

Complexité CM9

Antonio E. Porreca

aeporreca.org/complexite

**Précédemment
dans Complexité...**

! Définition 3-A (p. 64) !

Réductions (many-one) polynomiales

- Une **réduction (many-one) en temps polynomial** d'un problème L_1 (sur l'alphabet Σ_1) à un problème L_2 (sur l'alphabet Σ_2) est une fonction $f: \Sigma_1^* \rightarrow \Sigma_2^*$ calculable en temps polynomial déterministe telle que

$$\forall x \in \Sigma_1^* \quad x \in L_1 \iff f(x) \in L_2$$

- Si une telle f existe, on dit que L_1 **se réduit à L_2** (via f) et on notera $L_1 \leq_m^P L_2$ (ou parfois, en bref, $L_1 \leq L_2$)

! Définition 3-J (p. 67) !

Difficulté et complétude

Soit L un problème et \mathcal{C} une classe de complexité

- On dit que L est \mathcal{C} -difficile (ou \mathcal{C} -dur) si pour tout problème $L' \in \mathcal{C}$ on a $L' \leq L$
- On dit que L est \mathcal{C} -complet s'il est \mathcal{C} -difficile et en plus on a $L \in \mathcal{C}$

Proposition 3-M (p. 68)

La prédiction est NP-complète

Le problème suivant est NP-complet :

$$A = \{(\langle N \rangle, x, 1^t) : N(x) \text{ accepte en temps } \leq t\}$$

code d'une MT
non déterministe

mot d'entrée
pour la MT N

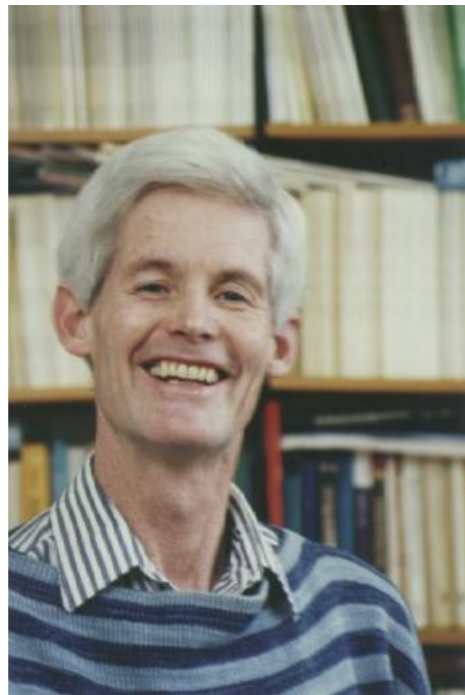
entier $t \in \mathbb{N}$
en unaire

**Et maintenant,
la suite**

Le théorème de
Cook-Levin, ou :
Enfin, un problème
NP-complet
intéressant ! 🎉

! Théorème 3-V (p. 72) !

Cook 1971, Levin 1973



Stephen Cook



Леонід Лєвин

SAT est NP-complet

! Théorème 3-V (p. 72) !

Cook 1971, Levin 1973

Le **fonctionnement** en temps polynomial d'une machine non déterministe N sur une entrée x **est décrit par une formule φ** calculable en temps polynomial telle que le nombre d'affectations satisfaisant φ est égal au nombre de chemins acceptants de $N(x)$.

Idée de la démonstration

- $\text{SAT} \in \text{NP}$ car il suffit de **deviner** une affectation des variables et **vérifier** en temps polynomial qu'elle satisfait la formule
- La complétude vient du fait qu'on peut décrire par une formule de taille polynomiale le **diagramme espace-temps** d'une exécution d'une machine non déterministe polynomiale car celui-ci répond à des **règles locales**

Idée de la démonstration

- En d'autres termes, on décrit par une formule $\varphi(\vec{y})$ le fonctionnement de la machine le long du chemin (découlant du choix des transitions) décrit par \vec{y}
- Pour savoir s'il existe un chemin acceptant dans le calcul de la machine, il suffit alors de savoir s'il existe une affectation des variables \vec{y} de la formule pour laquelle l'état final du diagramme décrit est acceptant, ce qui est un problème de type SAT

Démonstration : SAT \in NP

- Algo non déterministe pour SAT sur l'entrée $\varphi(x_1, \dots, x_n)$:
 - deviner $(a_1, \dots, a_n) \in \{0,1\}^n$
 - accepter ssi $\varphi(a_1, \dots, a_n) = 1$
- En alternative, un vérificateur déterministe sur l'entrée $(\varphi(x_1, \dots, x_n), a_1, \dots, a_n)$:
 - accepter ssi $\varphi(a_1, \dots, a_n) = 1$

Démonstration :

$B \leq \text{SAT}$ pour tout $B \in \text{NP}$ 😎

- Soit $B \in \text{NP}$
- À toute instance x de B on associe une formule $\varphi_x \dots$
- ...telle que φ_x est satisfaisable ssi $x \in B$
- Les **variables** de φ_x désigneront en quelque sorte **le chemin de calcul à suivre**

Démonstration :

$B \leq \text{SAT}$ pour tout $B \in \text{NP}$ 😎

- Soit N une machine non déterministe qui reconnaît B
 - en temps polynomiale $p(n)$
 - avec ensemble d'états Q , alphabet de travail Γ
- nous allons « simuler » le fonctionnement de N le long d'un chemin arbitraire par φ_x
- Pour cela, nous allons considérer le diagramme espace-temps de $N(x)$

