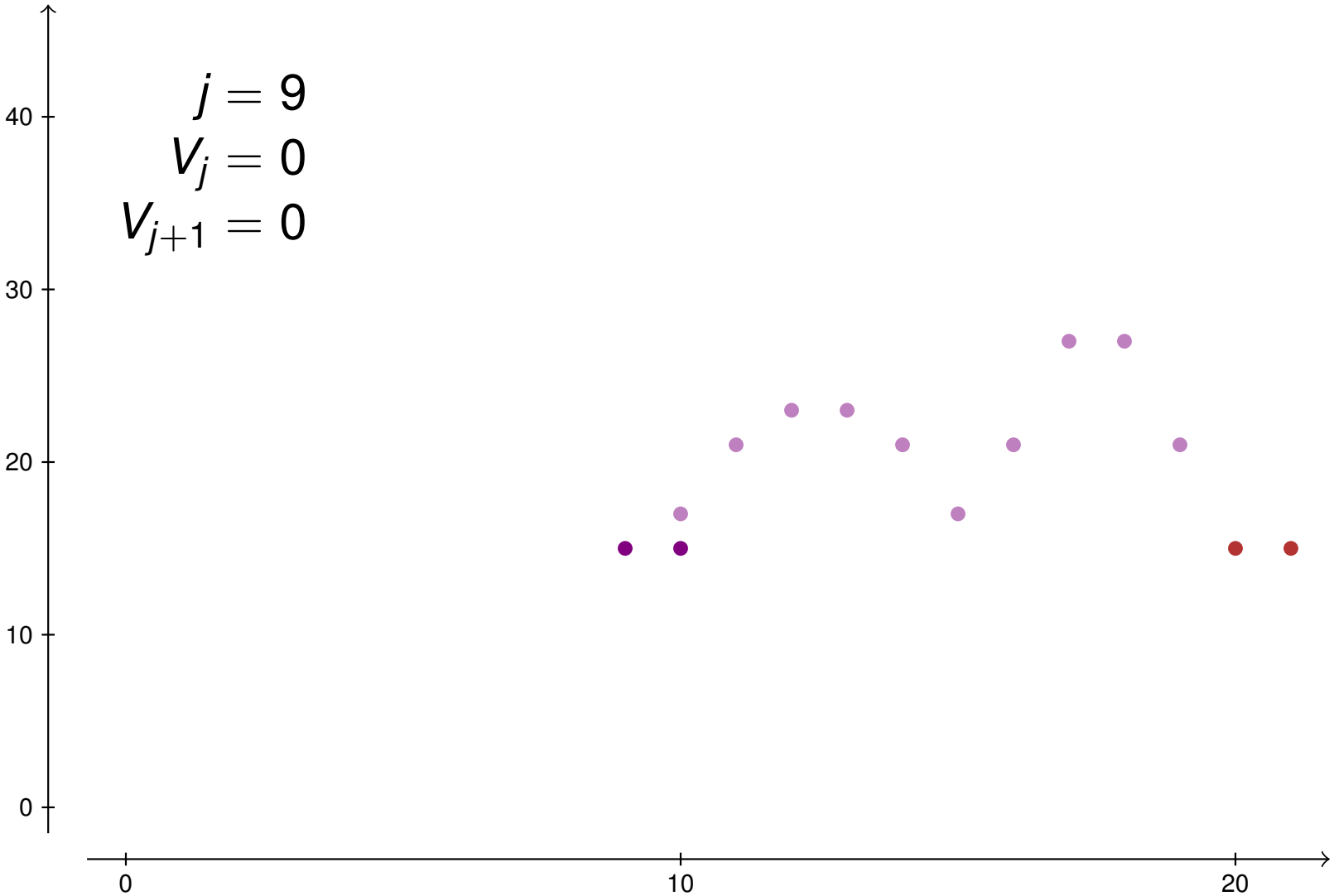
Une méthode adaptative



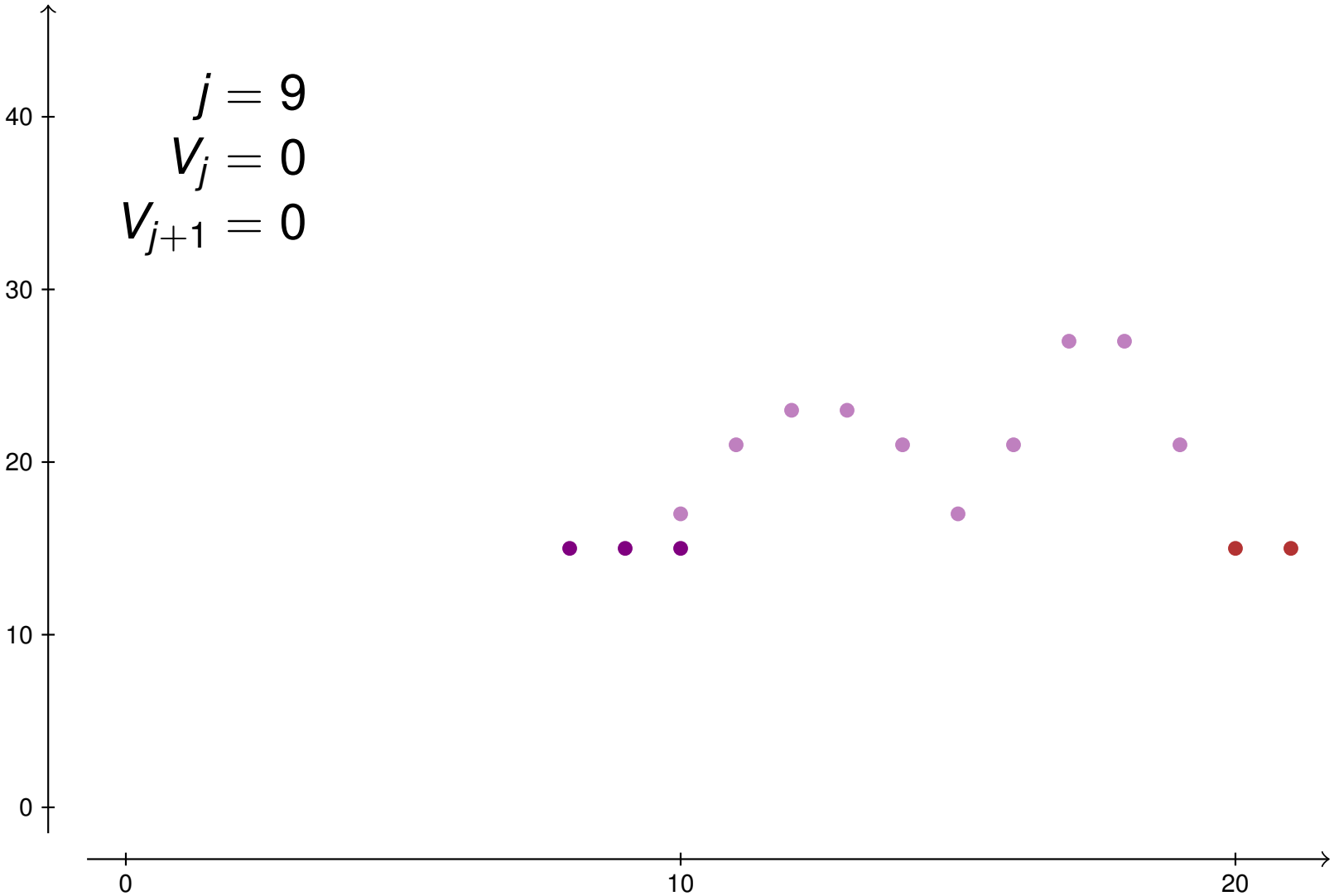
Une méthode adaptative



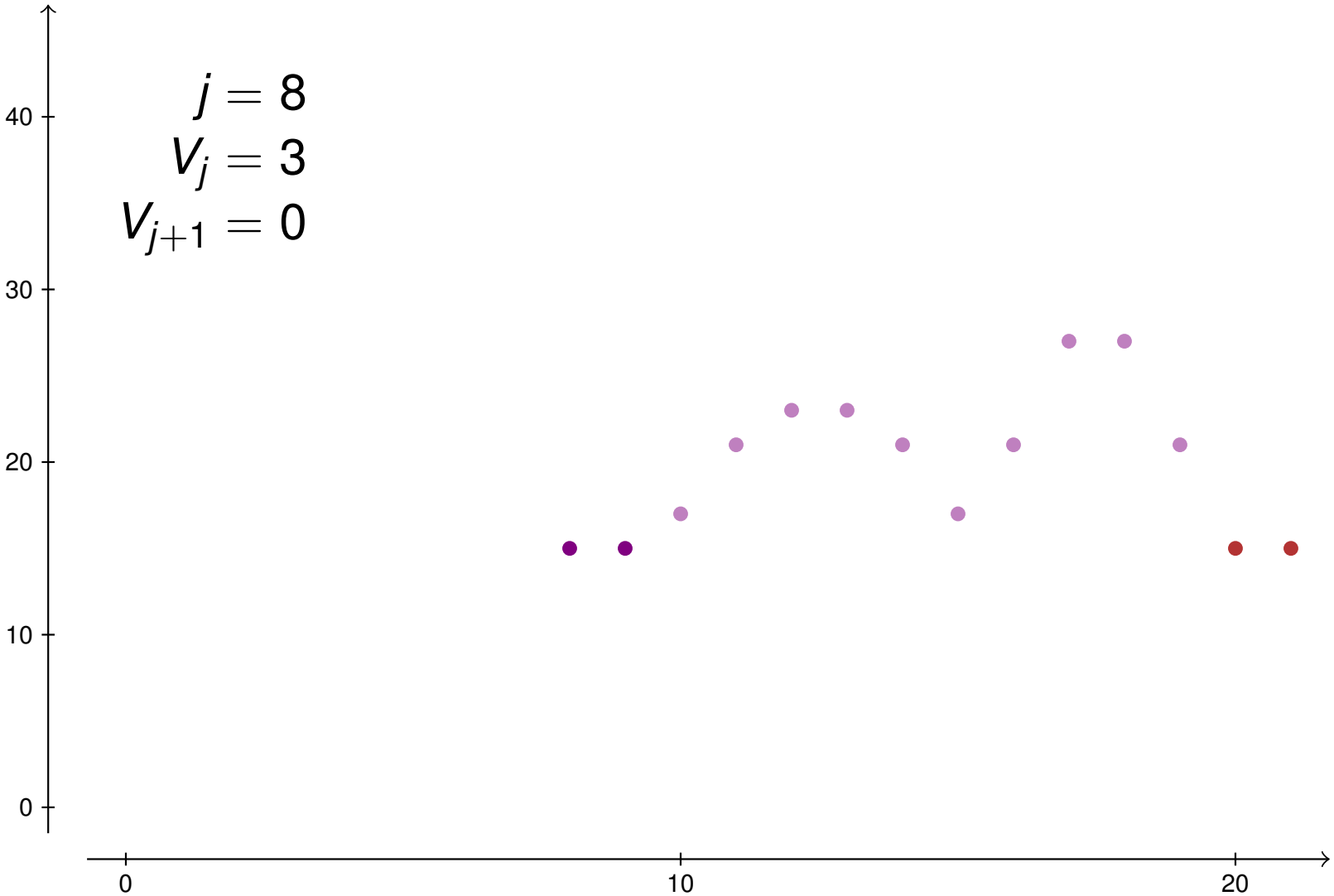
Une méthode adaptative



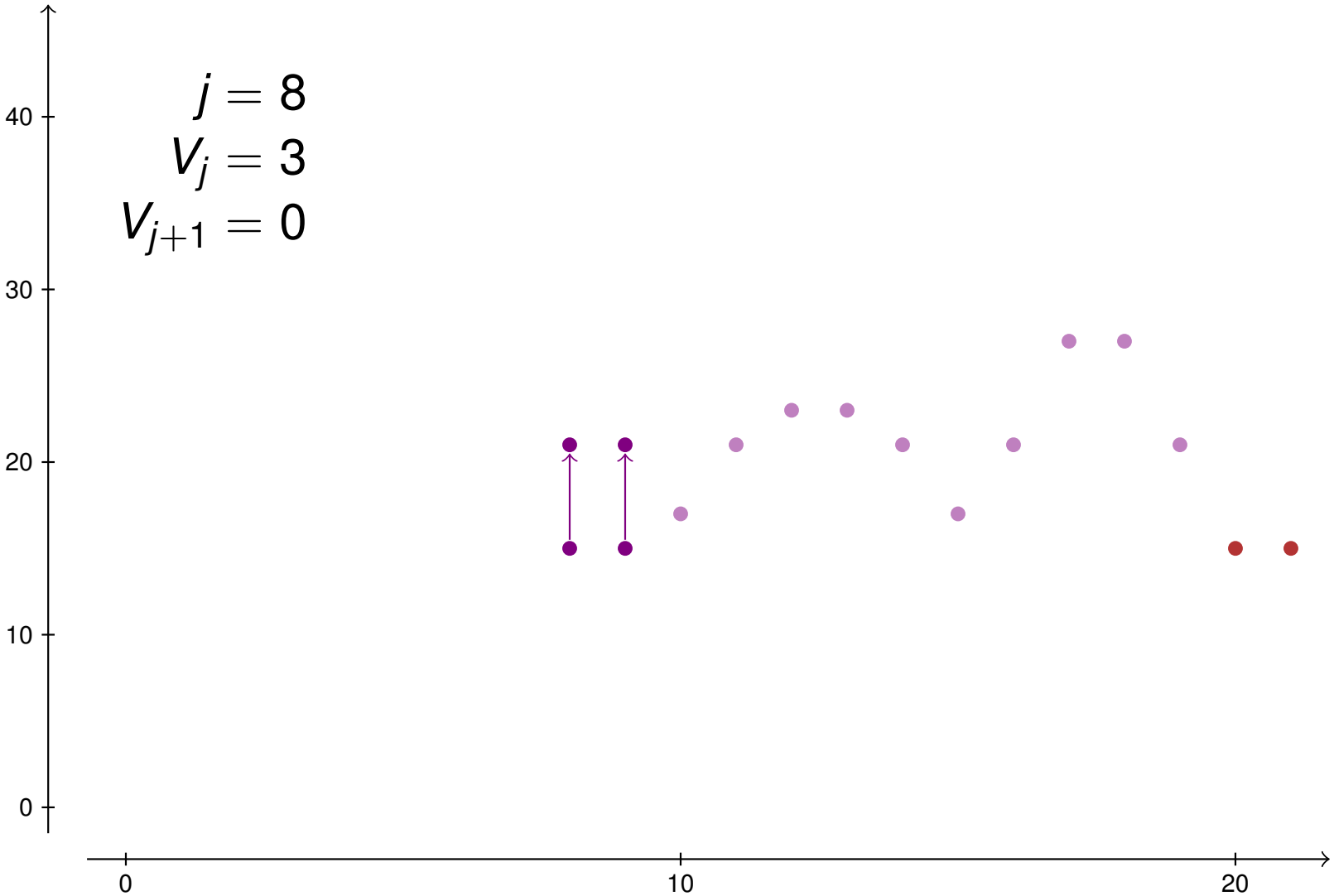
Une méthode adaptative



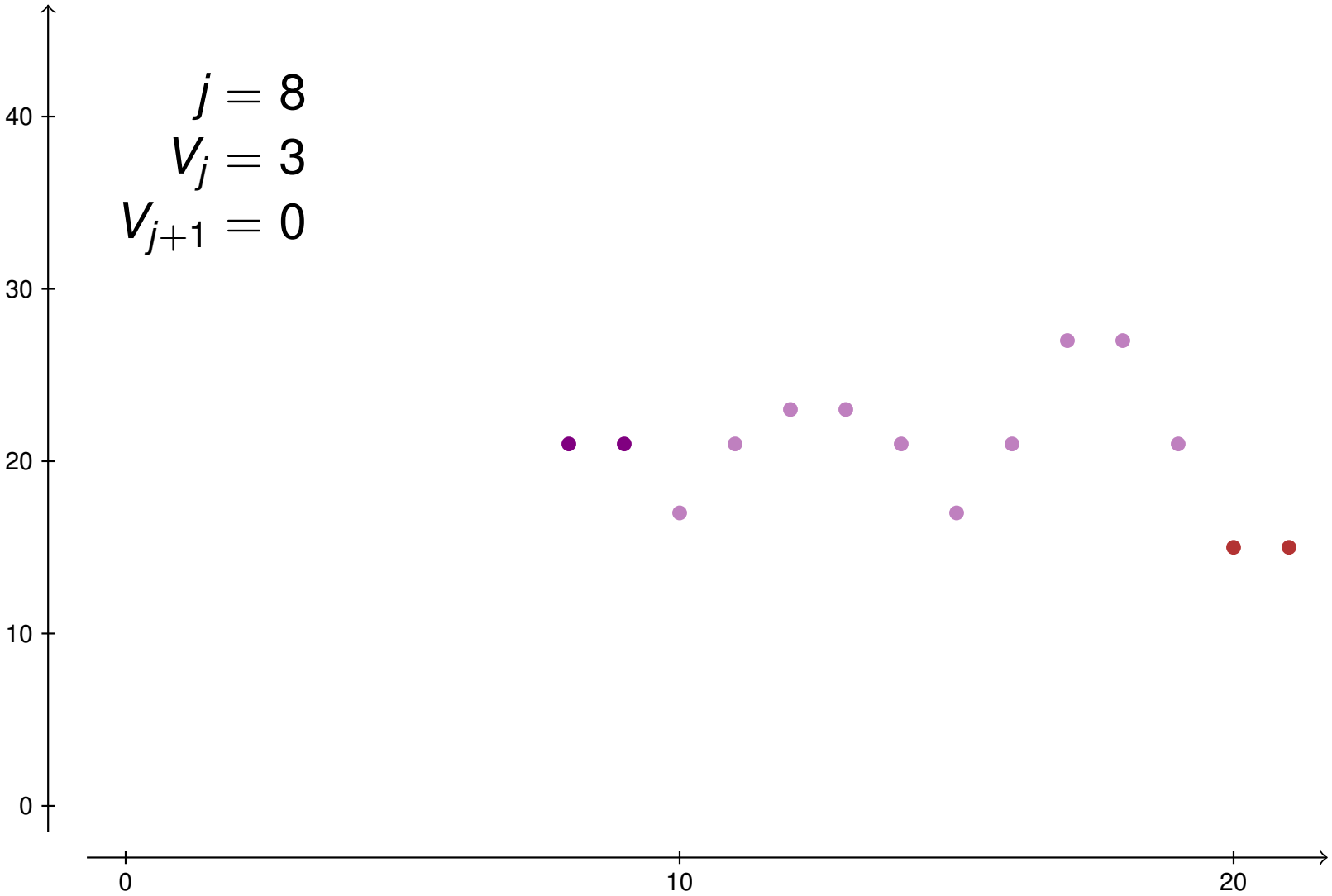
Une méthode adaptative



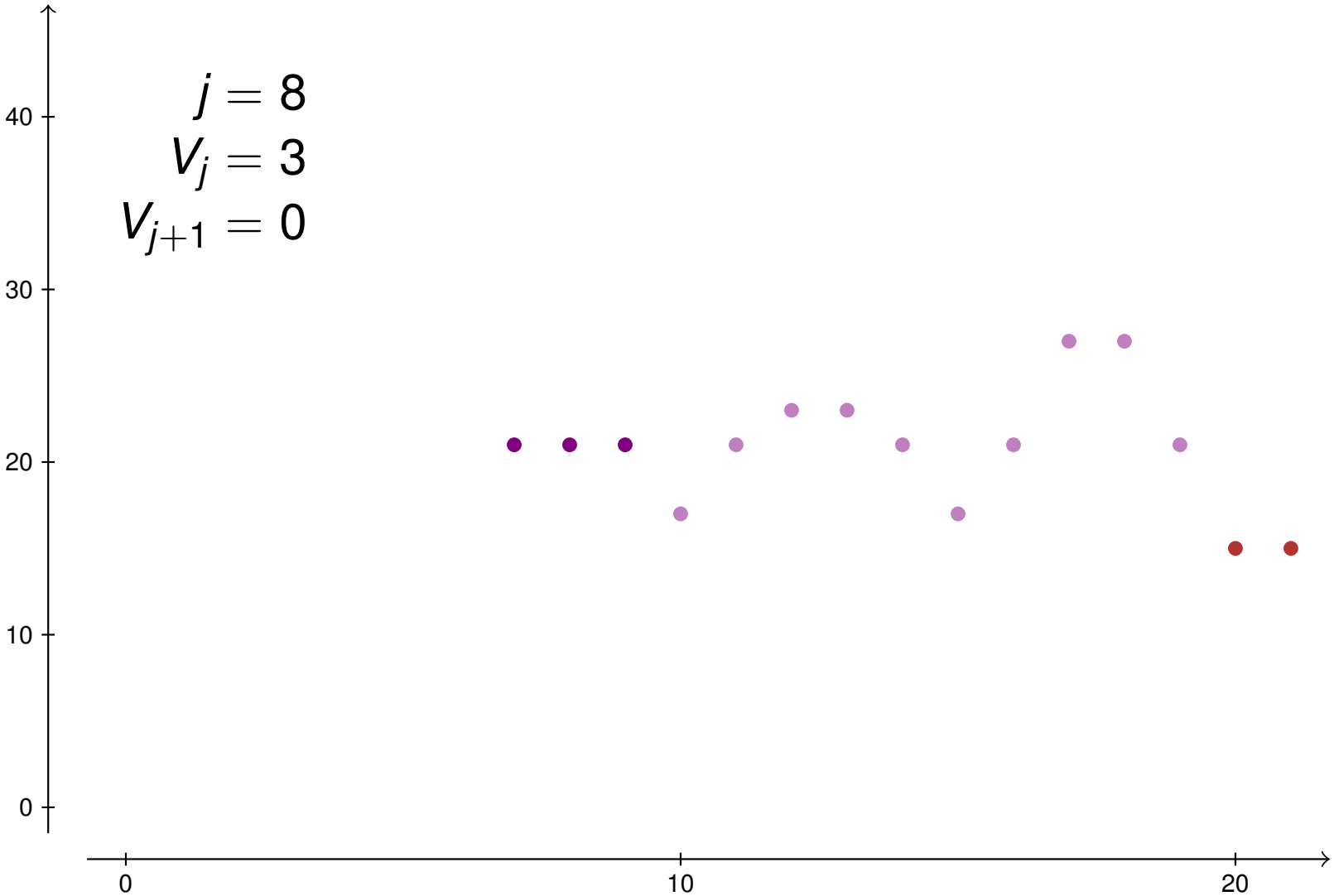
Une méthode adaptative



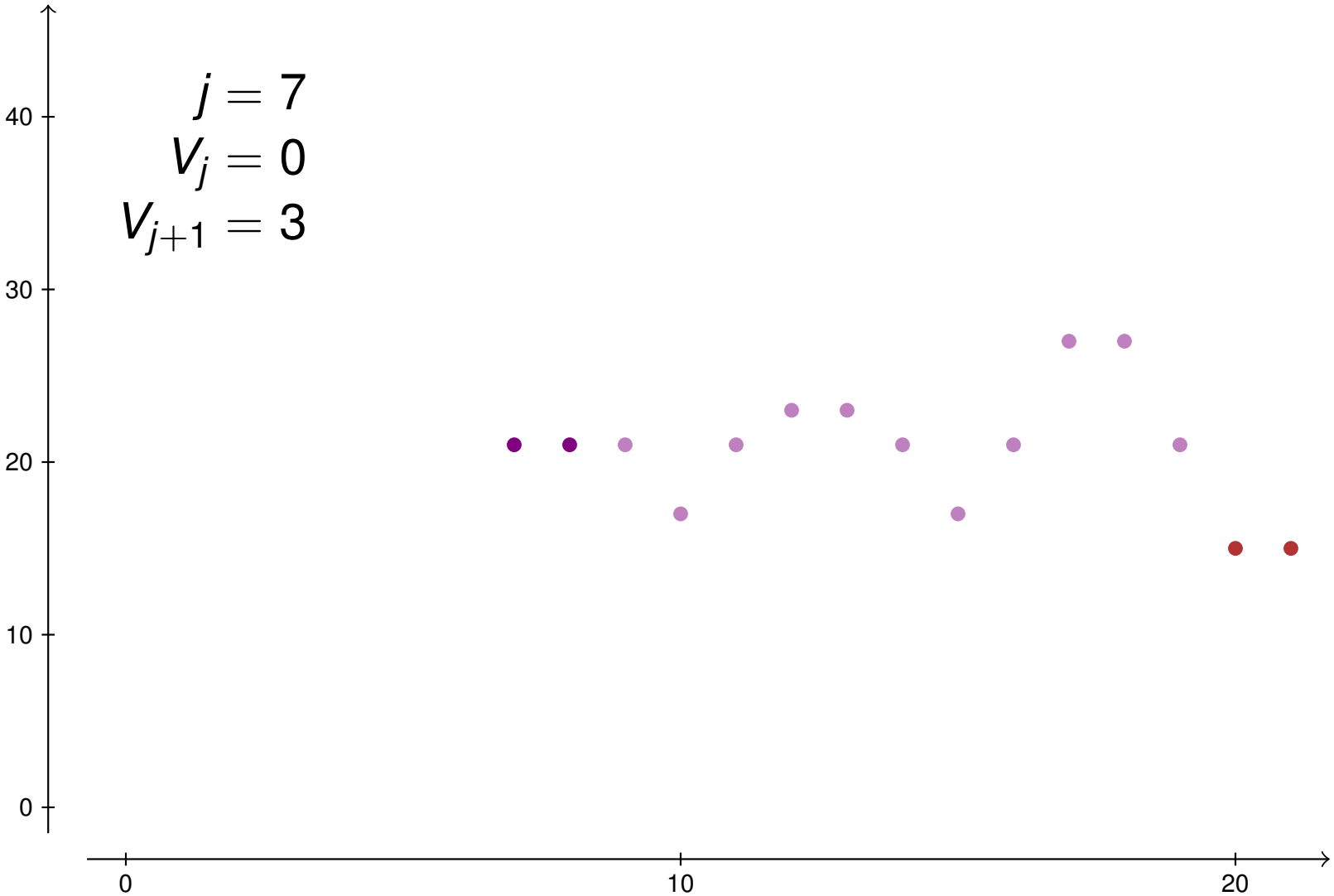
Une méthode adaptative



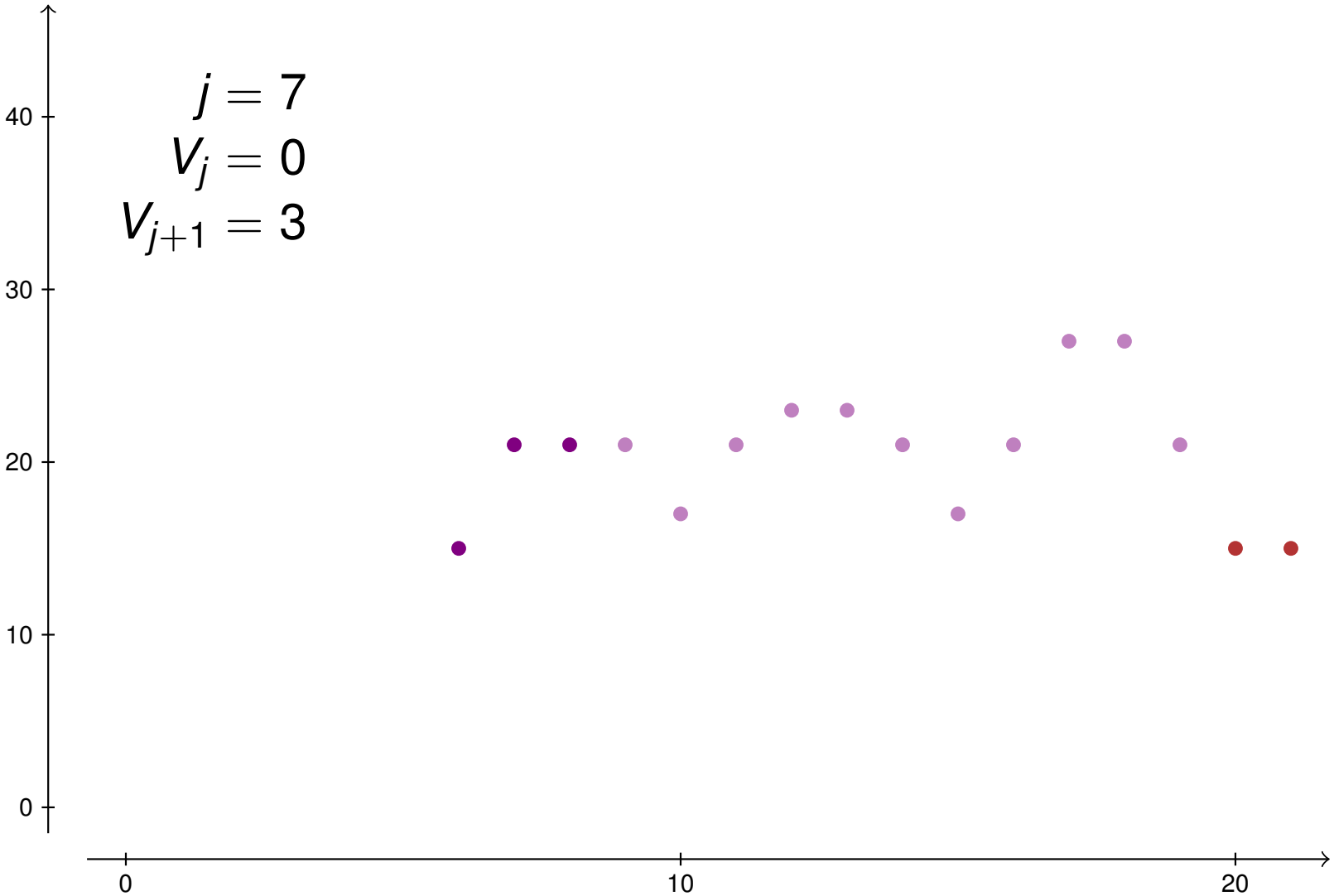
Une méthode adaptative



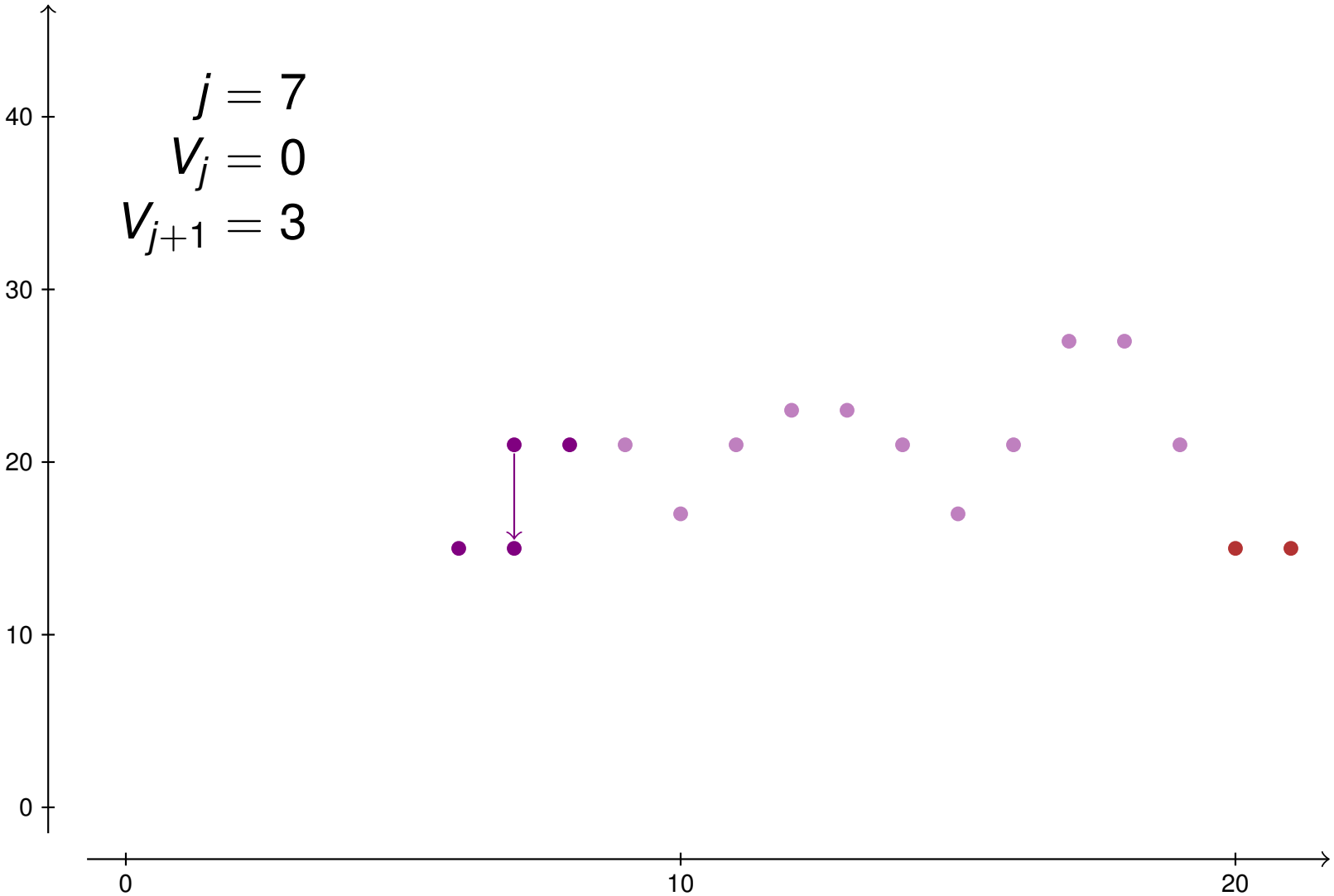
Une méthode adaptative



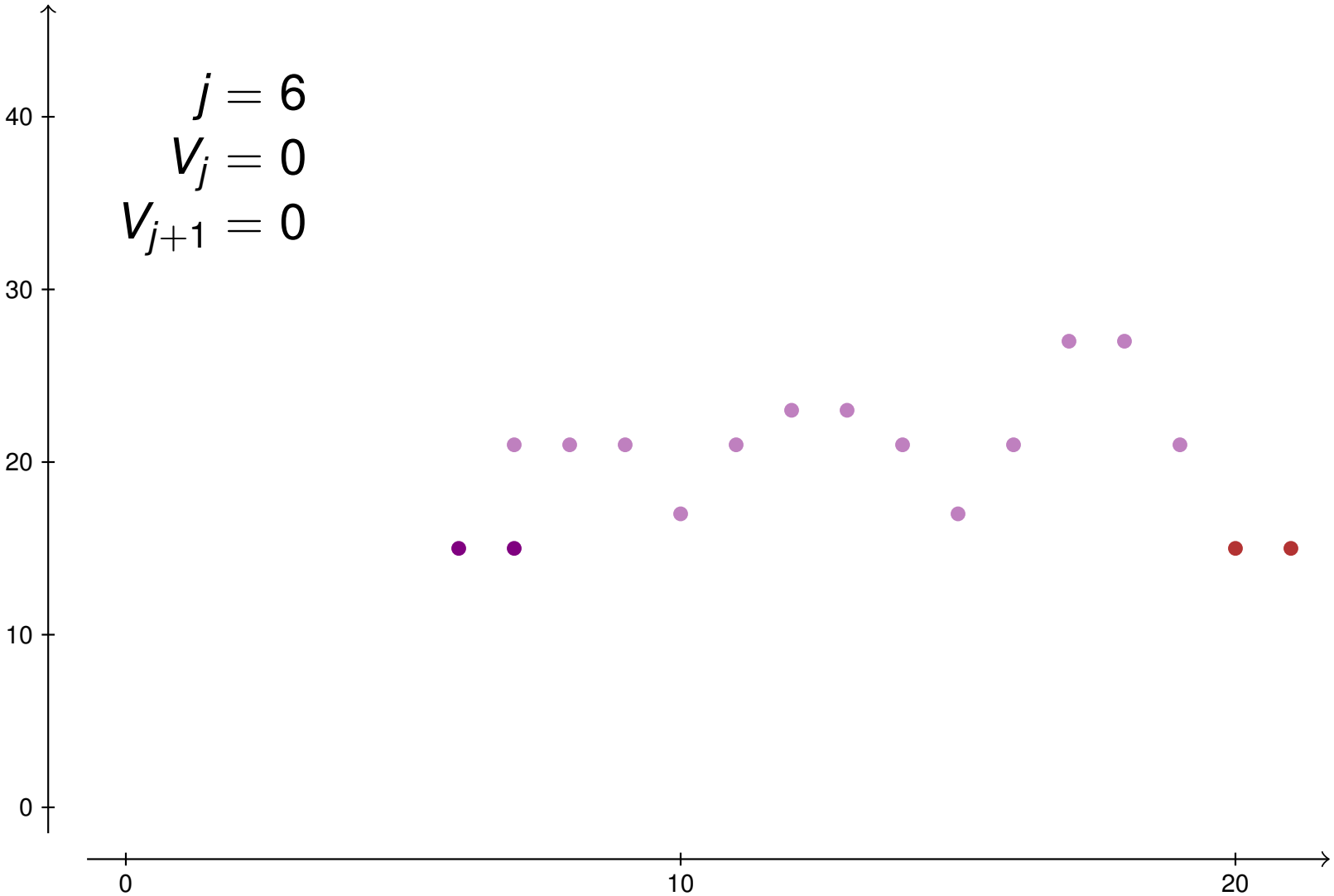
Une méthode adaptative



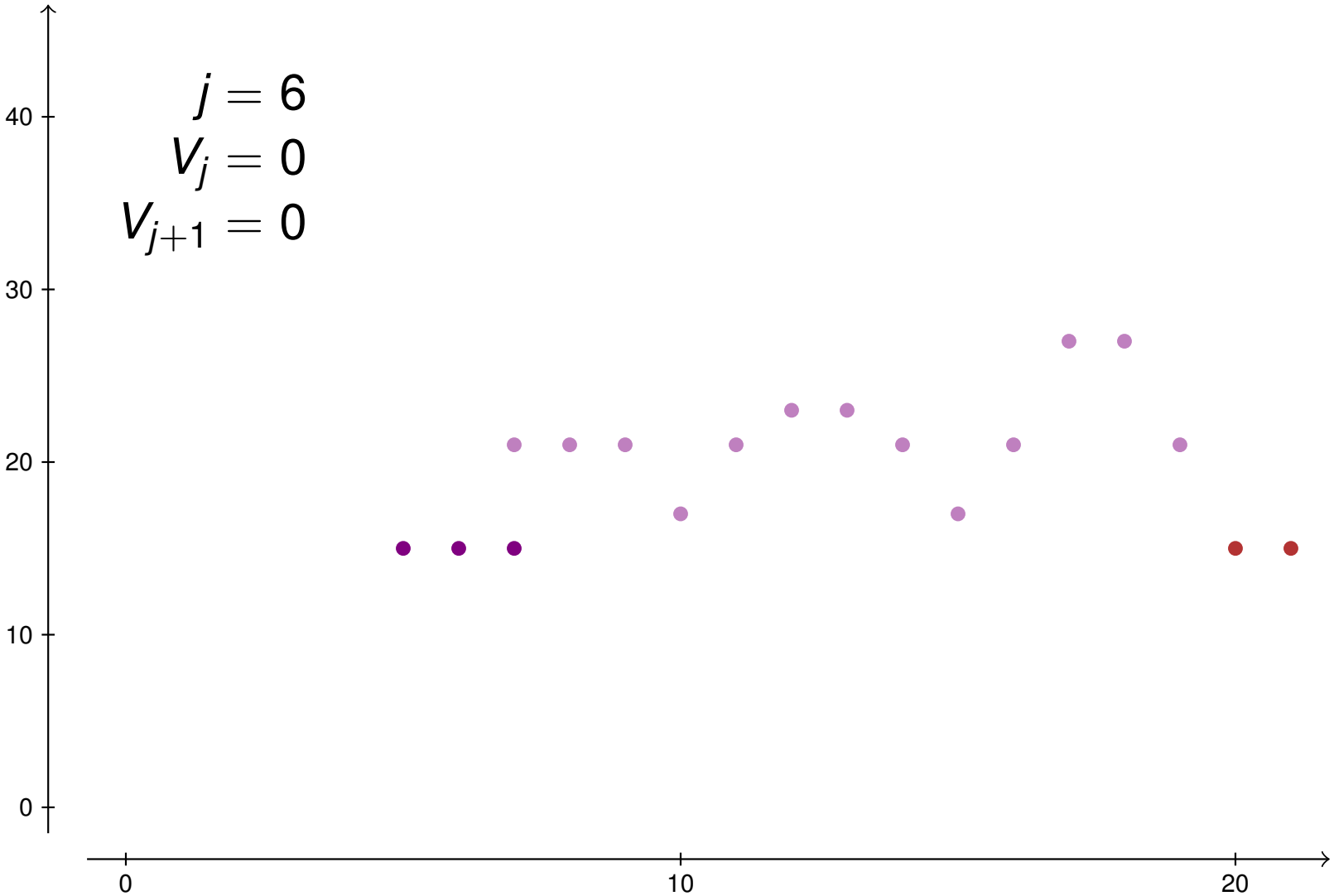
Une méthode adaptative



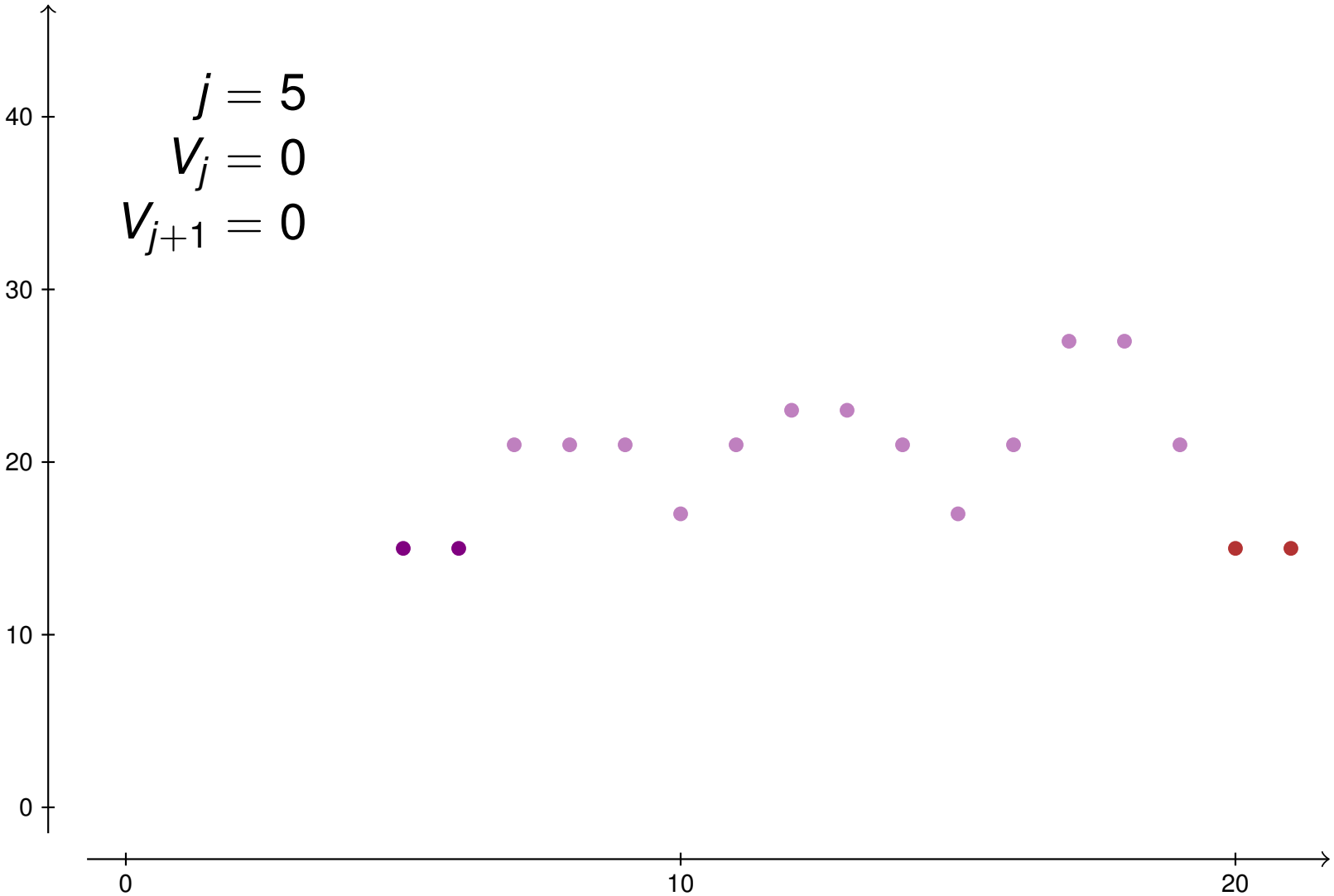
Une méthode adaptative



