- $H=\begin{bmatrix}0 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & 0 & 1\end{bmatrix}$
- H matrice kxn

Cover x=(x1,….xn)

Stego y=(y1,…,yn)

Mess m=(m1…mk)

Trouver y tels que
* Hy =m
* distance de Hamming (x,y) est la plus faible possible (dans le corps F^2)

=> Hy=m il y a 2^{n-k} y possibles
(projection, de y sur l'espace engendré par H de dimension k)

=> Pour trouver y qui est le plus proche de x on construit un treillis

- H=$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$

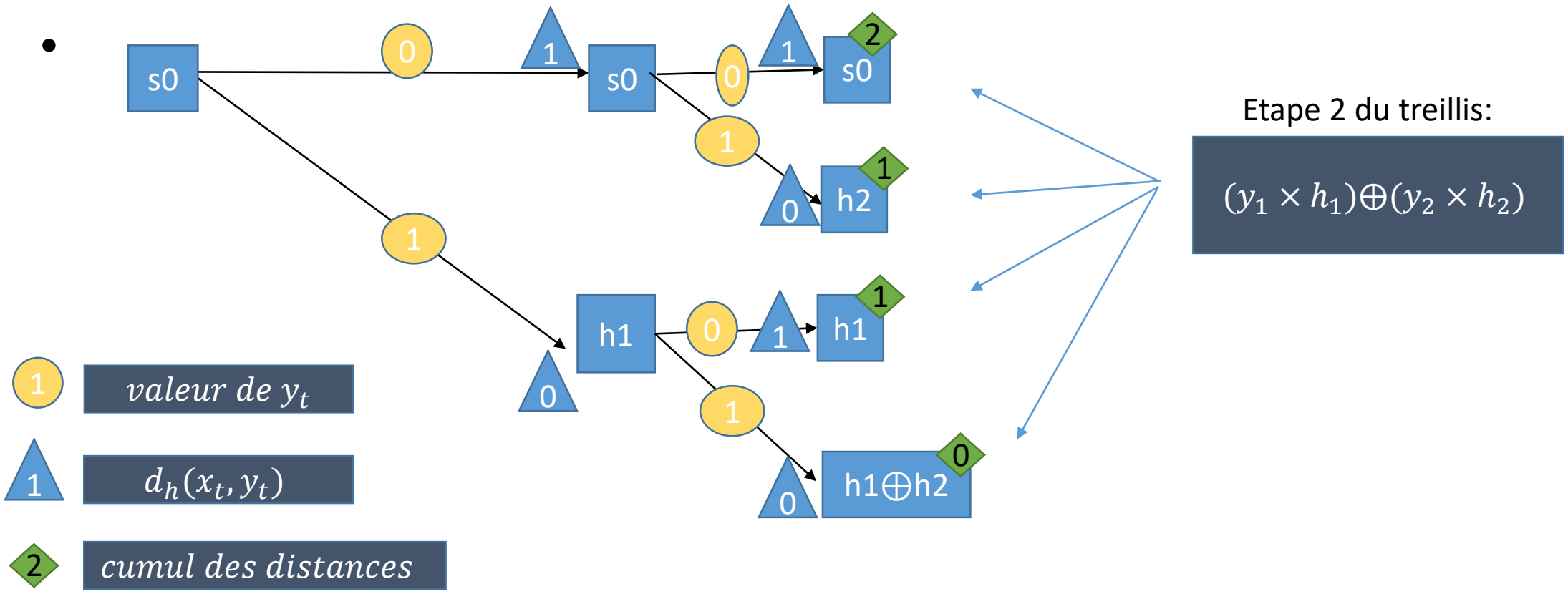
$x = (1\ 1\ 0\ 0)$

$m = (1\ 1\ 1)$

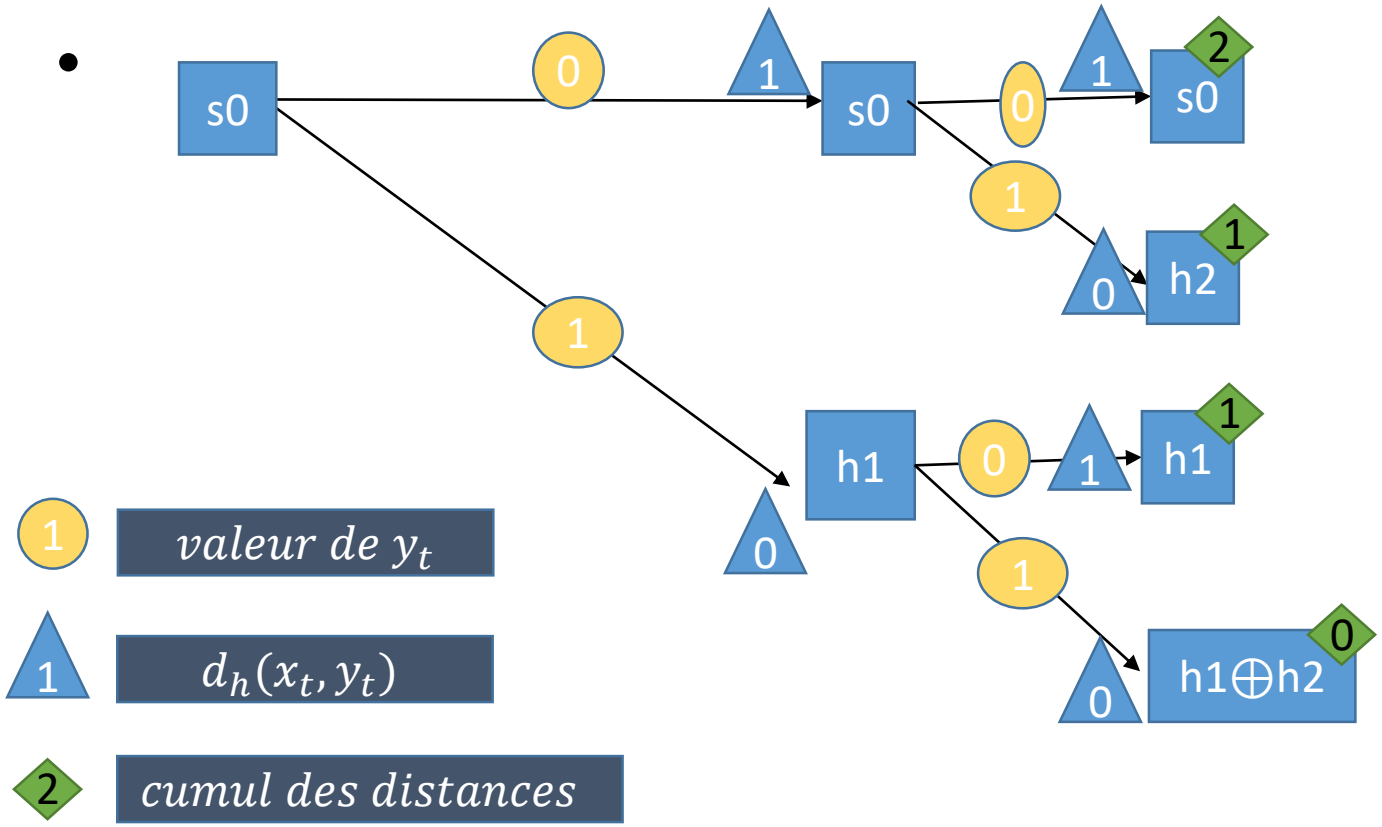
- Une modification naïve conduirait à $d_h(\mathrm{x}, \mathrm{y}) = 3$