Diagramme **espace-temps**

de la MT N sur l'entrée $x = x_0 \cdots x_{n-1}$

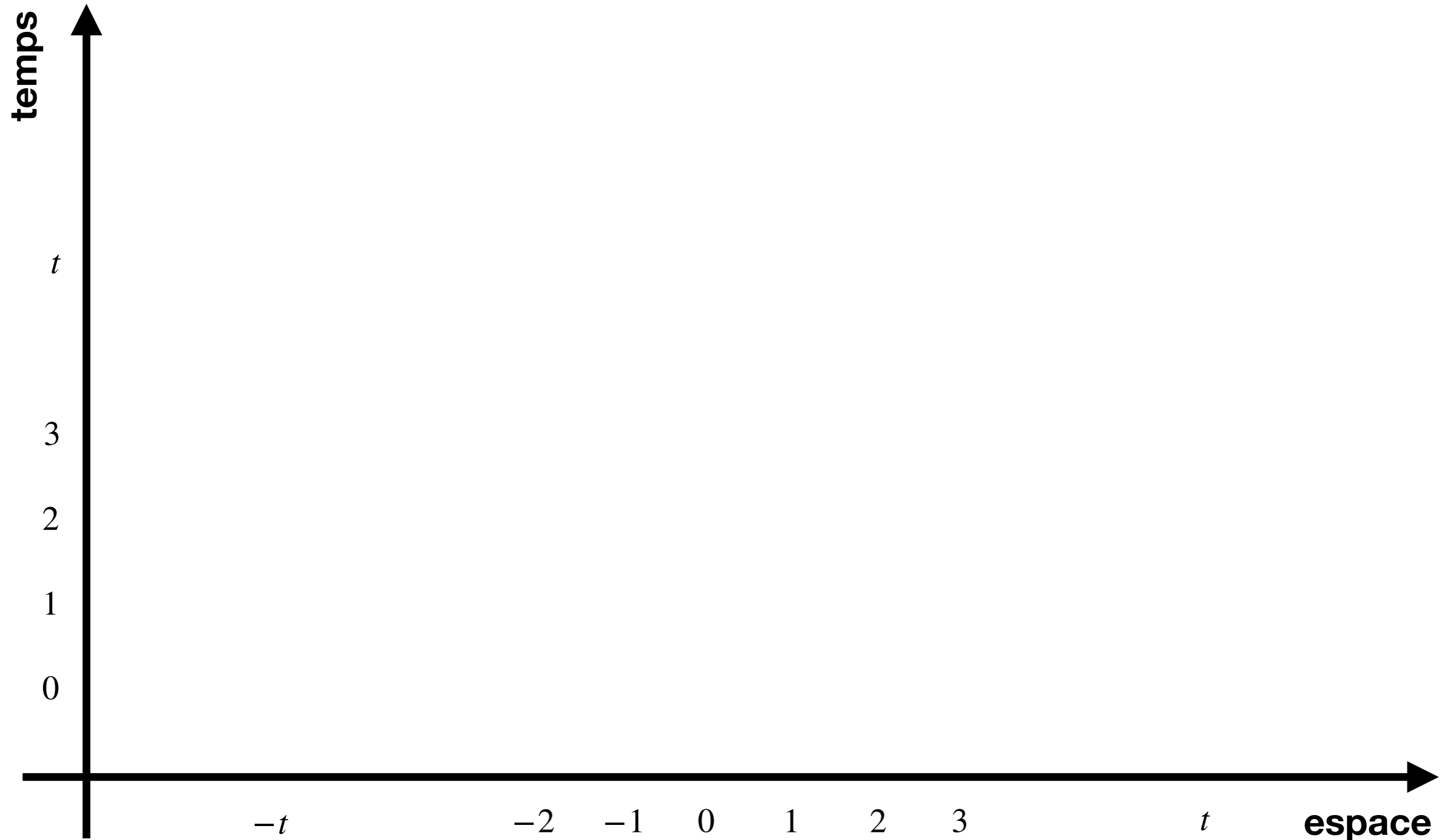
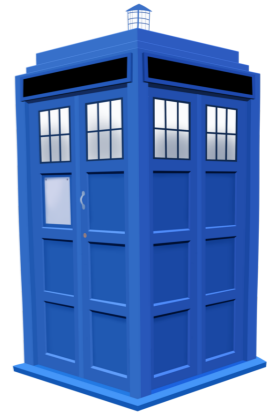


Diagramme **espace-temps**

de la MT N sur l'entrée $x = x_0 \cdots x_{n-1}$

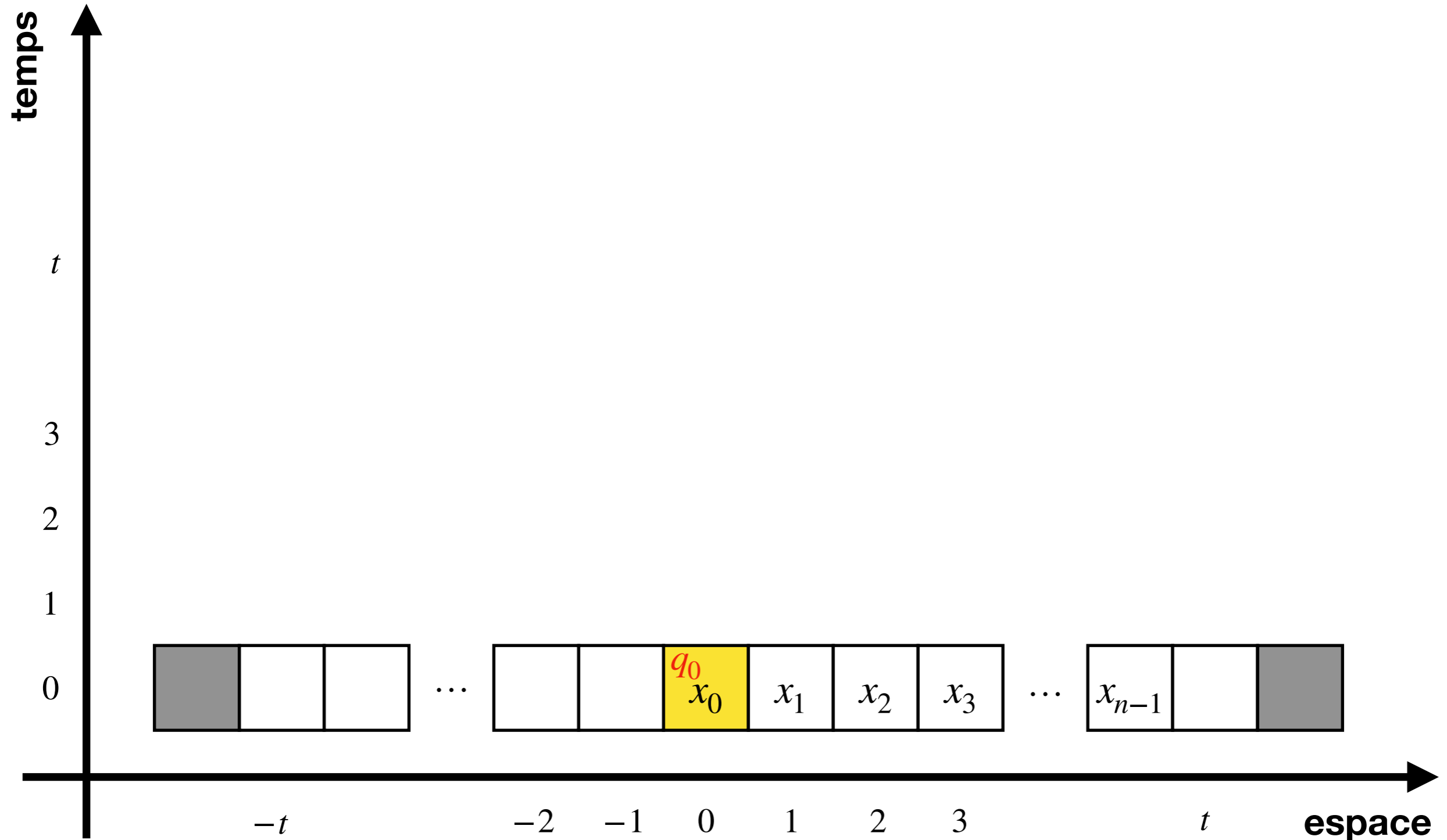
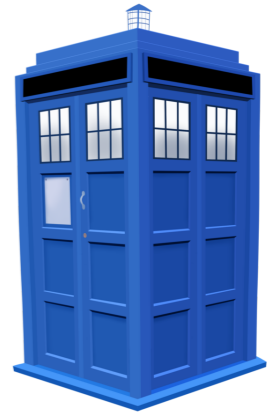