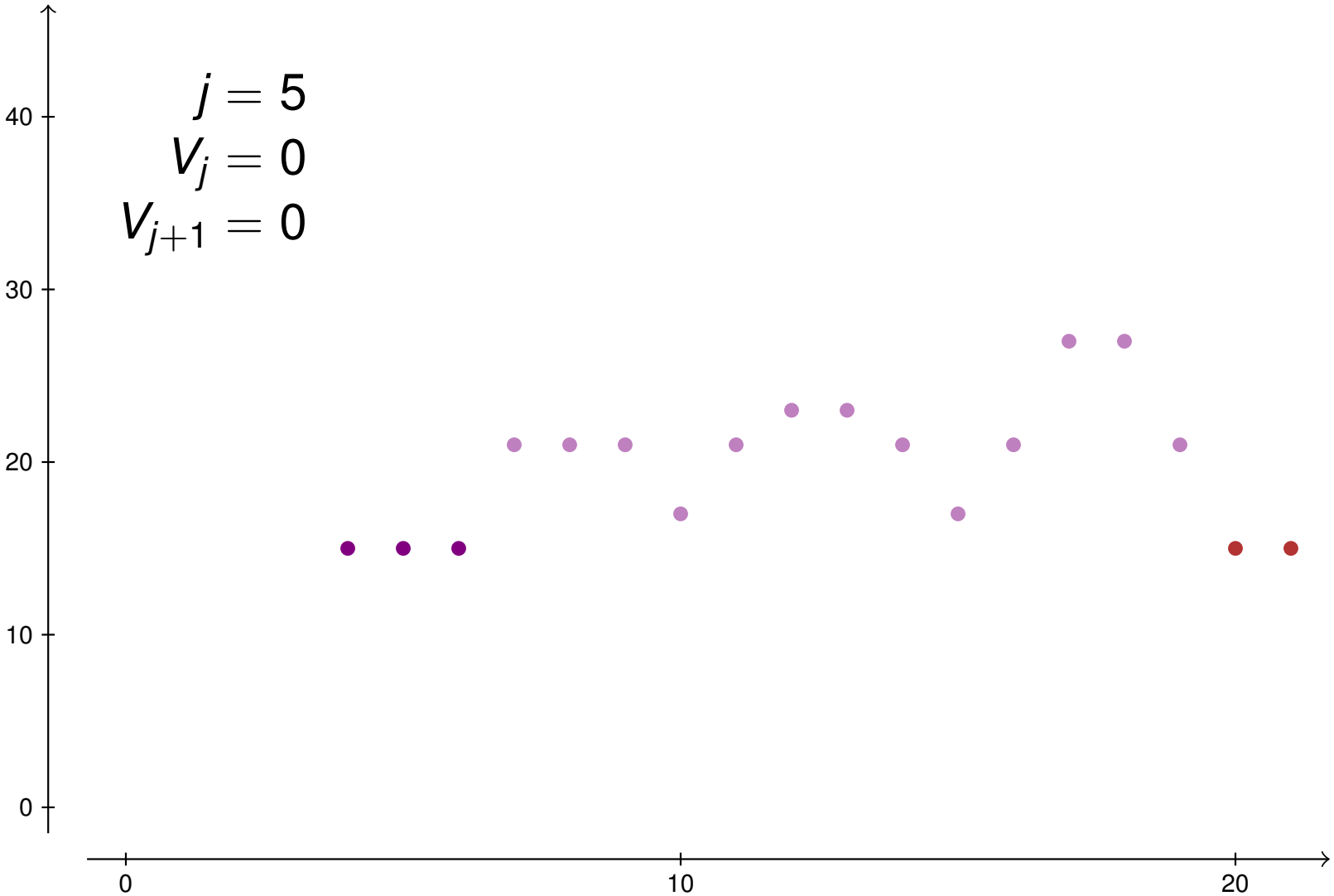
Une méthode adaptative



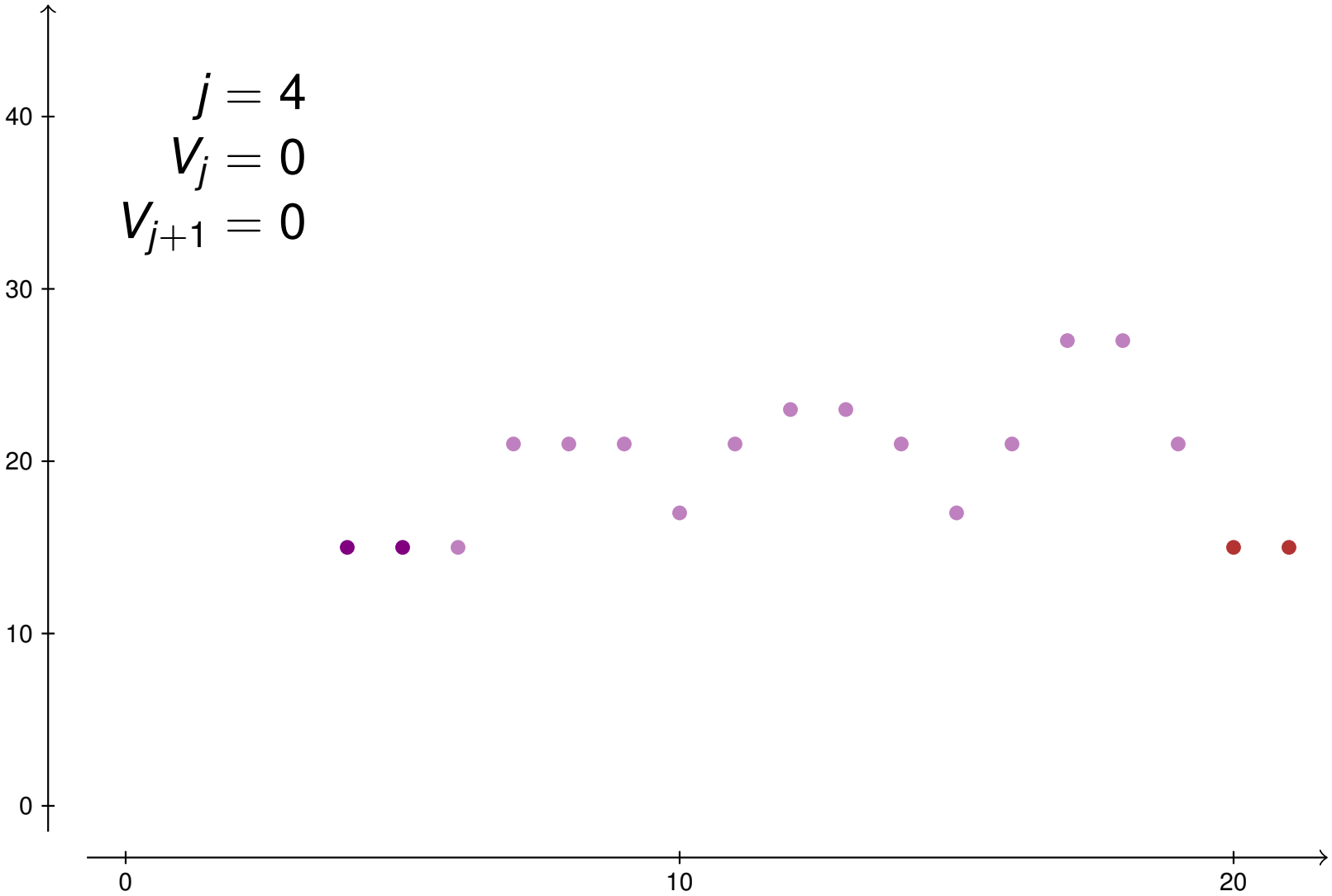
Une méthode adaptative



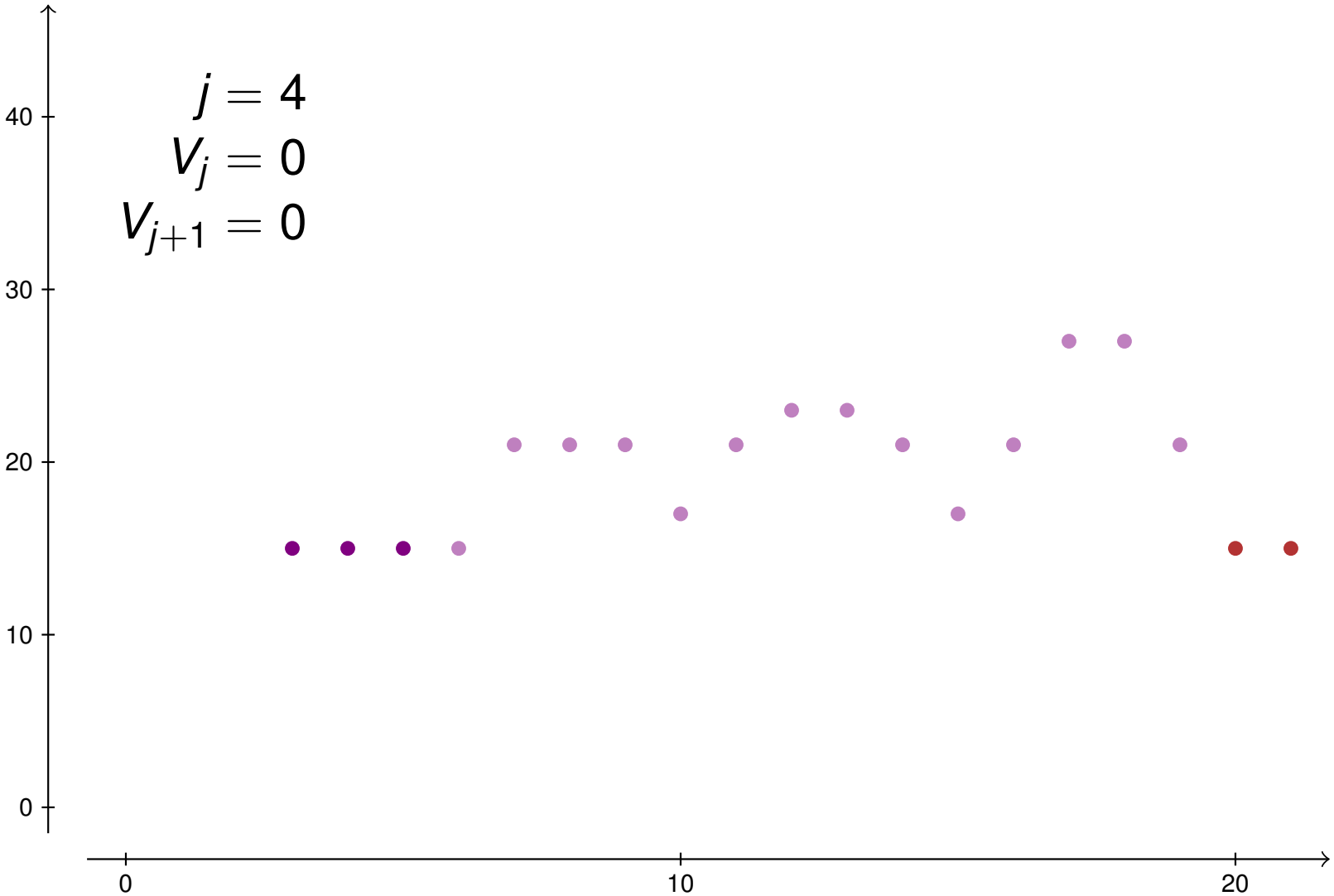
Une méthode adaptative



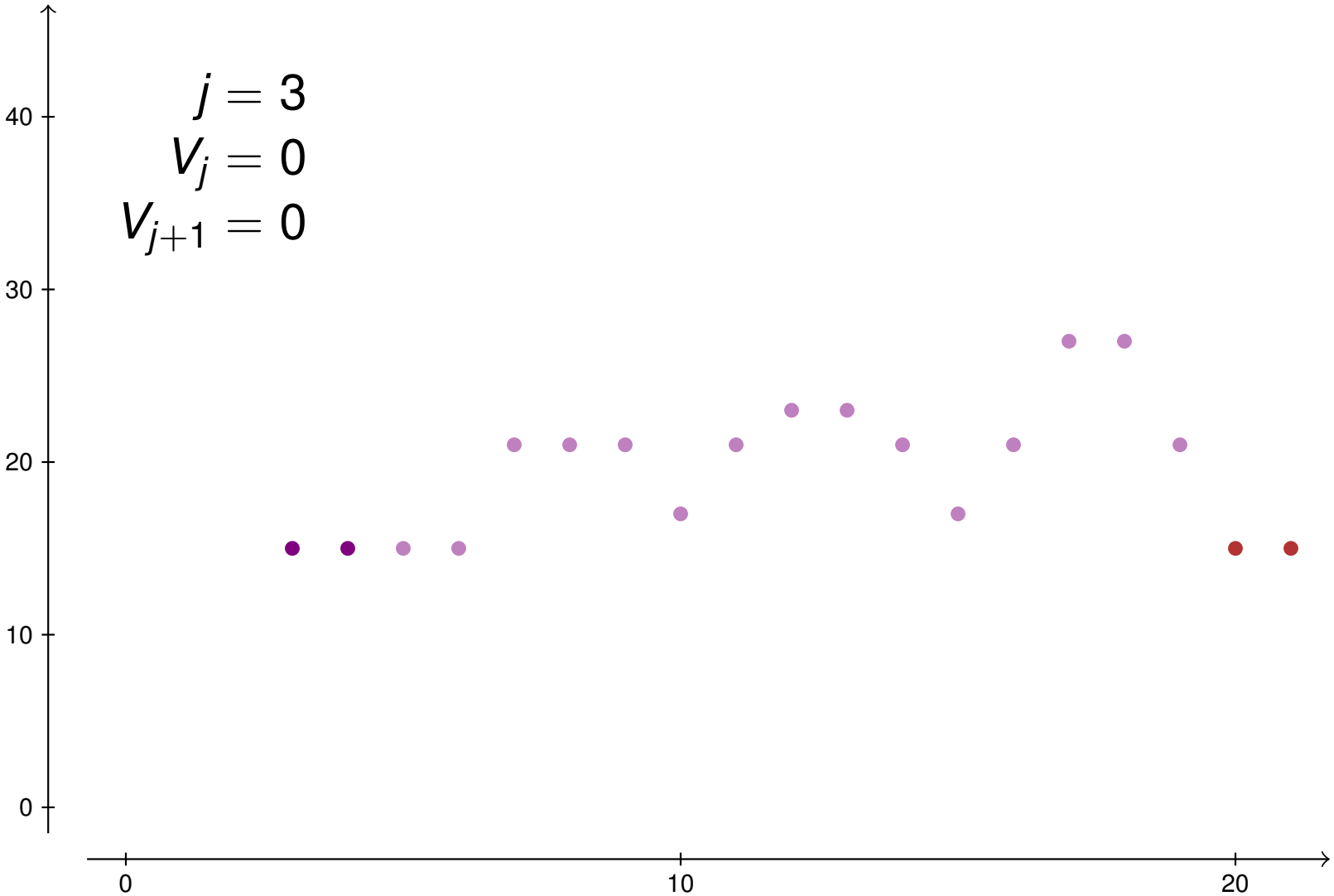
Une méthode adaptative



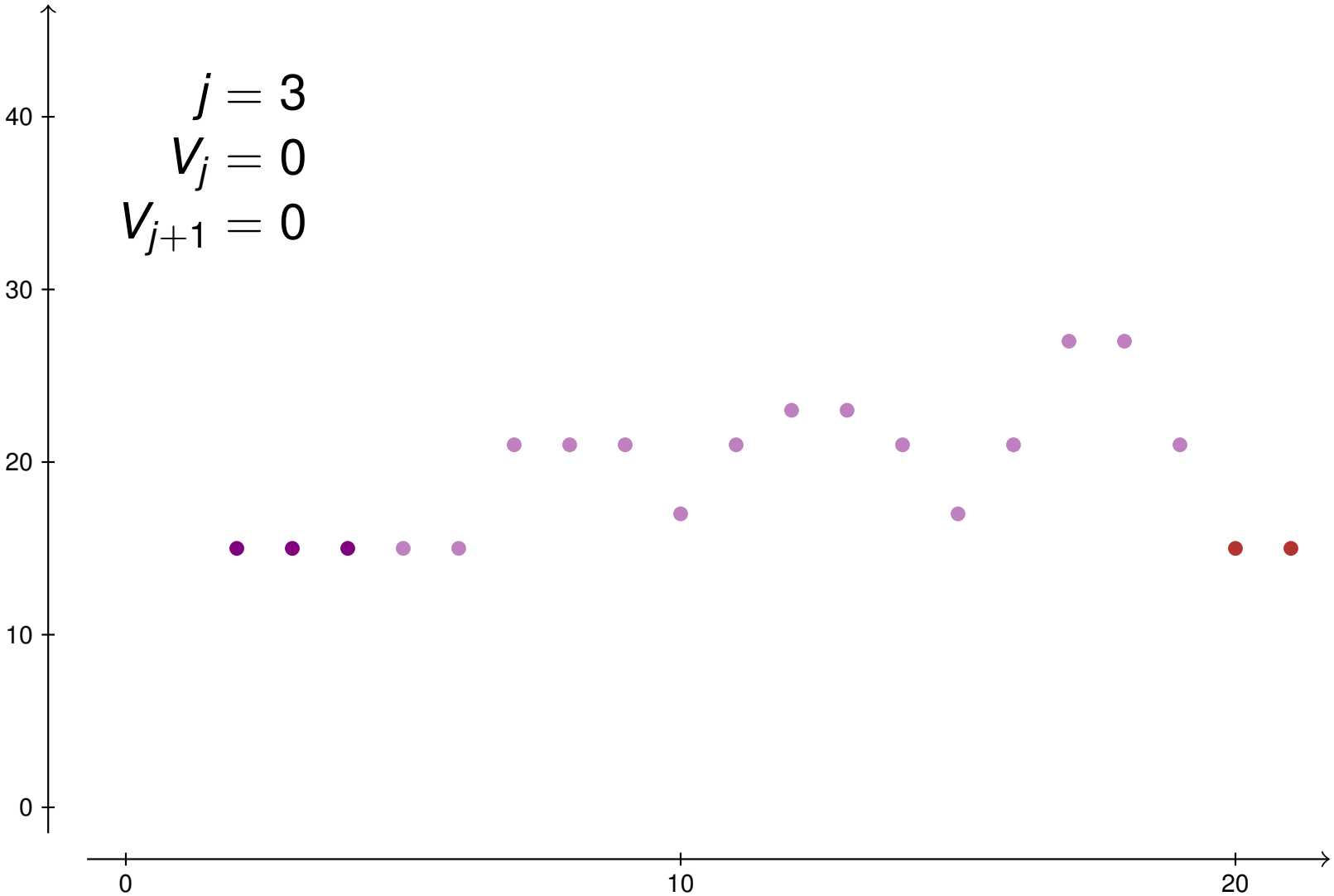
Une méthode adaptative



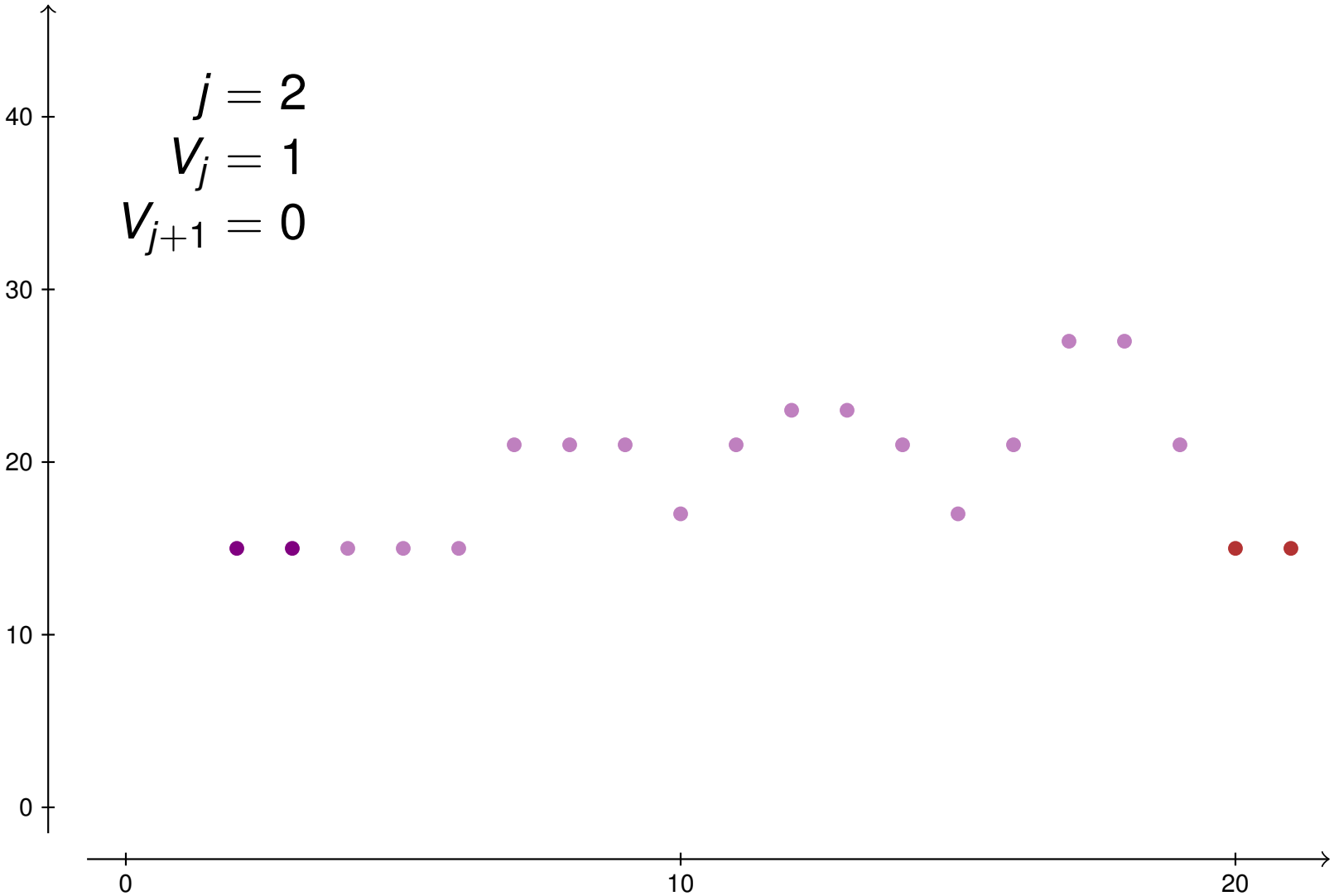
Une méthode adaptative



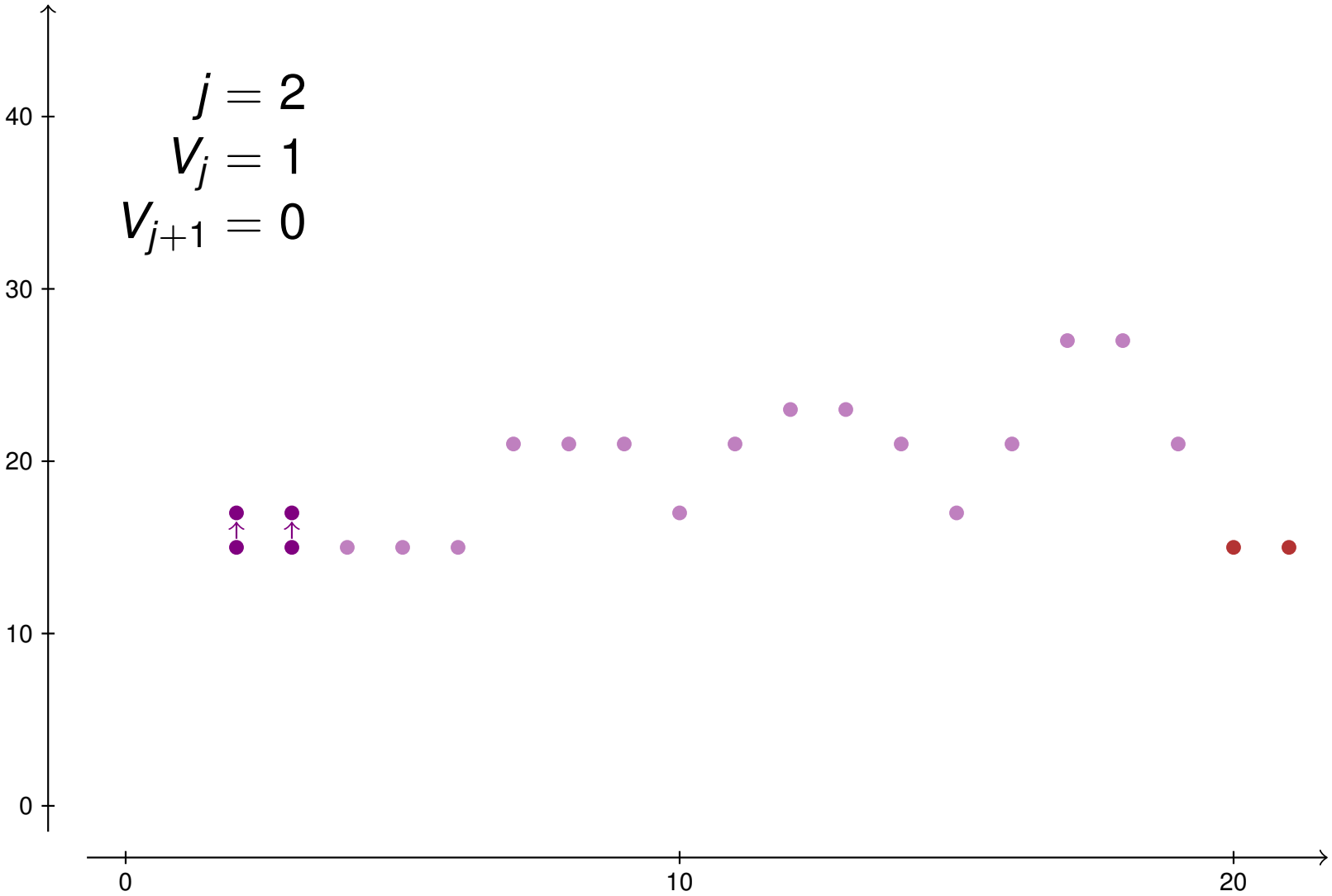
Une méthode adaptative



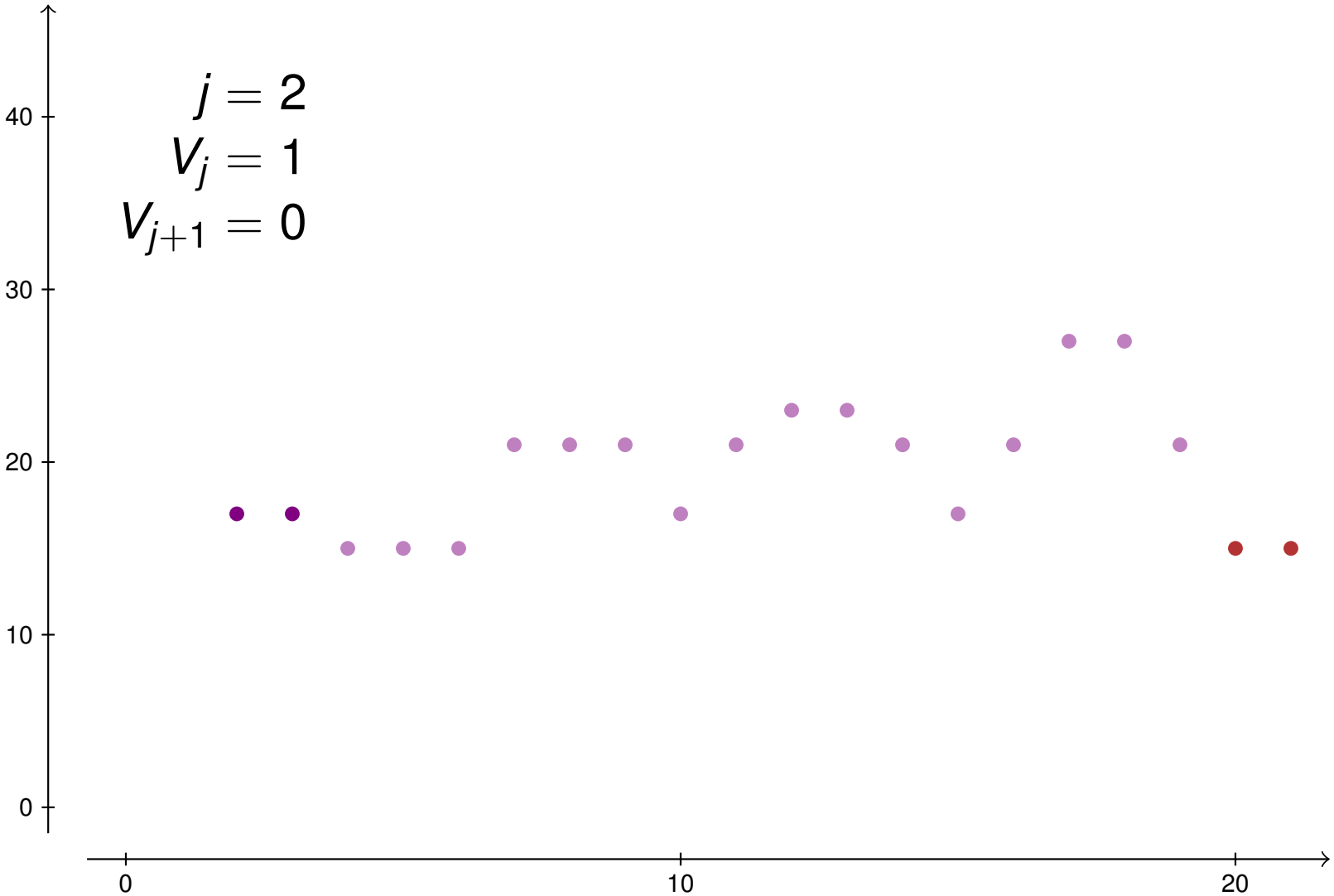
Une méthode adaptative



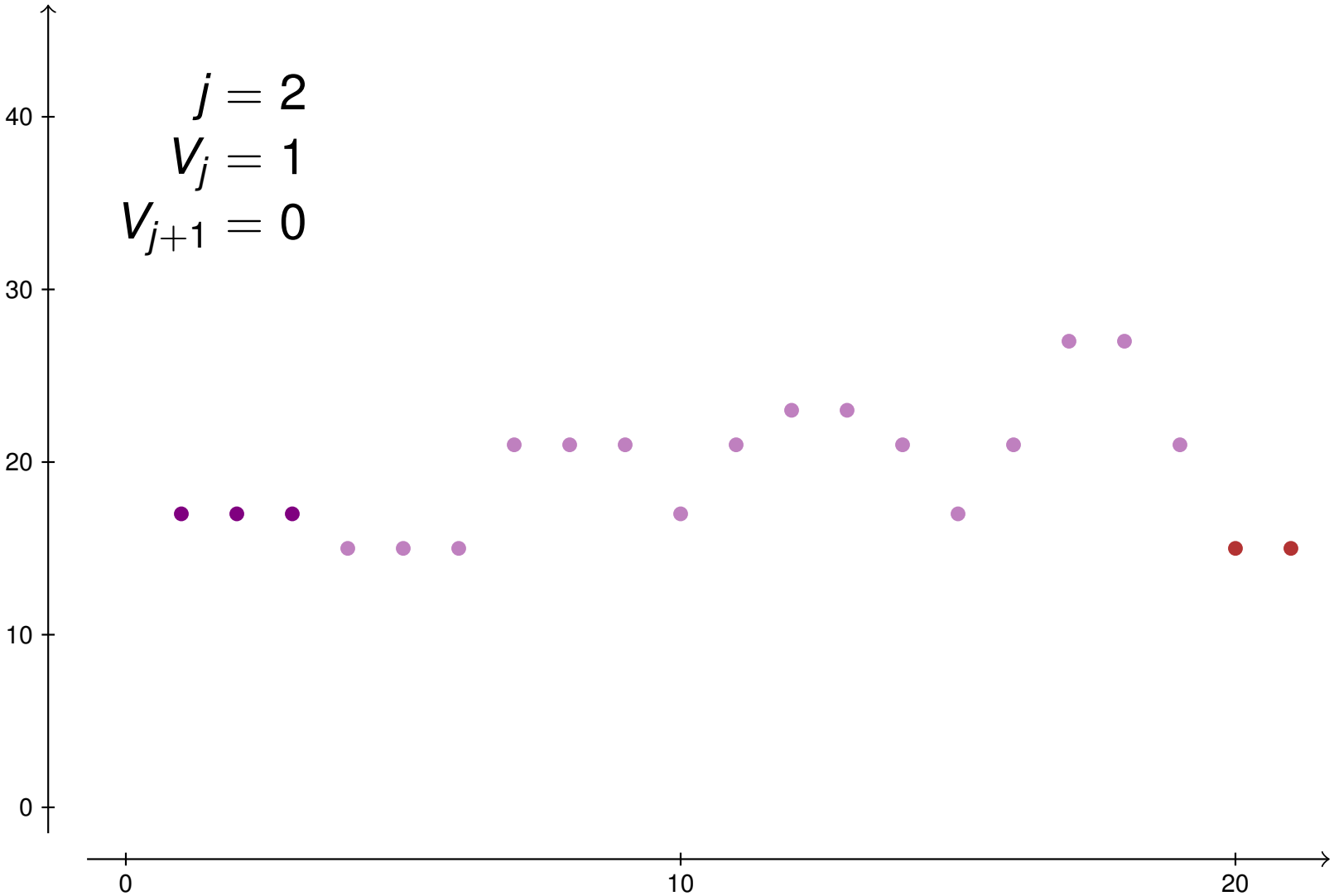
Une méthode adaptative



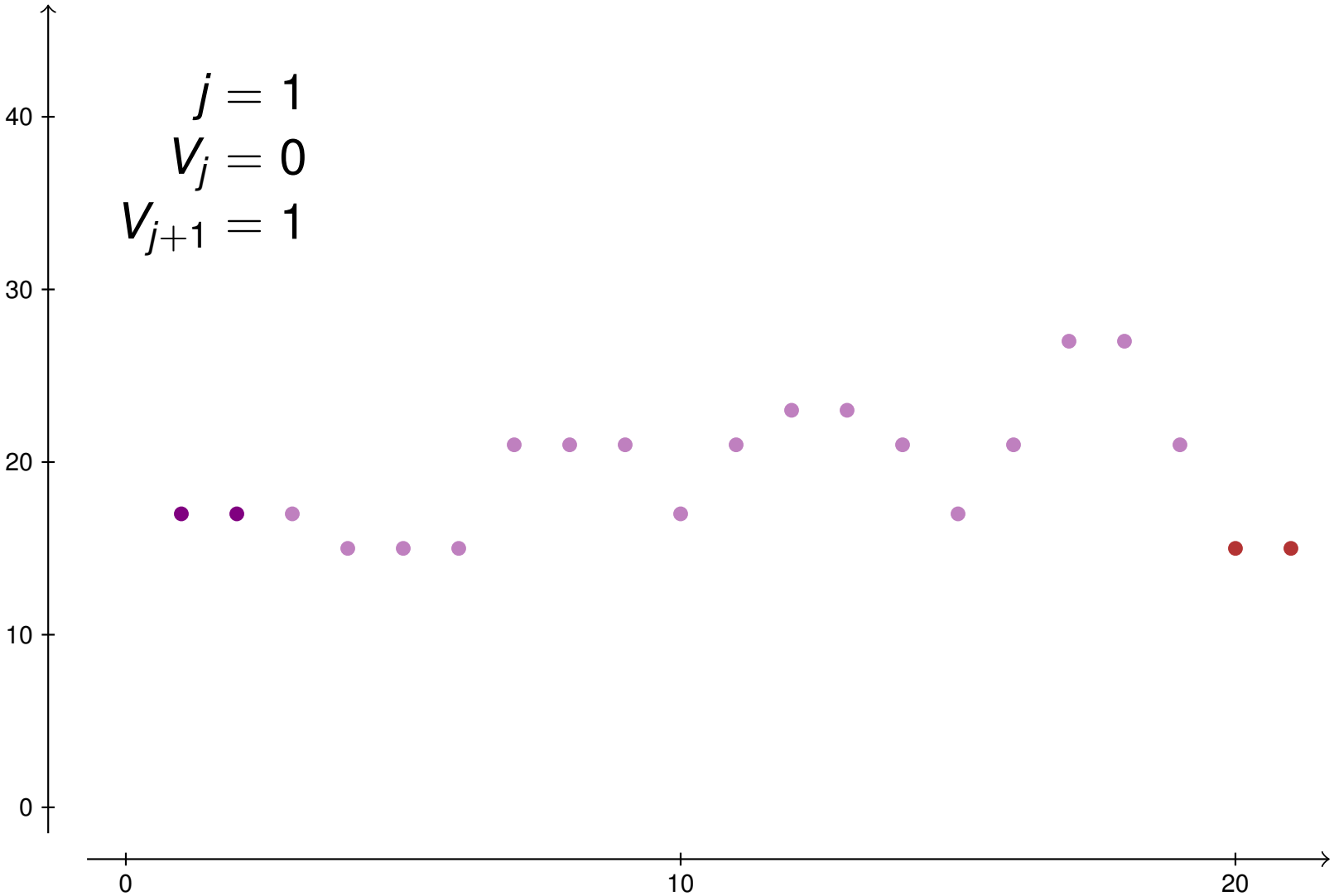
Une méthode adaptative



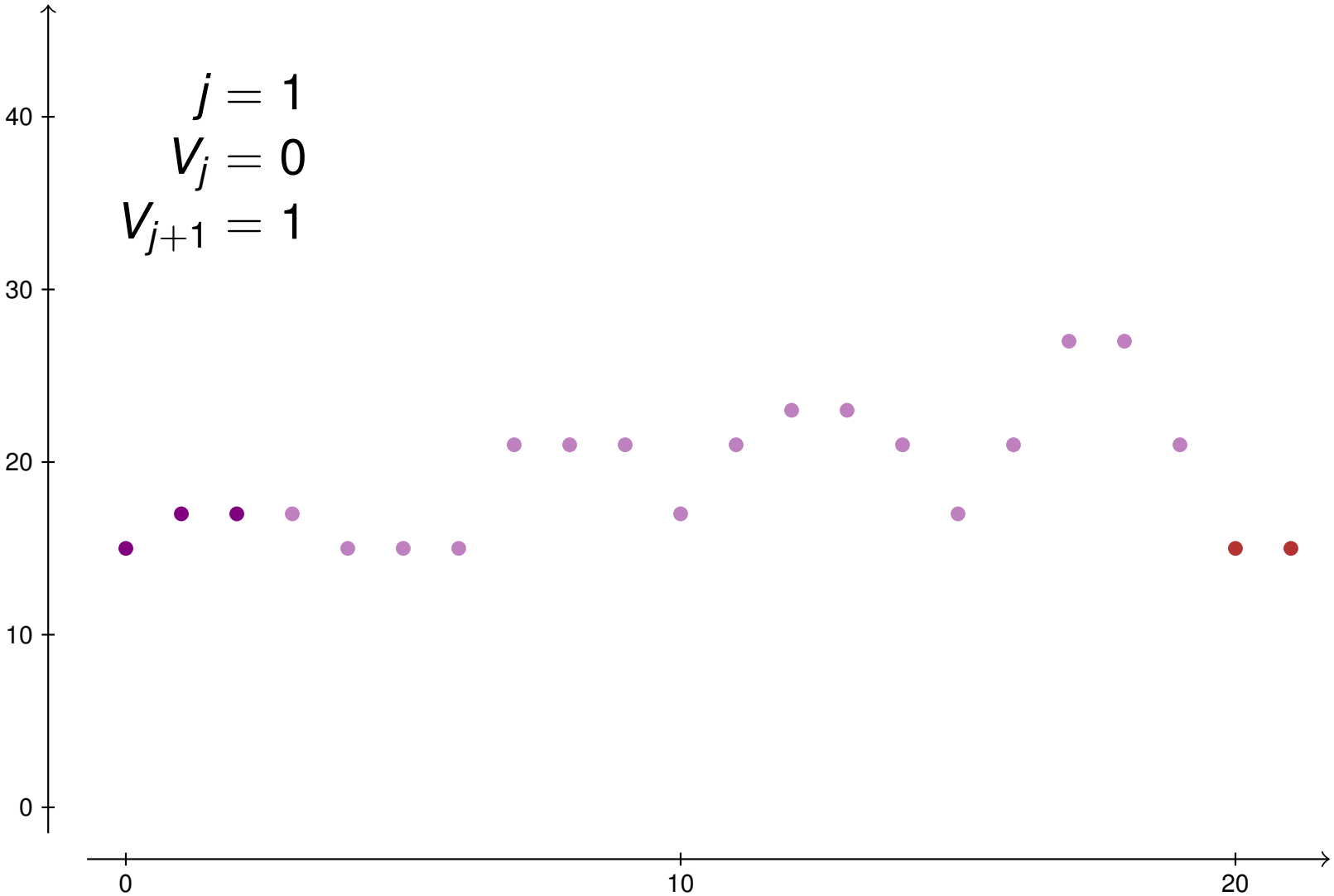
Une méthode adaptative



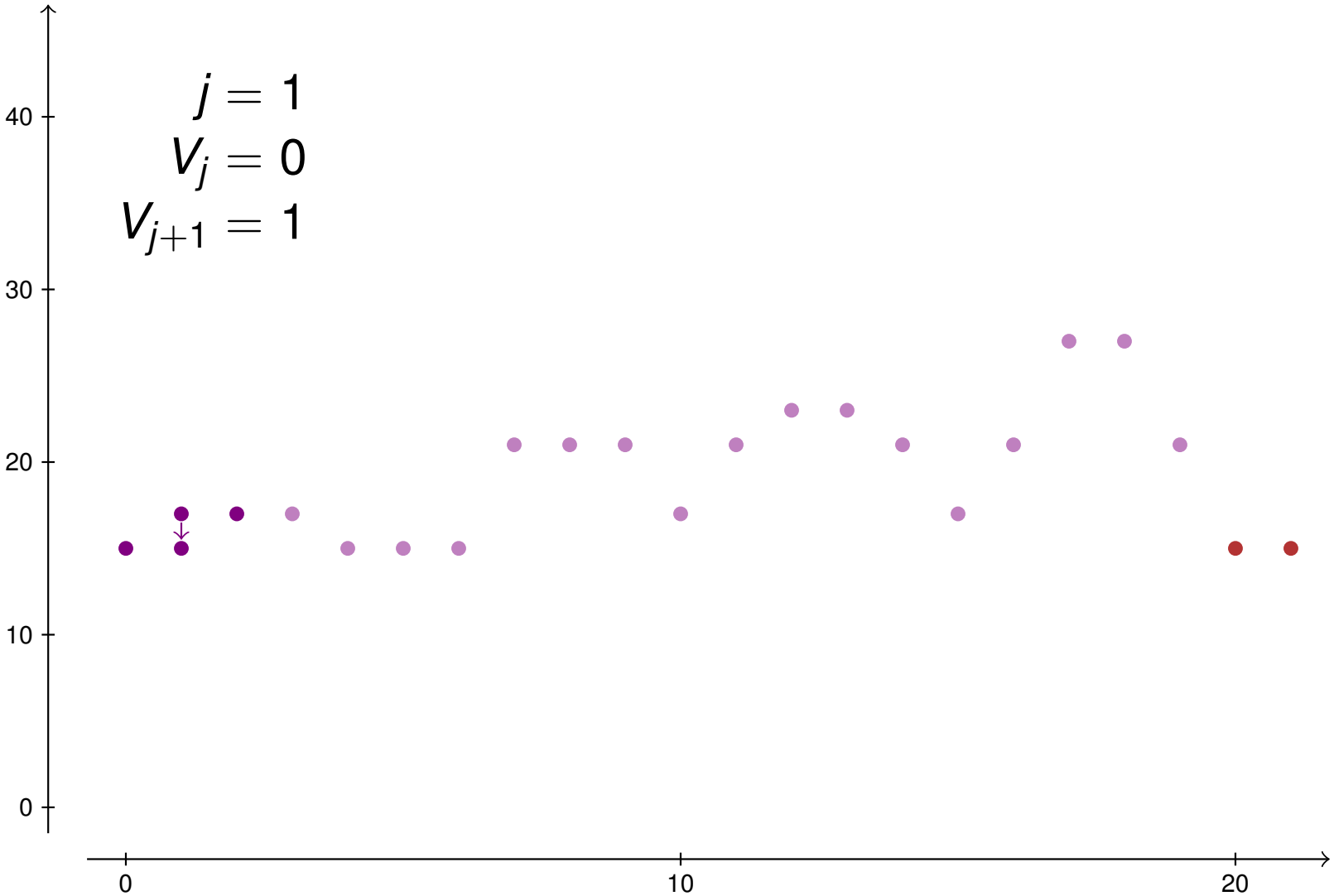
Une méthode adaptative