- H=$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$ => H=[h1 h2 h3 h4] ; x = (1 1 0 0)
- $s0 = \begin{matrix} 0 \\ 0 \\ 0 \end{matrix}$
- si y1=0 → $\begin{matrix} 0 \\ 0 \\ 0 \end{matrix}$ s1= s0⊕(y1 × h1) $d_h(y_1, x_1) = 1$
- si y1=1 → $\begin{matrix} 0 \\ 0 \\ 1 \end{matrix}$ s1= s0⊕(y1 × h1) $d_h(y_1, x_1) = 0$

- x = (1 1 0 0) H=[h1 h2 h3 h4]
-

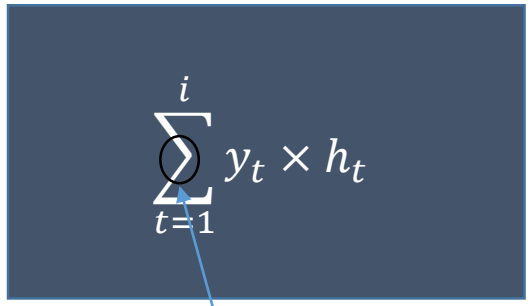


- x = (1 1 0 0) H=[h1 h2 h3 h4]
-

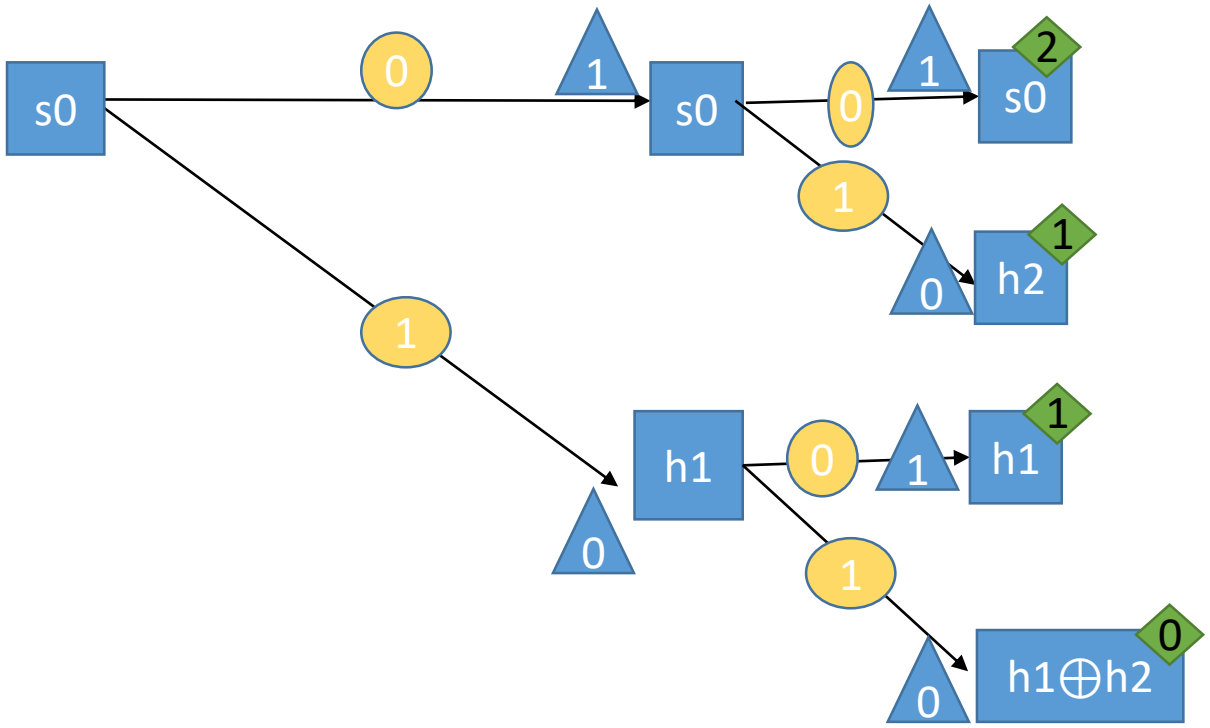


...

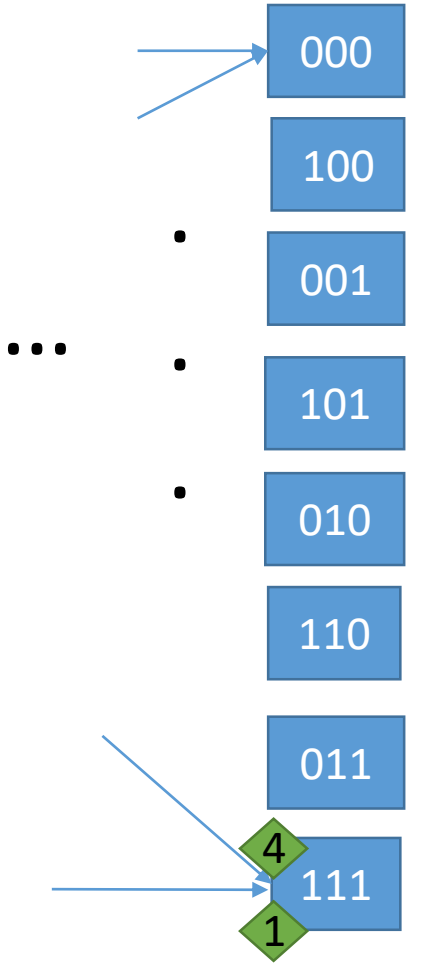
Etape *i* du treillis:



- x = (1 1 0 0) H=[h1 h2 h3 h4]



Etape *n* du treillis:

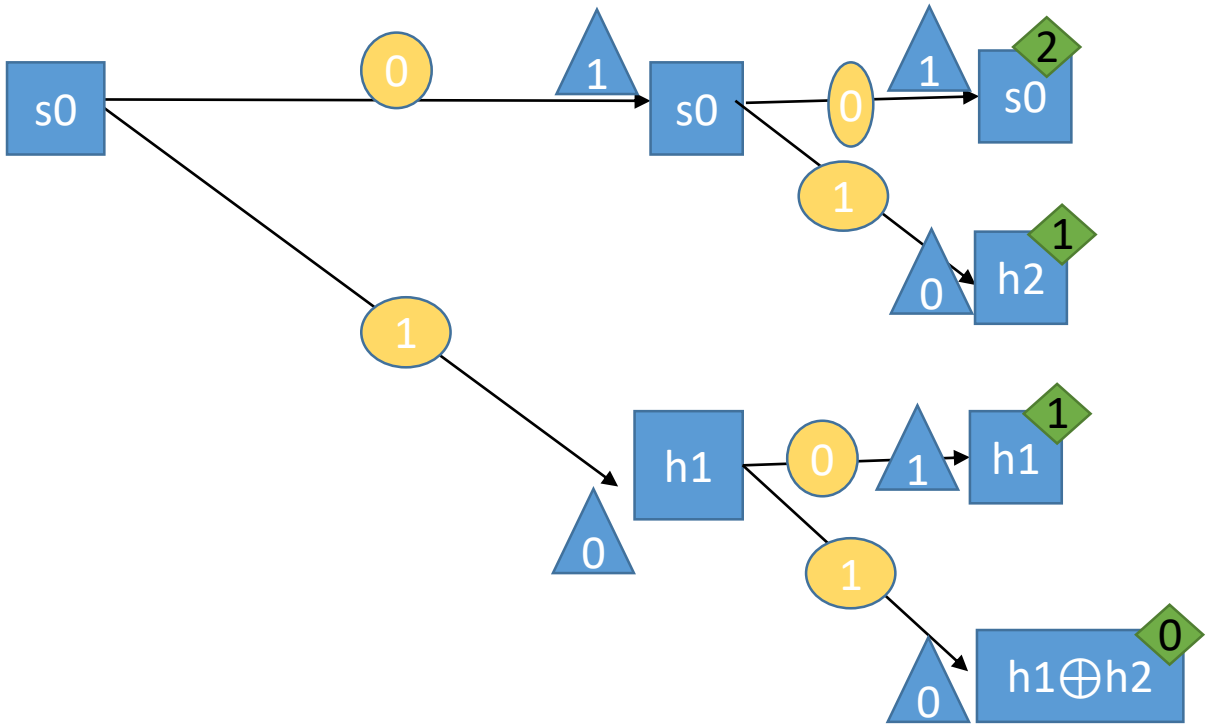


$Hy=\sum_{t=1}^{n} y_t \times h_t$

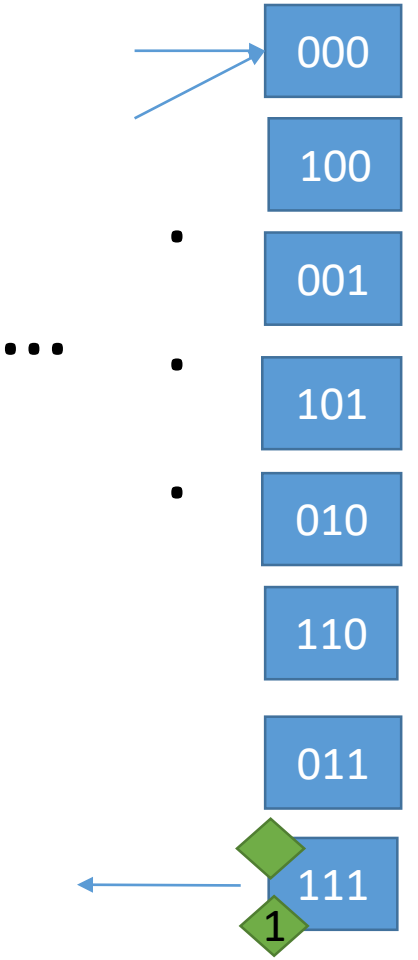
Hy=m=(111)

On remonte le treillis à partir de ce chemin , ce y offrant la plus petite distance avec x

- x = (1 1 0 0) H=[h1 h2 h3 h4]



Etape *n* du treillis:



$Hy=\sum_{t=1}^{n} y_t \times h_t$

Hy=m=(111)

On remonte le treillis à partir de ce chemin , ce y offrant la plus petite distance avec x

$\tilde{h}=\begin{bmatrix}0 & 1 & 1\\ 1 & 0 & 1\end{bmatrix}$ pour n=6 w=3

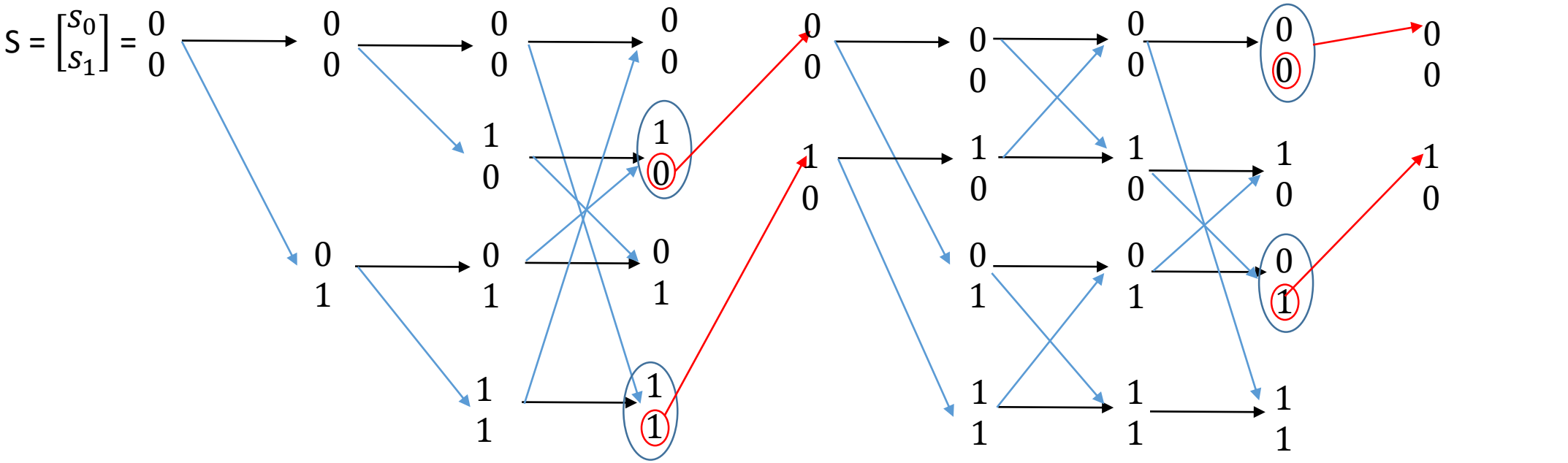
$$H=\begin{bmatrix}0 & 1 & 1 & & & \\ 1 & 0 & 1 & 0 & 1 & 1\\ & & & 1 & 0 & 1\end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