Diagramme **espace-temps**

de la MT N sur l'entrée $x = x_0 \cdots x_{n-1}$

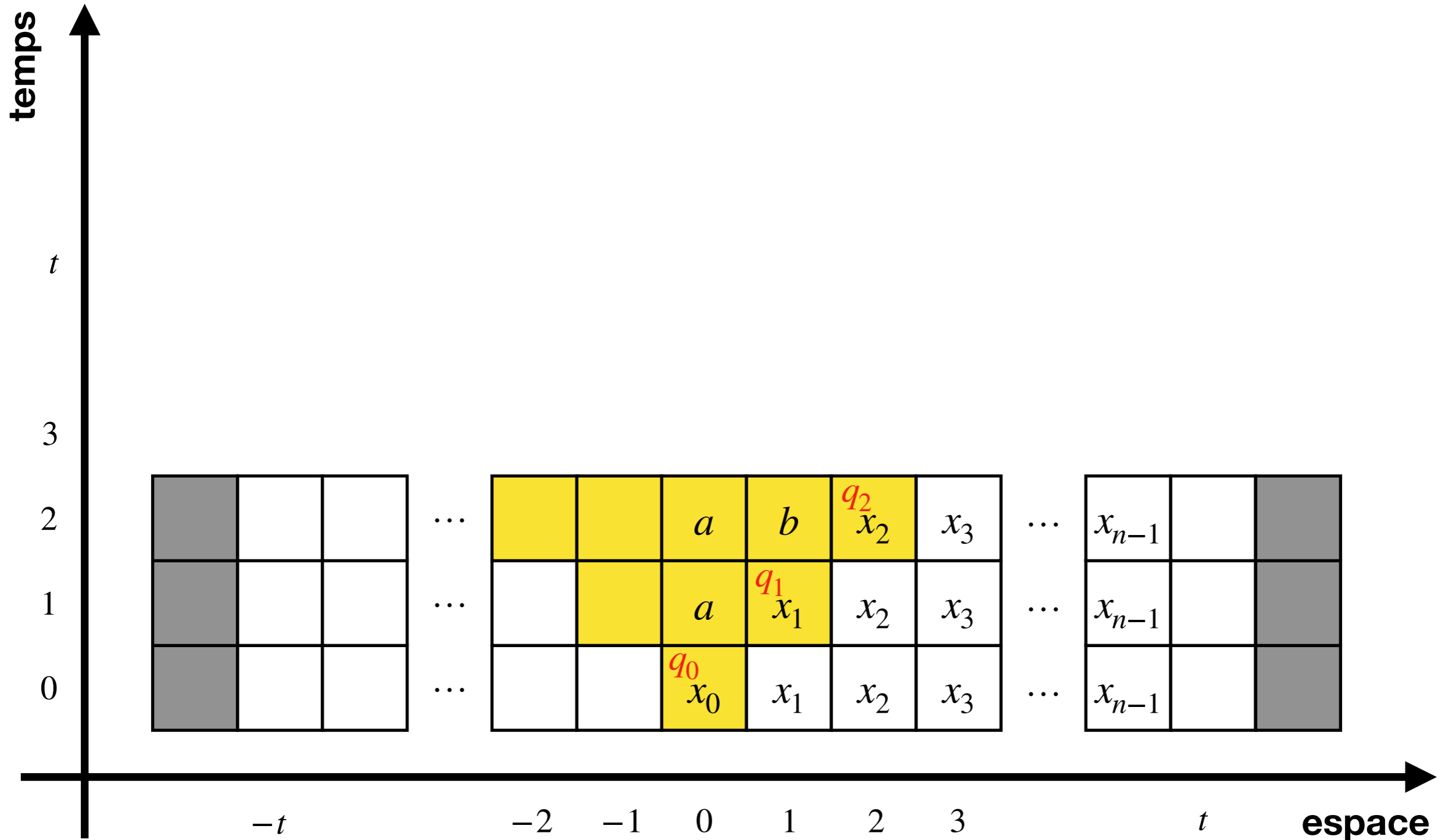
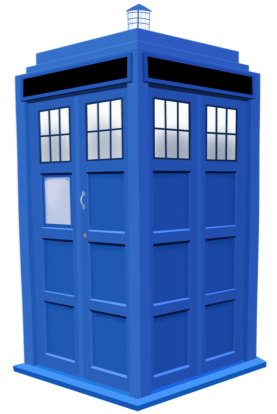