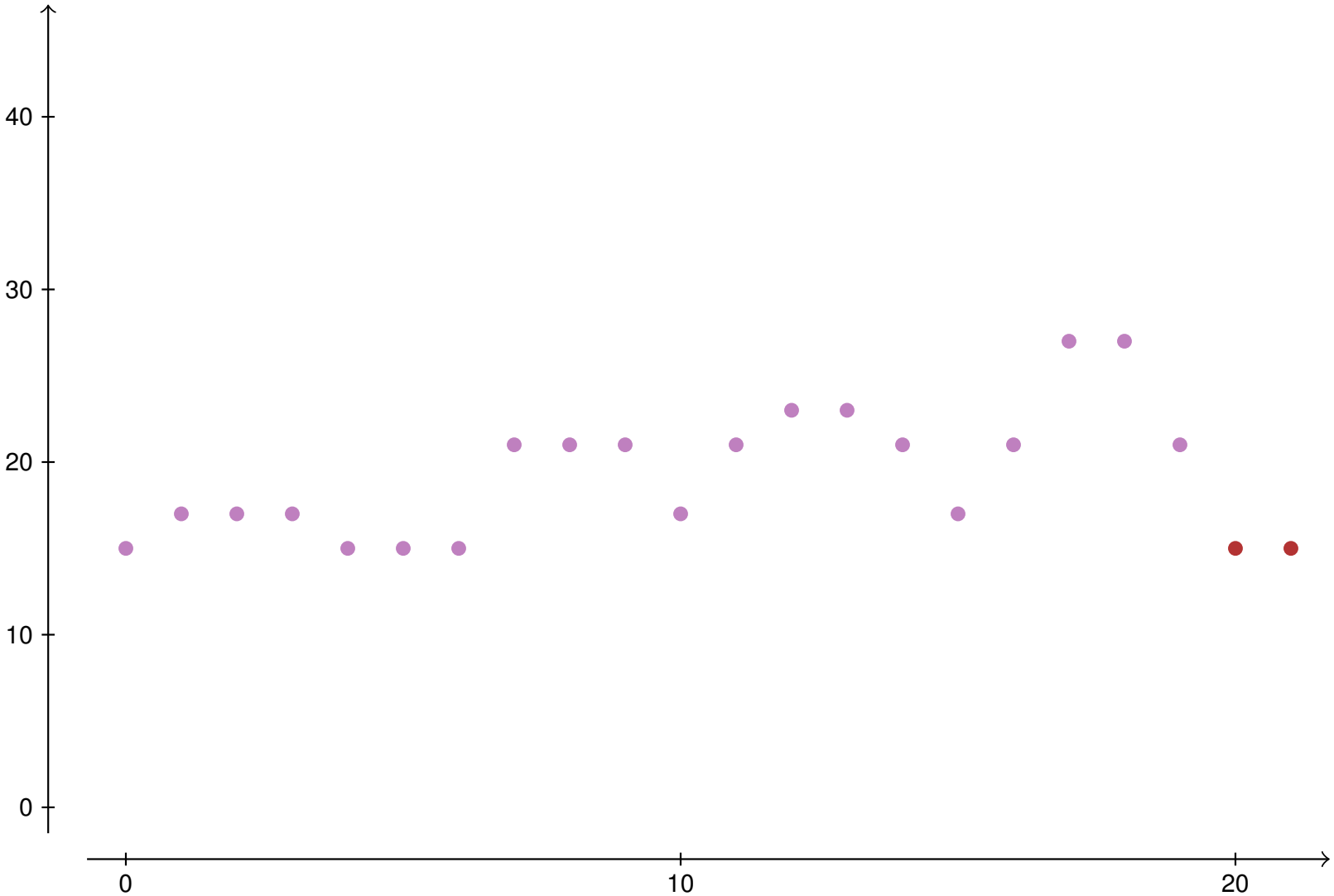
Une méthode adaptative



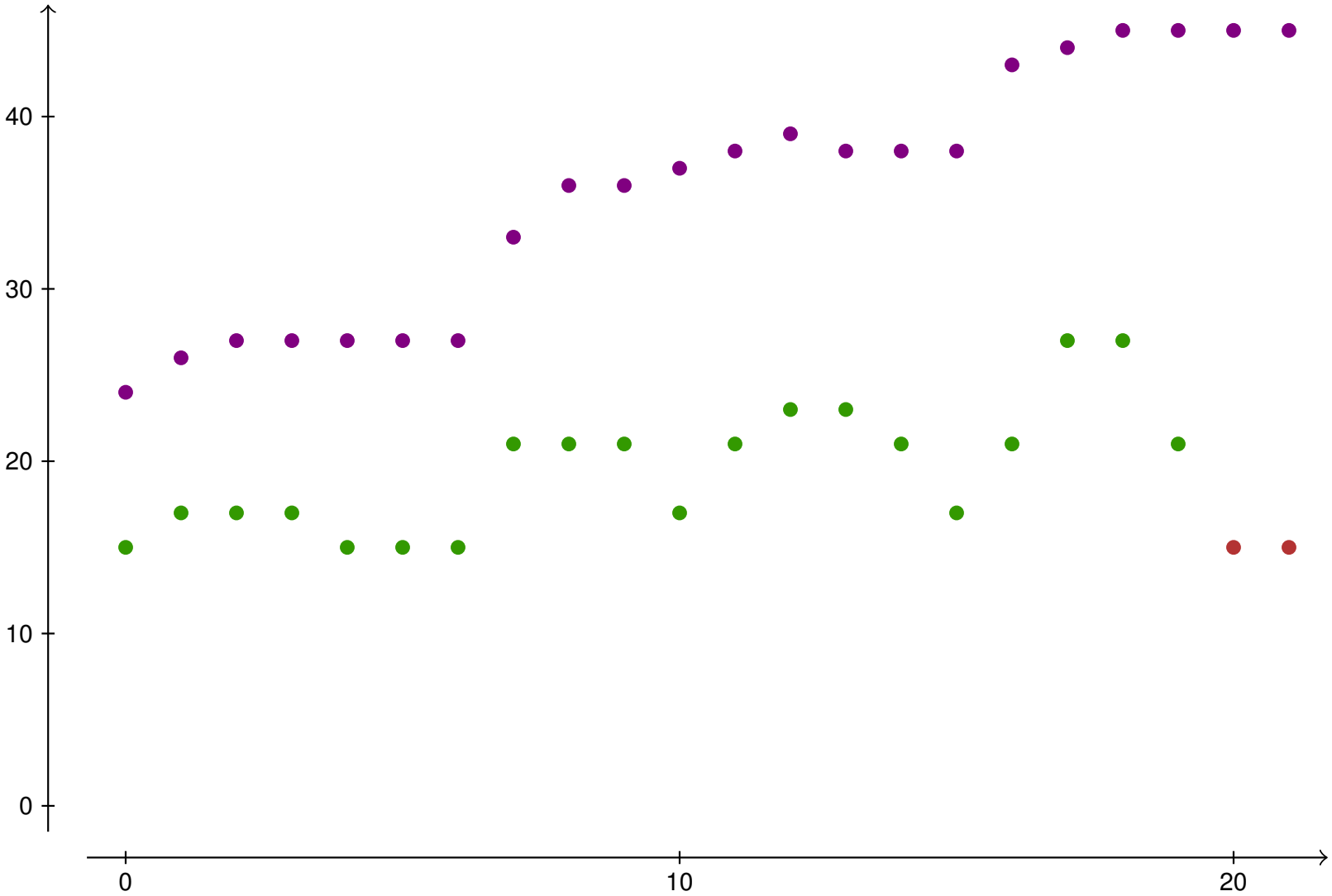
Une méthode adaptative



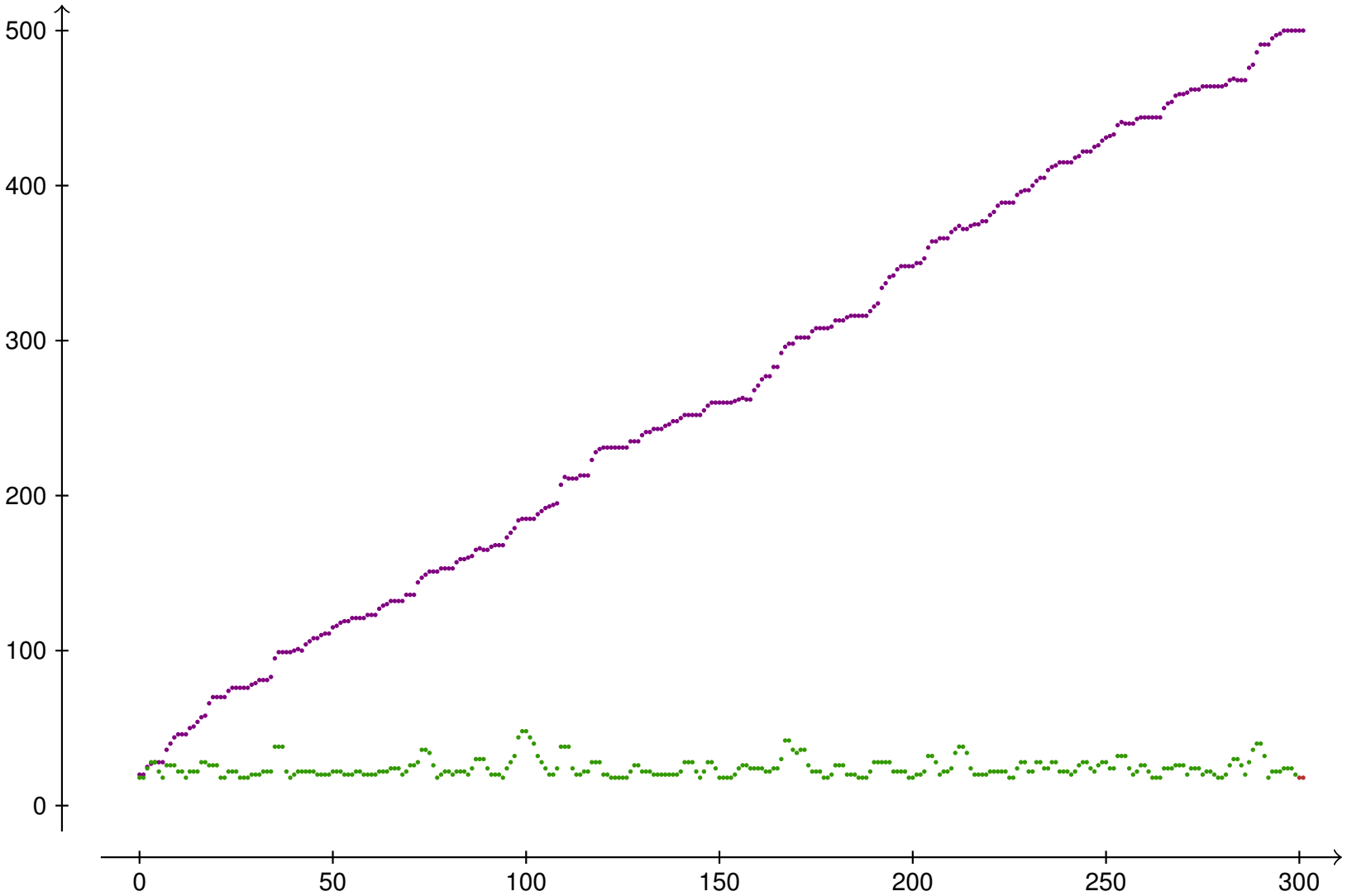
Une méthode adaptative



Comparaison des méthodes



Comparaison des méthodes



Conclusion

Vers les ≪ p-adiques flottants ≫ ?

Vers les ≪ p-adiques flottants ≫ ?

Concept

Vers les ≪ p-adiques flottants ≫ ?

Concept

On calcule avec un nombre de chiffres significatifs fixé *a priori*.

Vers les ≪ p-adiques flottants ≫ ?

Concept

On calcule avec un nombre de chiffres significatifs fixé *a priori*.
On complète par des zéros quand cela est nécessaire.

Vers les ≪ p-adiques flottants ≫ ?

Concept

On calcule avec un nombre de chiffres significatifs fixé *a priori*.
On complète par des zéros quand cela est nécessaire.

Inconvénient