m=1 => On garde les états tel que s_0 =m=1

$S = \begin{bmatrix} s_0 \\ s_1 \end{bmatrix}$

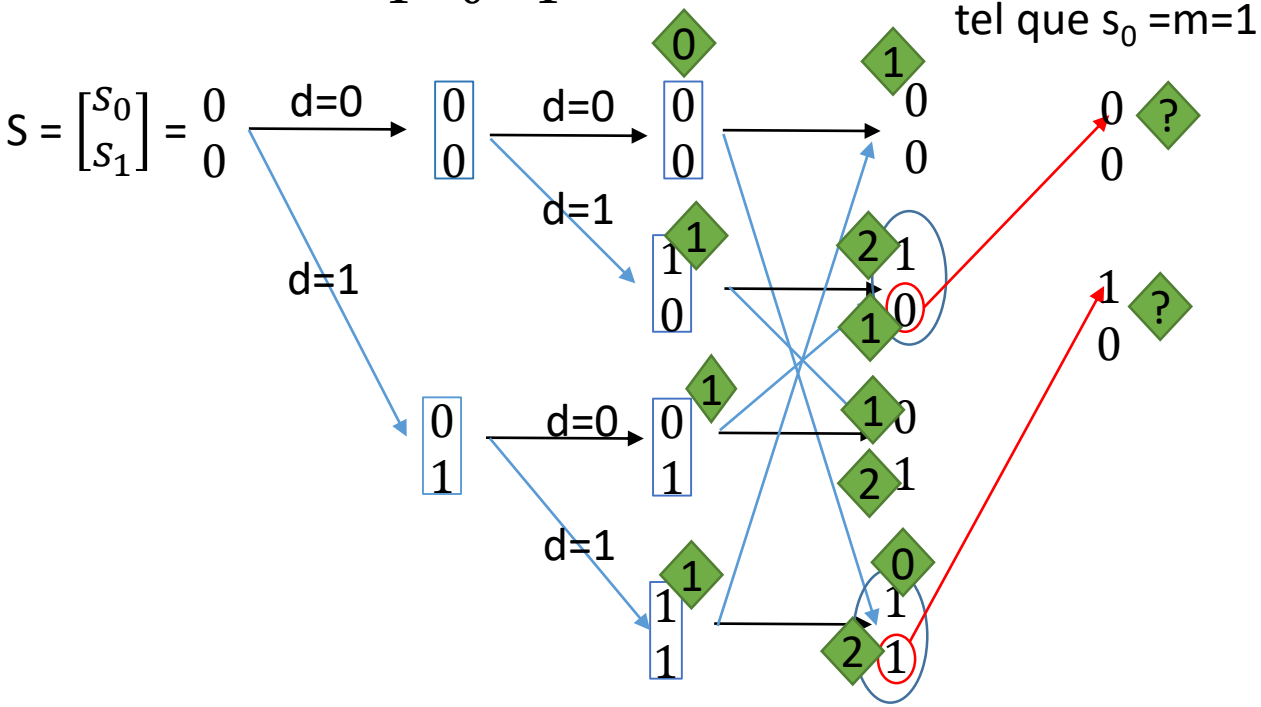
m=0 => On garde les états tel que s_0 =m=0



X = 0 0 1 1 0 1

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

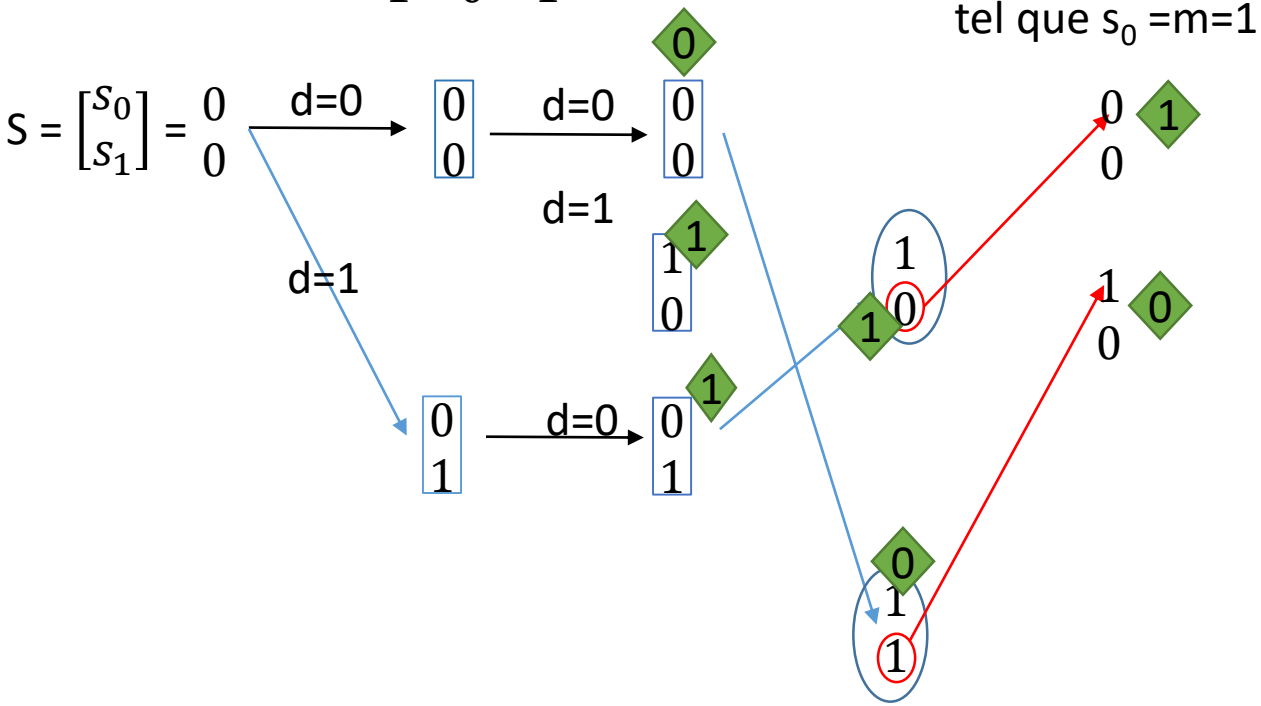
m=1 => On garde les états tel que s_0 =m=1