Diagramme **espace-temps**

de la MT N sur l'entrée $x = x_0 \cdots x_{n-1}$

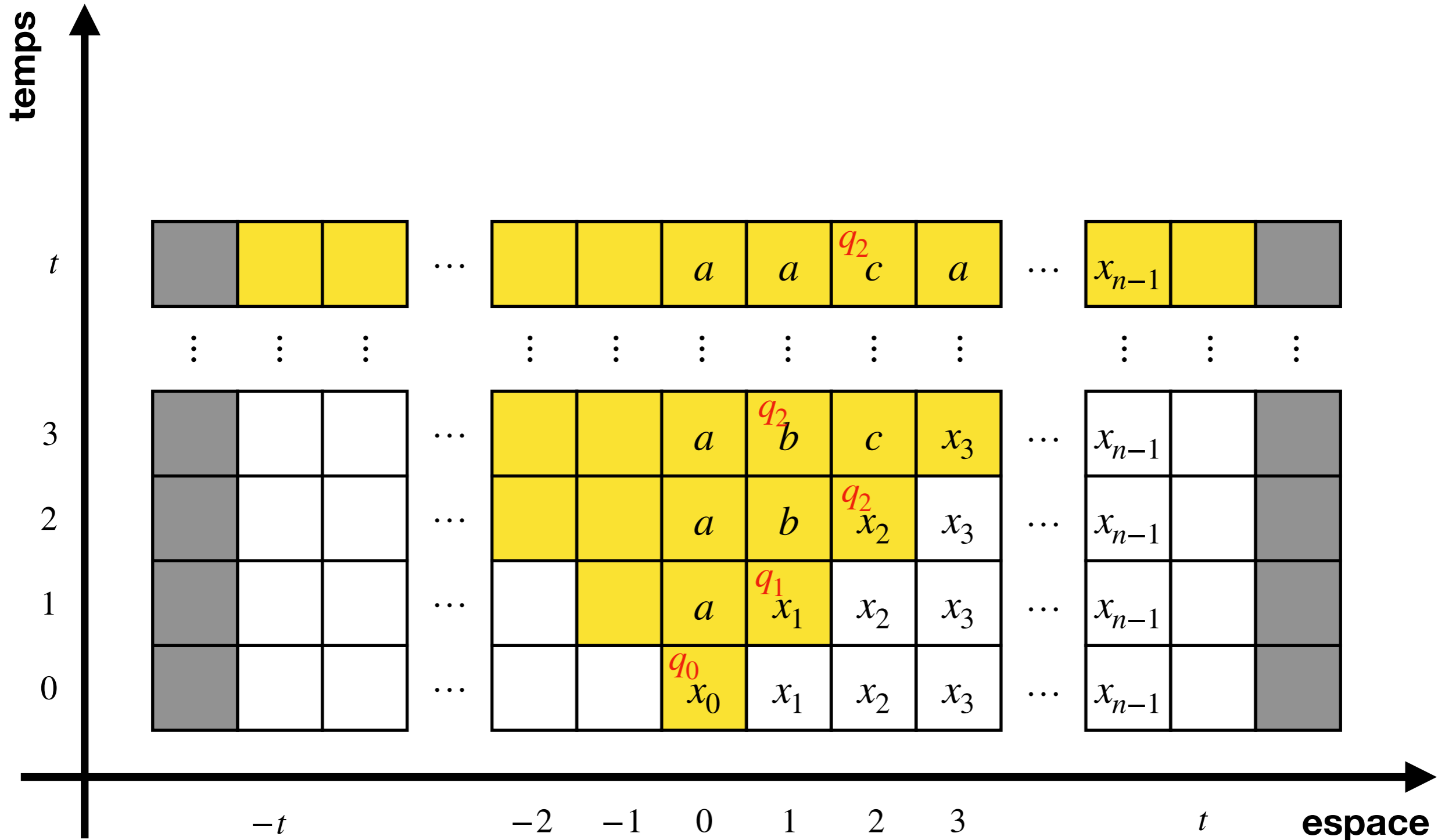
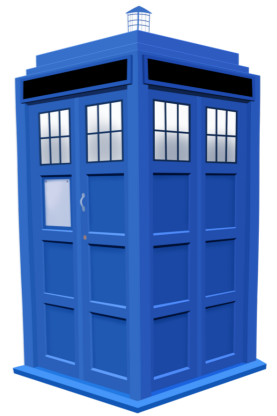


Diagramme **espace-temps**

de la MT N sur l'entrée $x = x_0 \cdots x_{n-1}$

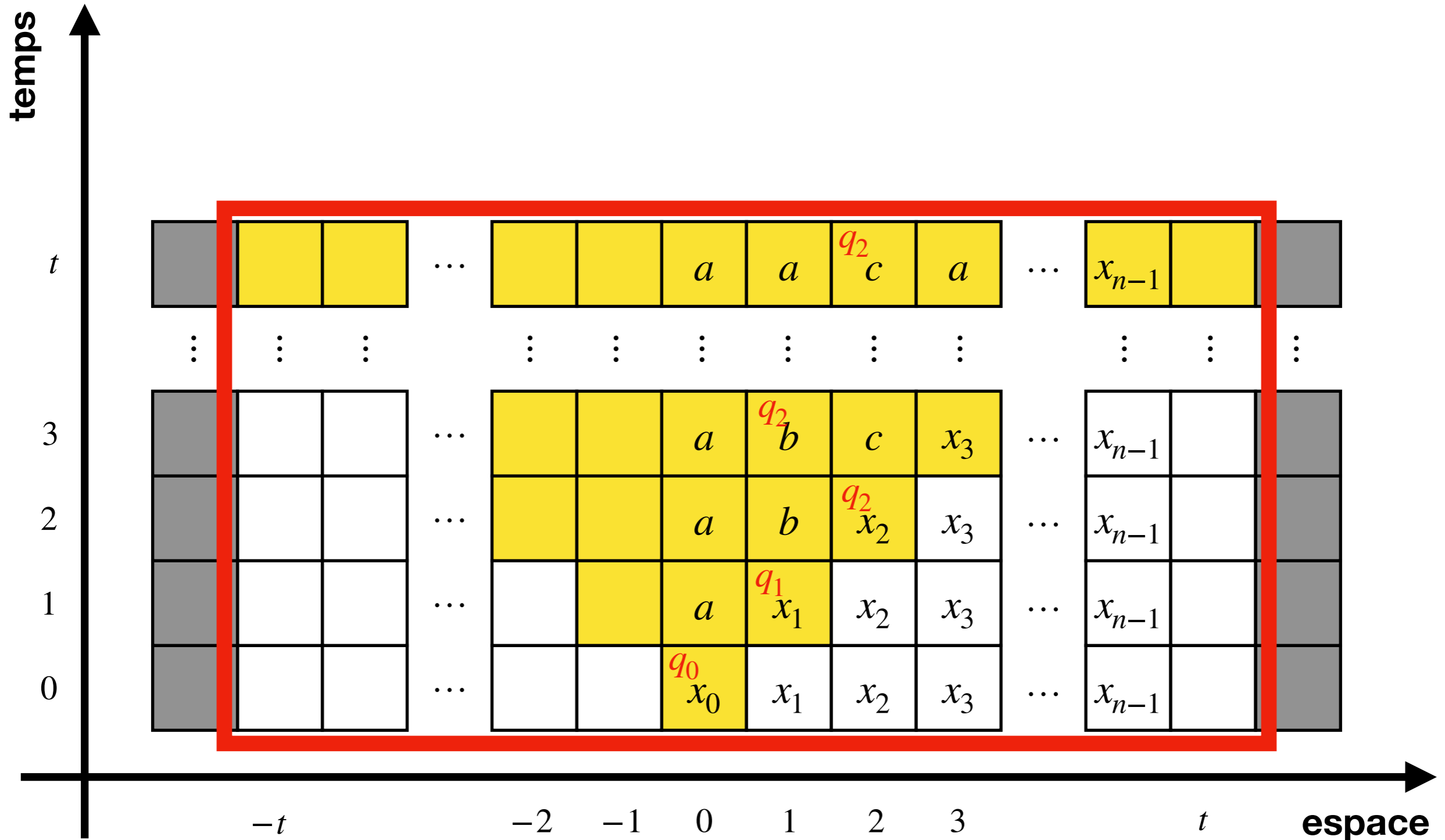
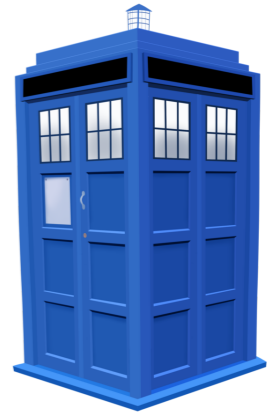