Vers les ≪ p-adiques flottants ≫ ?

Concept

On calcule avec un nombre de chiffres significatifs fixé *a priori*.
On complète par des zéros quand cela est nécessaire.

Inconvénient

Aucune garantie sur l'exactitude des chiffres du résultat calculé.

Vers les « p-adiques flottants » ?

Concept

On calcule avec un nombre de chiffres significatifs fixé *a priori*.
On complète par des zéros quand cela est nécessaire.

Inconvénient

Aucune garantie sur l'exactitude des chiffres du résultat calculé.

Avantages (potentiels)

Vers les ≪ *p*-adiques flottants ≫ ?

Concept

On calcule avec un nombre de chiffres significatifs fixé *a priori*.
On complète par des zéros quand cela est nécessaire.

Inconvénient

Aucune garantie sur l'exactitude des chiffres du résultat calculé.

Avantages (potentiels)

Implémentation plus simple (et possiblement plus rapide).

Vers les « p-adiques flottants » ?

Concept

On calcule avec un nombre de chiffres significatifs fixé *a priori*.
On complète par des zéros quand cela est nécessaire.

Inconvénient

Aucune garantie sur l'exactitude des chiffres du résultat calculé.

Avantages (potentiels)

Implémentation plus simple (et possiblement plus rapide).

En moyenne, beaucoup de chiffres pourraient être corrects.

Vers les « p-adiques flottants » ?

Concept

On calcule avec un nombre de chiffres significatifs fixé *a priori*.
On complète par des zéros quand cela est nécessaire.

Inconvénient

Aucune garantie sur l'exactitude des chiffres du résultat calculé.

Avantages (potentiels)

Implémentation plus simple (et possiblement plus rapide).