X = 0 0 1 1 0 1

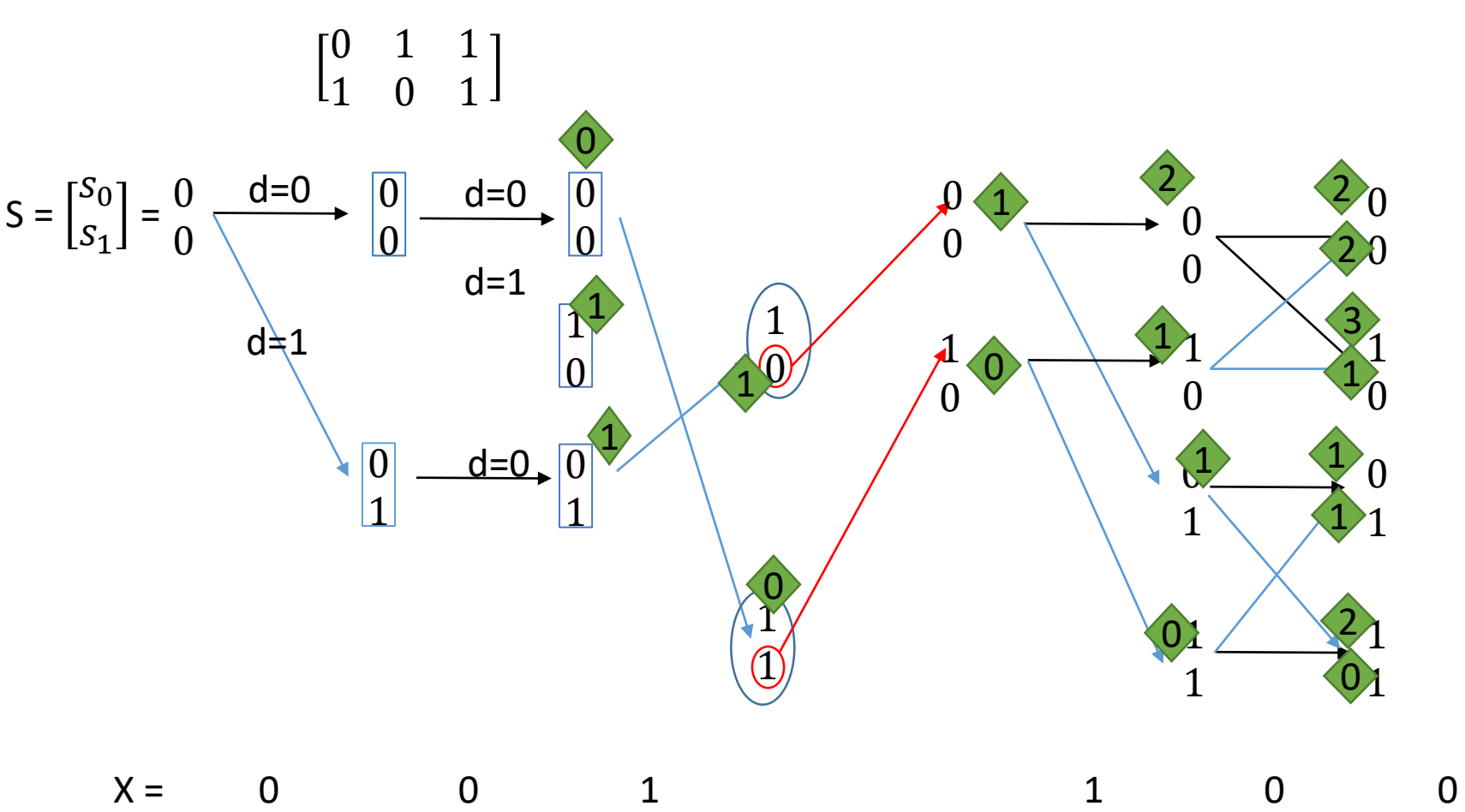
$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