Diagramme **espace-temps**

de la MT N sur l'entrée $x = x_0 \cdots x_{n-1}$

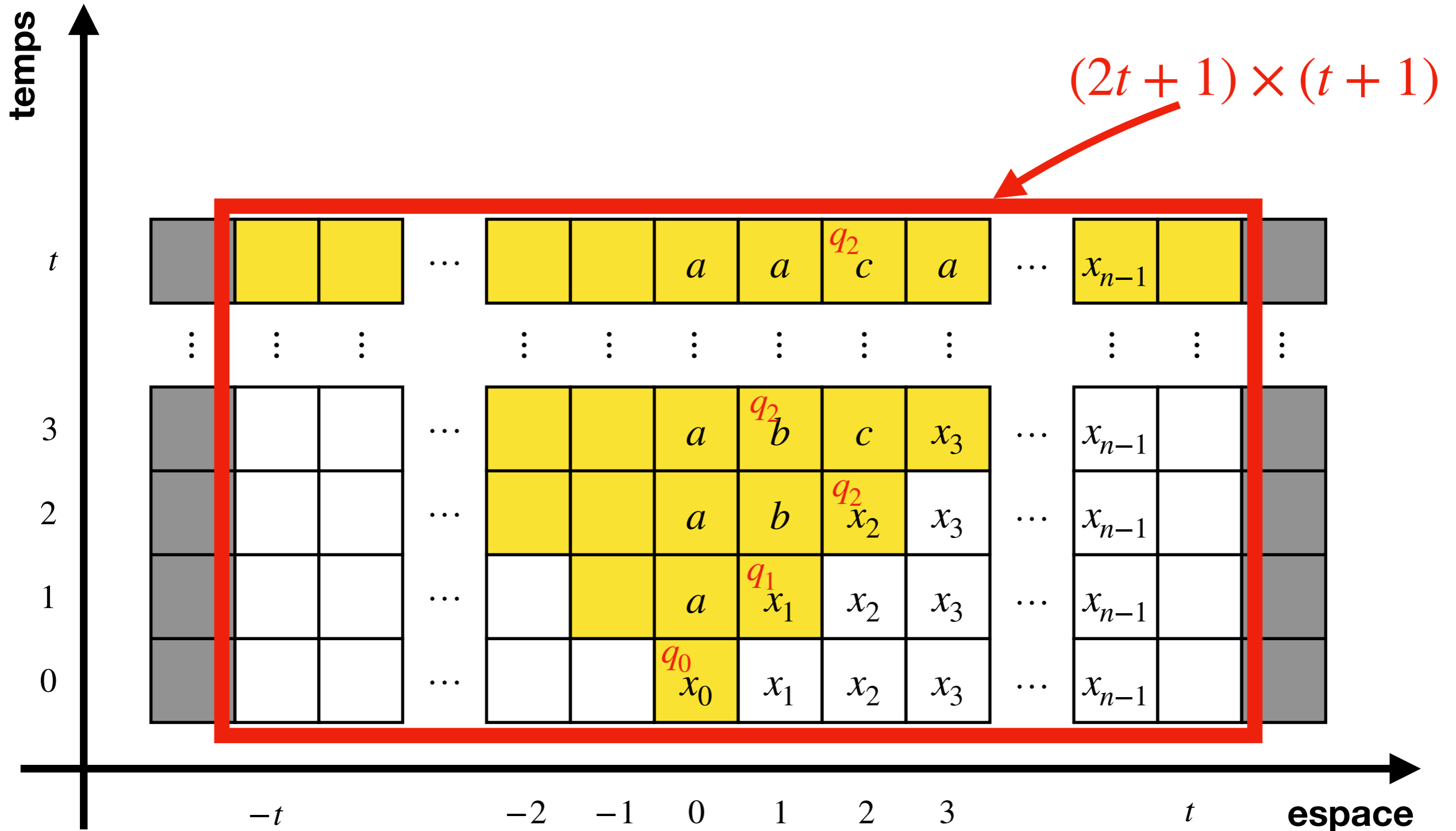
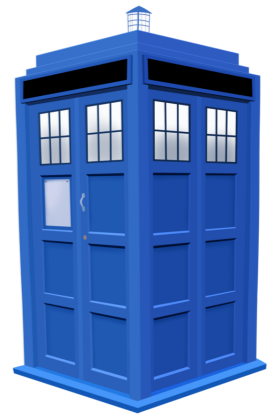
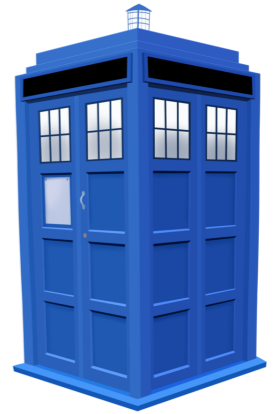


Diagramme **espace-temps** de la MT N sur l'entrée $x = x_1 \cdots x_n$



- Le diagramme espace-temps du ruban de N décrit le calcul sur l'entrée x
- Si le calcul de $N(x)$ termine en moins de t étapes, on suppose que le diagramme espace-temps répète la dernière ligne
- Notre formule φ_x va affirmer que le calcul **commence dans la configuration initiale**, que le diagramme **espace-temps** de la machine est **cohérent avec la relation de transition** et qu'on **termine dans un état acceptant**

La formule φ_x a quatre parties

- **cohérence**, signifiant que deux symboles ne sont pas assignés à la même case, deux positions à la tête, deux états à la même étape
- **début_x**, signifiant que la configuration initiale est la bonne
- pour chaque étape j : **transition_j**, signifiant que la j -ème transition est valide
- **accepte**, signifiant qu'on arrive dans un état acceptant à un temps $\leq t$, ou $t = p(n)$

Variables de la formule φ_x

Pour chaque étape $j \in \{0, \dots, t\}$, symbole $\gamma \in \Gamma$, position $i \in \{-t, \dots, 0, \dots, t\}$, état $q \in Q$:

- $c_{\gamma,i,j} = 1$ ssi la i -ème case du ruban contient le symbole γ au temps j
- $p_{i,j} = 1$ ssi la tête du ruban est à la position i au temps j
- $e_{q,j} = 1$ ssi l'état de la machine est q à l'instant j

En total on a $(t + 1)(2t + 1) |\Gamma| + (t + 1)(2t + 1) + (t + 1) |Q|$ variables, ce qui est polynomial par rapport à $n = |x|$

! Notation !