En moyenne, beaucoup de chiffres pourraient être corrects.

[beaucoup = bien plus que ceux prédits par un suivi naïf de la précision]

Vers les « p-adiques flottants » ?

Concept

On calcule avec un nombre de chiffres significatifs fixé *a priori*.
On complète par des zéros quand cela est nécessaire.

Inconvénient

Aucune garantie sur l'exactitude des chiffres du résultat calculé.

Avantages (potentiels)

Implémentation plus simple (et possiblement plus rapide).

En moyenne, beaucoup de chiffres pourraient être corrects.

[beaucoup = bien plus que ceux prédits par un suivi naïf de la précision]

Exemples :
- calcul des sous-résultants

Vers les « p-adiques flottants » ?

Concept

On calcule avec un nombre de chiffres significatifs fixé *a priori*.
On complète par des zéros quand cela est nécessaire.

Inconvénient

Aucune garantie sur l'exactitude des chiffres du résultat calculé.

Avantages (potentiels)

Implémentation plus simple (et possiblement plus rapide).

En moyenne, beaucoup de chiffres pourraient être corrects.

[beaucoup = bien plus que ceux prédits par un suivi naïf de la précision]

Exemples :
- calcul des sous-résultants
- résolution d'équations différentielles

Vers les « p-adiques flottants » ?

Concept

On calcule avec un nombre de chiffres significatifs fixé *a priori*.
On complète par des zéros quand cela est nécessaire.

Inconvénient

Aucune garantie sur l'exactitude des chiffres du résultat calculé.

Avantages (potentiels)

Implémentation plus simple (et possiblement plus rapide).

En moyenne, beaucoup de chiffres pourraient être corrects.

[beaucoup = bien plus que ceux prédits par un suivi naïf de la précision]

Exemples :

- calcul des sous-résultants
- résolution d'équations différentielles
- calcul de la décomposition LU d'une matrice

Vers les « p-adiques flottants » ?

Concept

On calcule avec un nombre de chiffres significatifs fixé *a priori*.
On complète par des zéros quand cela est nécessaire.

Inconvénient

Aucune garantie sur l'exactitude des chiffres du résultat calculé.

Avantages (potentiels)

Implémentation plus simple (et possiblement plus rapide).

En moyenne, beaucoup de chiffres pourraient être corrects.

[beaucoup = bien plus que ceux prédits par un suivi naïf de la précision]

Exemples :

- calcul des sous-résultants
- résolution d'équations différentielles
- calcul de la décomposition LU d'une matrice
- calcul de la suite de SOMOS 4

Merci pour votre attention