m=1 => On garde les états tel que s_0 =m=1



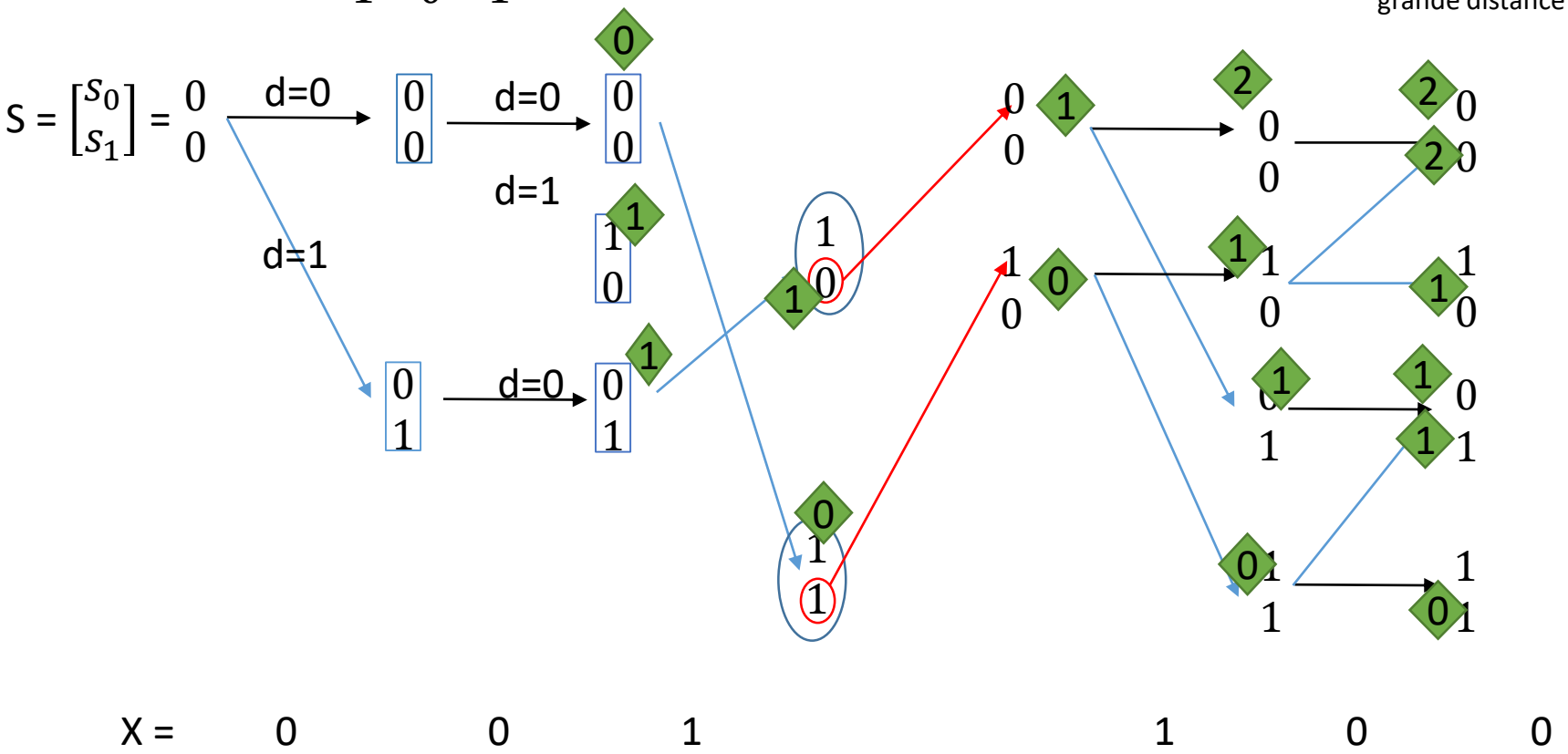
X = 0 0 1 1 0 1

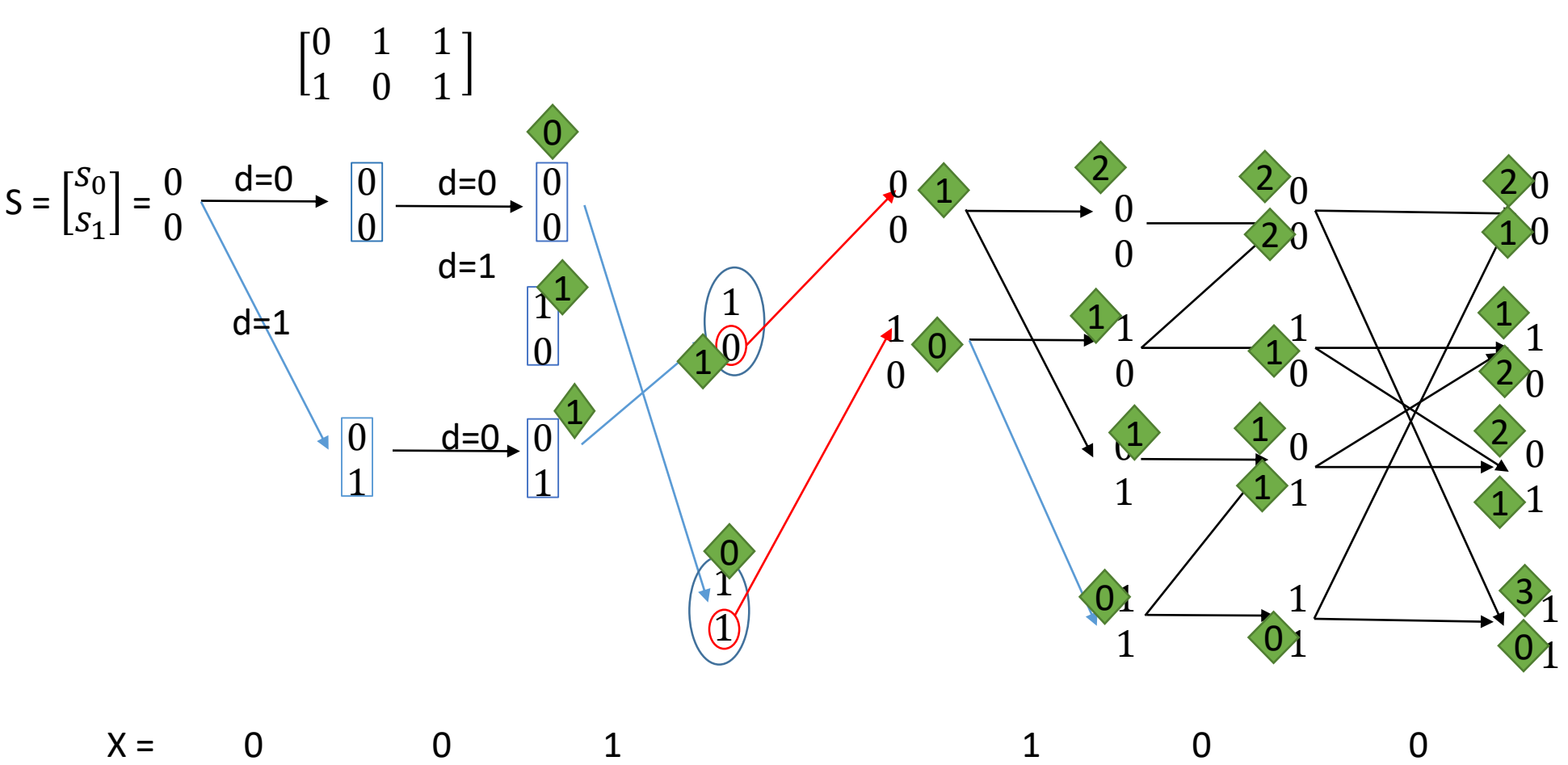
Y = 0 ou 1 0 1

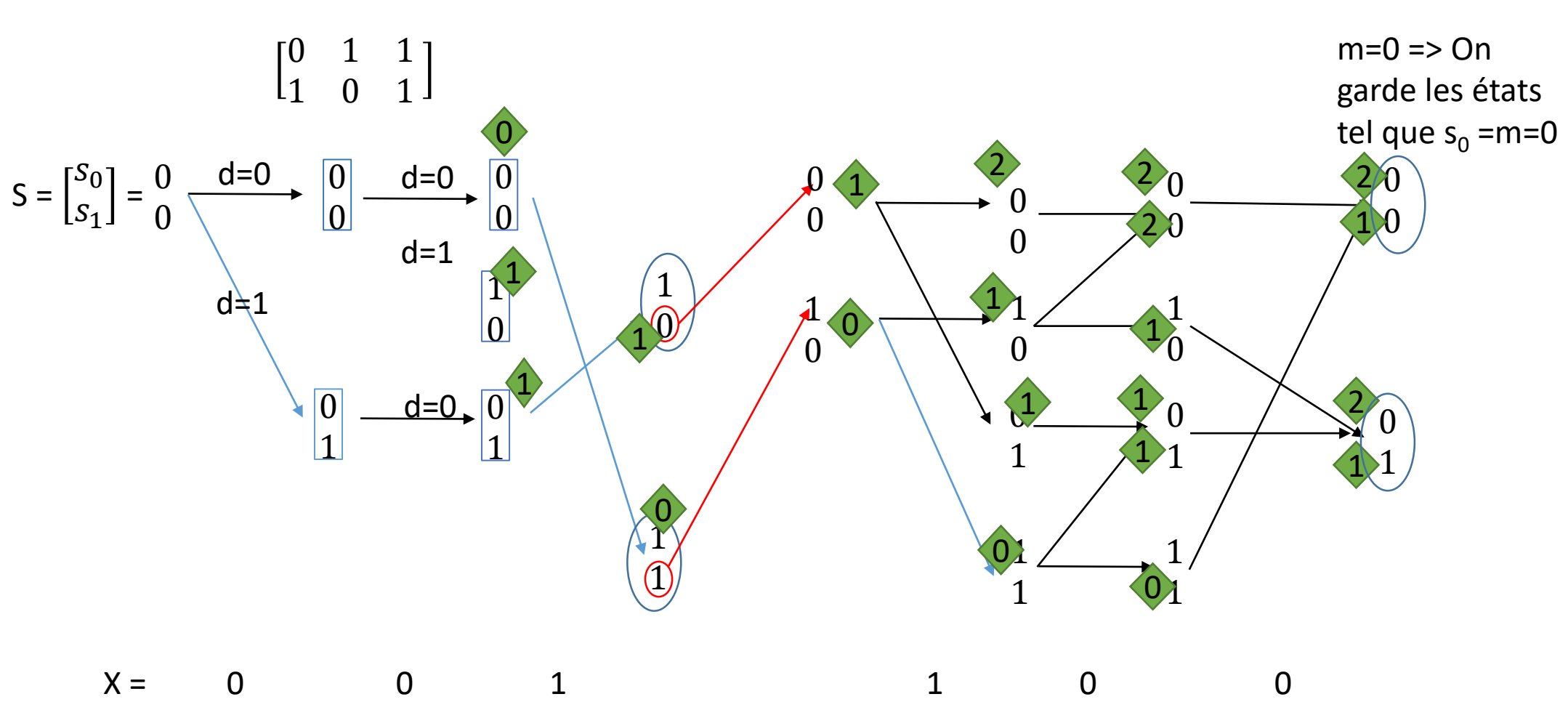

$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$
S = $\begin{bmatrix} S_0 \\ S_1 \end{bmatrix}$ = 0 0
d=0
d=1
d=0
d=1
d=0
X = 0 0 1 1 0 0

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Rejet des chemins convergent vers un même état et présentant une plus grande distance de Hamming