Dans les formules logiques suivantes, les symboles

$$\bigwedge_{i=1}^n \phi_i \quad \bigvee_{i=1}^n \phi_i$$

représentent succinctement les conjonctions ou disjonctions

$$\phi_1 \wedge \phi_2 \wedge \dots \wedge \phi_n \quad \phi_1 \vee \phi_2 \vee \dots \vee \phi_n$$

c'est-à-dire, en réalité il faut **répliquer explicitement** les sous-formules ϕ_i pour toutes les valeurs de l'indice i

Par exemple :

$$\bigwedge_{i=1}^2 \bigvee_{j=1}^2 (x_i \wedge \neg y_j) = ((x_1 \wedge \neg y_1) \vee (x_1 \wedge \neg y_2)) \wedge ((x_2 \wedge \neg y_1) \vee (x_2 \wedge \neg y_2))$$

Sous-formule **cohérence**

$$\bigwedge_{i,j} \bigvee_{\gamma} \left(c_{\gamma,i,j} \wedge \bigwedge_{\gamma' \neq \gamma} \neg c_{\gamma',i,j} \right)$$

\wedge

$$\bigwedge_j \bigvee_i \left(p_{i,j} \wedge \bigwedge_{i' \neq i} \neg p_{i',j} \right)$$

\wedge

$$\bigwedge_j \bigvee_q \left(e_{q,j} \wedge \bigwedge_{q' \neq q} \neg e_{q',j} \right)$$

Sous-formule **cohérence**

$$\bigwedge_{i,j} \bigvee_{\gamma} \left(c_{\gamma,i,j} \wedge \bigwedge_{\gamma' \neq \gamma} \neg c_{\gamma',i,j} \right)$$

à tout moment chaque case
contient exactement un symbole



\wedge

$$\bigwedge_j \bigvee_i \left(p_{i,j} \wedge \bigwedge_{i' \neq i} \neg p_{i',j} \right)$$

\wedge

$$\bigwedge_j \bigvee_q \left(e_{q,j} \wedge \bigwedge_{q' \neq q} \neg e_{q',j} \right)$$

rappel : i est une position, j une étape, γ un symbole

Sous-formule **cohérence**

$$\bigwedge_{i,j} \bigvee_{\gamma} \left(c_{\gamma,i,j} \wedge \bigwedge_{\gamma' \neq \gamma} \neg c_{\gamma',i,j} \right)$$

à tout moment chaque case
contient exactement un symbole

\wedge

$$\bigwedge_j \bigvee_i \left(p_{i,j} \wedge \bigwedge_{i' \neq i} \neg p_{i',j} \right)$$

à tout moment la tête
a exactement une position

\wedge

$$\bigwedge_j \bigvee_q \left(e_{q,j} \wedge \bigwedge_{q' \neq q} \neg e_{q',j} \right)$$

rappel : i est une position, j une étape, γ un symbole

Sous-formule **cohérence**

$$\bigwedge_{i,j} \bigvee_{\gamma} \left(c_{\gamma,i,j} \wedge \bigwedge_{\gamma' \neq \gamma} \neg c_{\gamma',i,j} \right)$$

à tout moment chaque case
contient exactement un symbole

\wedge

$$\bigwedge_j \bigvee_i \left(p_{i,j} \wedge \bigwedge_{i' \neq i} \neg p_{i',j} \right)$$

à tout moment la tête
a exactement une position

\wedge

$$\bigwedge_j \bigvee_q \left(e_{q,j} \wedge \bigwedge_{q' \neq q} \neg e_{q',j} \right)$$

à tout moment on est
dans exactement un état

rappel : i est une position, j une étape, γ un symbole

Sous-formule début x

 $e_{q_0,0}$ \wedge $\left(\bigwedge_{i < 0 \vee i \geq n} c_{B,i,0} \right) \wedge \left(\bigwedge_{0 \leq i < n} c_{x_i,i,0} \right)$ \wedge $p_{0,0}$

Sous-formule **début**_x

$e_{q_0,0}$



l'état de départ
est l'état initial q_0

\wedge

$$\left(\bigwedge_{i < 0 \vee i \geq n} c_{B,i,0} \right) \wedge \left(\bigwedge_{0 \leq i < n} c_{x_i,i,0} \right)$$

\wedge

$p_{0,0}$

rappel : i est une position, j une étape, γ un symbole

Sous-formule **début**_{*x*}

$e_{q_0,0}$

l'état de départ
est l'état initial q_0

\wedge

$$\left(\bigwedge_{i < 0 \vee i \geq n} c_{B,i,0} \right) \wedge \left(\bigwedge_{0 \leq i < n} c_{x_i,i,0} \right)$$

le ruban contient x entre
les positions 0 et $n - 1$ et B ailleurs

\wedge

$p_{0,0}$

rappel : i est une position, j une étape, γ un symbole

Sous-formule **début**_{*x*}

$e_{q_0,0}$

l'état de départ
est l'état initial q_0

\wedge

$$\left(\bigwedge_{i < 0 \vee i \geq n} c_{B,i,0} \right) \wedge \left(\bigwedge_{0 \leq i < n} c_{x_i,i,0} \right)$$

le ruban contient x entre
les positions 0 et $n - 1$ et B ailleurs

\wedge

$p_{0,0}$

la tête de lecture
est en position 0 au temps 0

rappel : i est une position, j une étape, γ un symbole

Sous-formule **accepte**

- Pour alléger les notations qui suivent et par abus de notation on pose

$$\delta(q_{oui}, \gamma) = \{(q_{oui}, \gamma, 0)\}$$

$$\delta(q_{no}, \gamma) = \{(q_{no}, \gamma, 0)\}$$

- C'est-à-dire, **quand on accepte ou rejette**, les configurations suivantes **restent identiques**
- Du coup on a tout simplement **accepte** = $e_{q_{oui}, t}$
(au temps t on est dans l'état acceptant q_{oui})

On est où ? 

cohérence \wedge **début**_{*x*} \wedge **accepte**

On est où ?

deux symboles ne sont pas assignés
à la même case, deux positions
à la tête, deux états à la même étape


cohérence \wedge **début**_{*x*} \wedge **accepte**

On est où ?

deux symboles ne sont pas assignés
à la même case, deux positions
à la tête, deux états à la même étape

cohérence \wedge **début**_{*x*} \wedge **accepte**

la configuration initiale
est la bonne

On est où ?

deux symboles ne sont pas assignés
à la même case, deux positions
à la tête, deux états à la même étape

cohérence \wedge **début**_{*x*} \wedge **accepte**

la configuration initiale
est la bonne

on arrive dans un état
acceptant à un temps $\leq t$

**Il reste le cœur de la simulation :
spécifier que le comportement
de la machine **correspond**
à la relation de **transition****

Sous-formule **transition**_{*j*}

$$\psi_{\text{contenu}} = \bigwedge_i \left(\neg p_{i,j-1} \rightarrow \bigwedge_{\gamma} (c_{\gamma,i,j} \leftrightarrow c_{\gamma,i,j-1}) \right)$$

Sous-formule **transition**_{*j*}

$$\psi_{\text{contenu}} = \bigwedge_i \left(\neg p_{i,j-1} \rightarrow \bigwedge_{\gamma} (c_{\gamma,i,j} \leftrightarrow c_{\gamma,i,j-1}) \right)$$

si la tête n'est pas sur
la case i à l'étape $j - 1 \dots$



Sous-formule **transition**_{*j*}

$$\psi_{\text{contenu}} = \bigwedge_i \left(\neg p_{i,j-1} \rightarrow \bigwedge_{\gamma} \left(c_{\gamma,i,j} \leftrightarrow c_{\gamma,i,j-1} \right) \right)$$

si la tête n'est pas sur
la case *i* à l'étape *j* - 1...

...alors le symbole sur cette case
ne change pas à l'étape *j*

Sous-formule **transition**_{*j*}

$$\begin{aligned} \psi^{\text{trans}} &= \bigwedge_{q,i,\gamma} \left((e_{q,j-1} \wedge p_{i,j-1} \wedge c_{\gamma,i,j-1}) \right. \\ &\quad \left. \rightarrow \bigvee_{(q',\gamma',d') \in \delta(q,\gamma)} (e_{q',j} \wedge c_{\gamma',i,j} \wedge p_{i+d',j}) \right) \end{aligned}$$

rappel : i est une position, j une étape, γ un symbole, q un état, $d' \in \{-1, 0, +1\}$

Sous-formule **transition**_{*j*}

si la machine est dans l'état q
à l'étape $j - 1 \dots$

$$\psi^{\text{trans}} = \bigwedge_{q,i,\gamma} \left(\left(e_{q,j-1} \wedge p_{i,j-1} \wedge c_{\gamma,i,j-1} \right) \right. \\ \left. \rightarrow \bigvee_{(q',\gamma',d') \in \delta(q,\gamma)} \left(e_{q',j} \wedge c_{\gamma',i,j} \wedge p_{i+d',j} \right) \right)$$

rappel : i est une position, j une étape, γ un symbole, q un état, $d' \in \{-1, 0, +1\}$

Sous-formule **transition**_{*j*}

si la machine est dans l'état q
à l'étape $j - 1$...

...est que sa tête est sur
la case i et lit γ ...

$$\psi^{\text{trans}} = \bigwedge_{q,i,\gamma} \left(\left(e_{q,j-1} \wedge p_{i,j-1} \wedge c_{\gamma,i,j-1} \right) \rightarrow \bigvee_{(q',\gamma',d') \in \delta(q,\gamma)} \left(e_{q',j} \wedge c_{\gamma',i,j} \wedge p_{i+d',j} \right) \right)$$

rappel : i est une position, j une étape, γ un symbole, q un état, $d' \in \{-1, 0, +1\}$

Sous-formule **transition**_{*j*}

si la machine est dans l'état q
à l'étape $j - 1$...

...est que sa tête est sur
la case i et lit γ ...

$$\psi^{\text{trans}} = \bigwedge_{q,i,\gamma} \left((e_{q,j-1} \wedge p_{i,j-1} \wedge c_{\gamma,i,j-1}) \right)$$

$$\rightarrow \bigvee_{(q',\gamma',d') \in \delta(q,\gamma)} \left(e_{q',j} \wedge c_{\gamma',i,j} \wedge p_{i+d',j} \right)$$

...alors la machine fait l'une des transitions
décrites par sa relation δ à l'étape j

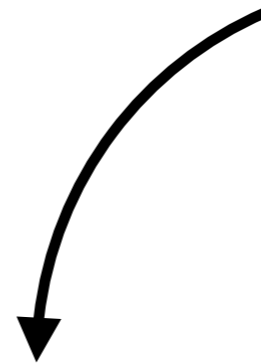
rappel : i est une position, j une étape, γ un symbole, q un état, $d' \in \{-1, 0, +1\}$

Sous-formule **transition**_{*j*}

$$\mathbf{transition}_j = \psi_{\mathbf{contenu}} \wedge \psi_{\mathbf{trans}}$$

Sous-formule **transition**_j

les cases qui ne sont pas sous
la tête ne changent pas



$$\text{transition}_j = \psi_{\text{contenu}} \wedge \psi_{\text{trans}}$$

Sous-formule **transition**_{*j*}

les cases qui ne sont pas sous
la tête ne changent pas

$$\mathbf{transition}_j = \psi_{\text{contenu}} \wedge \psi_{\text{trans}}$$

celle qui l'est change selon
la relation de transition δ

Le pire est passé !



Enfin, voilà la formule φ_x

cohérence \wedge **début** _{x} \wedge $\bigwedge_{1 \leq j \leq t}$ **transition** _{j} \wedge **accepte**

Enfin, voilà la formule φ_x

deux valeurs ne sont pas assignés
à la même case, deux positions
à la même tête, deux états à la même étape

$$\text{cohérence} \wedge \text{début}_x \wedge \bigwedge_{1 \leq j \leq t} \text{transition}_j \wedge \text{accepte}$$

la configuration initiale
est la bonne

on fait une bonne
transition à chaque étape

on arrive dans un état
acceptant à un temps $\leq t$

Enfin, voilà la formule φ_x

$$\bigwedge_{i,j} \bigvee_{\gamma} \left(c_{\gamma,i,j} \wedge \bigwedge_{\gamma' \neq \gamma} \neg c_{\gamma',i,j} \right) \wedge \bigwedge_j \bigvee_i \left(p_{i,j} \wedge \bigwedge_{i' \neq i} \neg p_{i',j} \right) \wedge \bigwedge_j \bigvee_q \left(e_{q,j} \wedge \bigwedge_{q' \neq q} \neg e_{q',j} \right)$$

^

$$e_{q_0,0} \wedge \left(\bigwedge_{i < 0 \vee i \geq n} c_{B,i,0} \right) \wedge \left(\bigwedge_{0 \leq i < n} c_{x_i,i,0} \right) \wedge p_{1,0}$$

^

$$= \bigwedge_{q,i,\gamma} \left(\left(e_{q,j-1} \wedge p_{i_r,j-1} \wedge c_{\gamma_r,i_r,j-1} \right) \rightarrow \bigvee_{(q',\gamma',d') \in \delta(q,\vec{\gamma})} \left(e_{q',j} \wedge c_{\gamma',i_r,j} \wedge p_{i_r+d'_r,j} \right) \right)$$