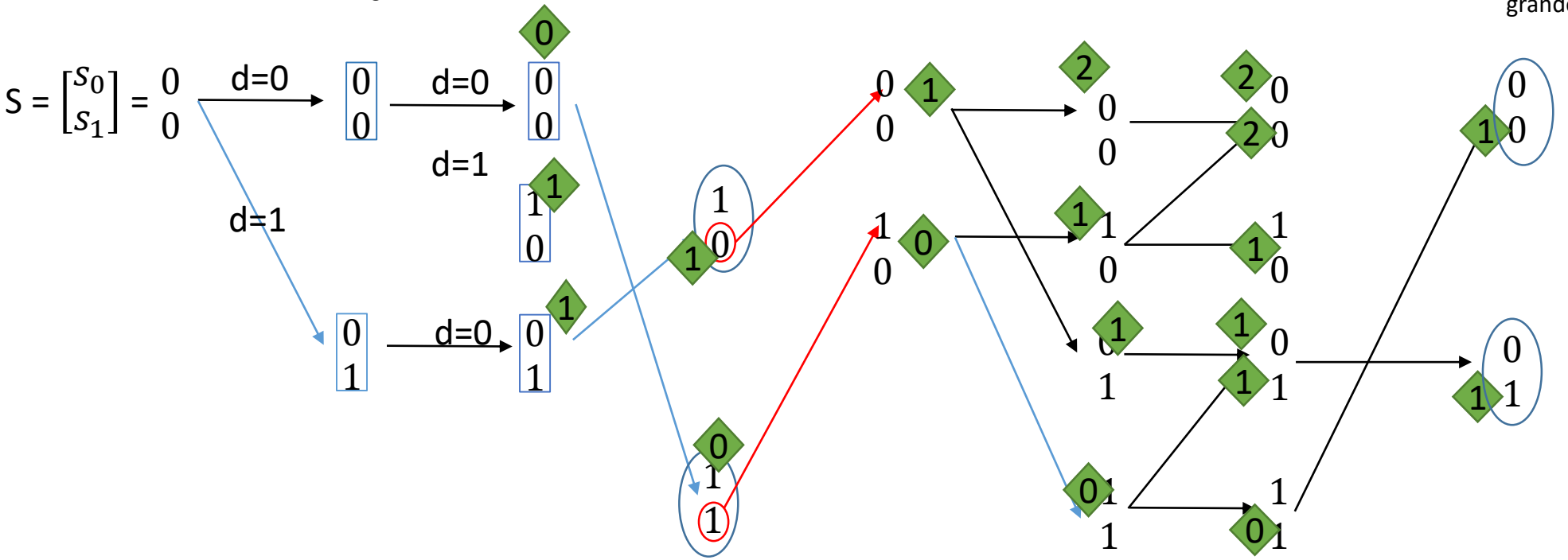



$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$
S = $\begin{bmatrix} S_0 \\ S_1 \end{bmatrix}$ = 0 0
d=0
d=1
d=0
d=1
d=0
X = 0 0 1 1 0 0


$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$
m=0 => On garde les états tel que s_0 =m=0
S = $\begin{bmatrix} s_0 \\ s_1 \end{bmatrix}$ = 0 0
d=0
d=1
d=0
d=1
d=0
X = 0 0 1 1 0 0