^

$$e_{q_{oui},t}$$

Enfin, voilà la formule φ_x

$$\bigwedge_{i,j} \bigvee_{\gamma} \left(c_{\gamma,i,j} \wedge \bigwedge_{\gamma' \neq \gamma} \neg c_{\gamma',i,j} \right) \wedge \bigwedge_j \bigvee_i \left(p_{i,j} \wedge \bigwedge_{i' \neq i} \neg p_{i',j} \right) \wedge \bigwedge_j \bigvee_q \left(e_{q,j} \wedge \bigwedge_{q' \neq q} \neg e_{q',j} \right)$$

\wedge

$$e_{q_0,0} \wedge \left(\bigwedge_{i < 0 \vee i \geq n} c_{B,i,0} \right) \wedge \left(\bigwedge_{0 \leq i < n} c_{x_i,i,0} \right) \wedge p_{1,0}$$

\wedge

$$= \bigwedge_{q,i,\gamma} \left(\left(e_{q,j-1} \wedge p_{i_r,j-1} \wedge c_{\gamma_r,i_r,j-1} \right) \rightarrow \bigvee_{(q',\gamma',d') \in \delta(q,\vec{\gamma})} \left(e_{q',j} \wedge c_{\gamma',i_r,j} \wedge p_{i_r+d'_r,j} \right) \right)$$

\wedge

$e_{q_{oui},t}$

**$|\varphi_x| = \text{polynomial}$
par rapport à $n = |x|$**

φ_x est satisfaisable
ssi N accepte x !

Sous-formule **cohérence**

$$\bigwedge_{i,j} \bigvee_{\gamma} \left(c_{\gamma,i,j} \wedge \bigwedge_{\gamma' \neq \gamma} \neg c_{\gamma',i,j} \right)$$

à tout moment chaque case
contient exactement un symbole

\wedge

$$\bigwedge_j \bigvee_i \left(p_{i,j} \wedge \bigwedge_{i' \neq i} \neg p_{i',j} \right)$$

à tout moment la tête
a exactement une position

\wedge

$$\bigwedge_j \bigvee_q \left(e_{q,j} \wedge \bigwedge_{q' \neq q} \neg e_{q',j} \right)$$

à tout moment on est
dans exactement un état

rappel : i est une position, j une étape, γ un symbole

Sous-formule **début**_{*x*}

$e_{q_0,0}$

l'état de départ
est l'état initial q_0

\wedge

$$\left(\bigwedge_{i < 0 \vee i \geq n} c_{B,i,0} \right) \wedge \left(\bigwedge_{0 \leq i < n} c_{x_i,i,0} \right)$$

le ruban contient x entre
les positions 1 et n et B ailleurs

\wedge

$p_{1,0}$

la tête de lecture
est en position 1 au temps 0

rappel : i est une position, j une étape, γ un symbole

Sous-formule **transition**_{*j*}

$$\psi_{\text{contenu}} = \bigwedge_{r,i} \left(\neg p_{i,j-1}^r \rightarrow \bigwedge_{\gamma} \left(c_{\gamma,i,j}^r \leftrightarrow c_{\gamma,i,j-1}^r \right) \right)$$

si la tête n'est pas sur
la case i à l'étape $j - 1$...

...alors le symbole sur cette case
ne change pas à l'étape j

Sous-formule **transition**_{*j*}

si la machine est dans l'état q
à l'étape $j - 1$...

...est que sa tête est sur
la case i et lit γ ...

$$\psi^{\text{trans}} = \bigwedge_{q,i,\gamma} \left((e_{q,j-1} \wedge p_{i,j-1} \wedge c_{\gamma,i,j-1}) \right)$$

$$\rightarrow \bigvee_{(q',\gamma',d') \in \delta(q,\vec{\gamma})} \left(e_{q',j} \wedge c_{\gamma',i,j} \wedge p_{i+d',j} \right)$$

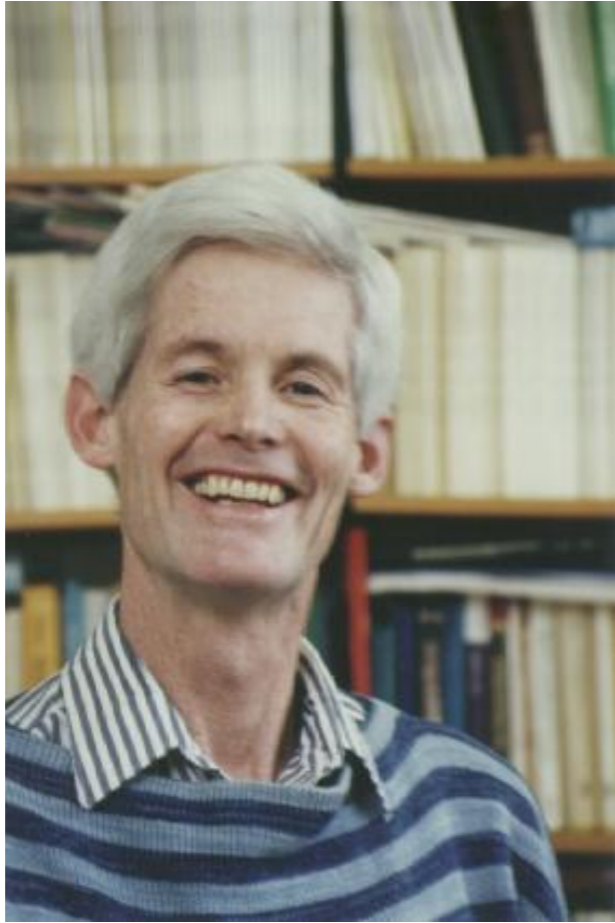
...alors la machine fait l'une des transitions
décrites par sa relation δ à l'étape j

rappel : i est une position, j une étape, γ un symbole, q un état, $d' \in \{-1, 0, +1\}$

Conclusion de la démonstration

- On a pris $B \in \mathbf{NP}$ et une machine non déterministe N qui le reconnaît en temps polynomial $p(n)$
- Pour chaque entrée x de B on construit une formule φ_x de taille polynomiale qui décrit le calcul de $N(x)$
- Cette construction on peut la faire en temps polynomial, parce que la formule φ_x ne sera peut-être pas jolie, mais elle est régulière
- En plus on a $x \in B$ ssi $\varphi_x \in \text{SAT}$
- Donc $B \leq \text{SAT}$, et comme B était un langage quelconque dans \mathbf{NP} , on obtient la \mathbf{NP} -complétude de SAT





Stephen Cook



Леонід Лєвін



SAT est NP-complete