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

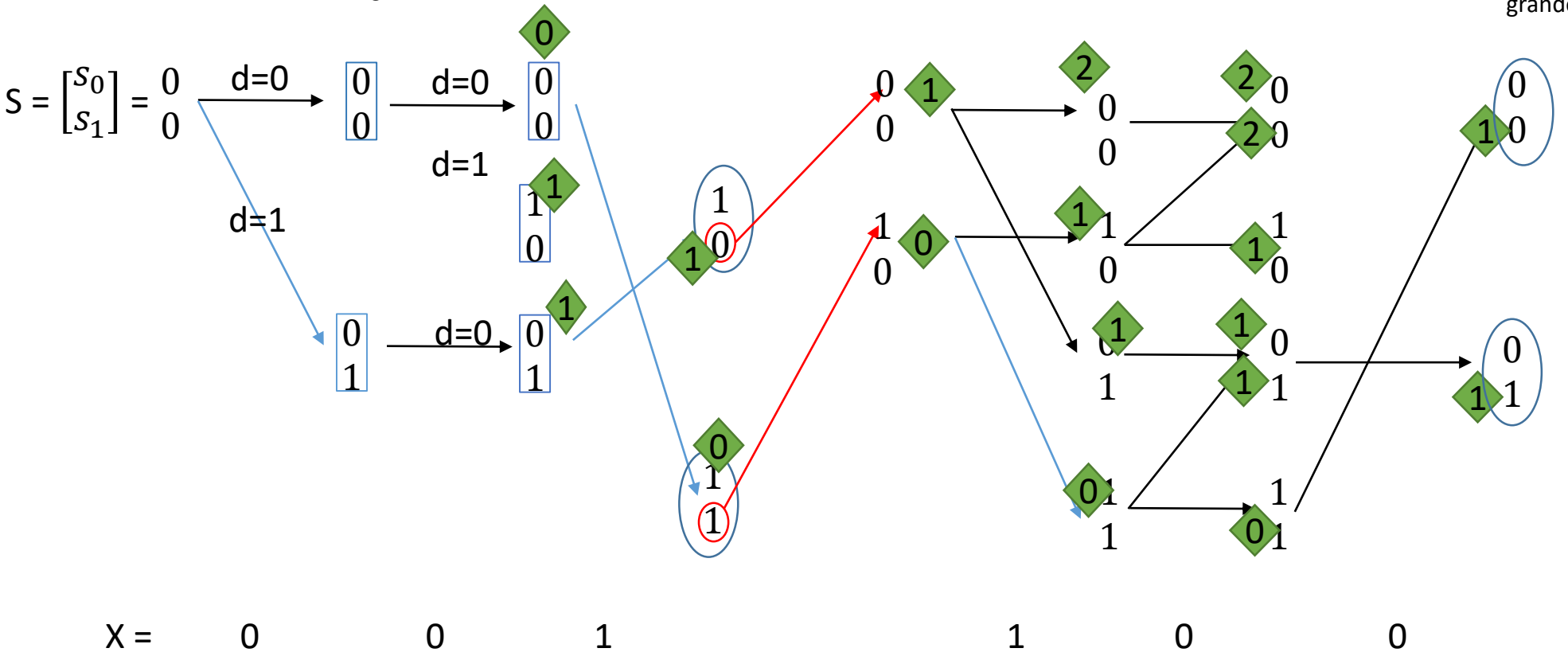
Rejet des chemins convergent vers un même état et présentant une plus grande distance de Hamming



X = 0 0 1 1 0 0

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

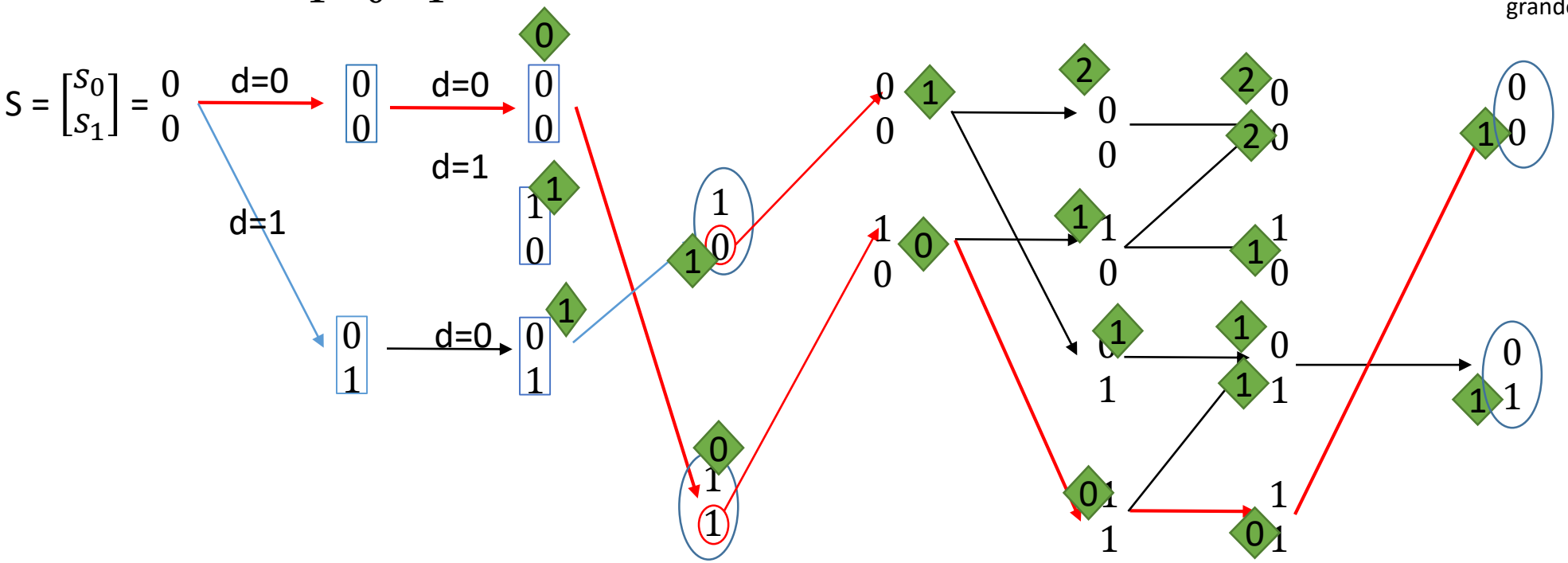
Rejet des chemins convergent vers un même état et présentant une plus grande distance de Hamming



Si m=[1 0] seulement on a deux choix pour Y:

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Rejet des chemins convergent vers un même état et présentant une plus grande distance de Hamming



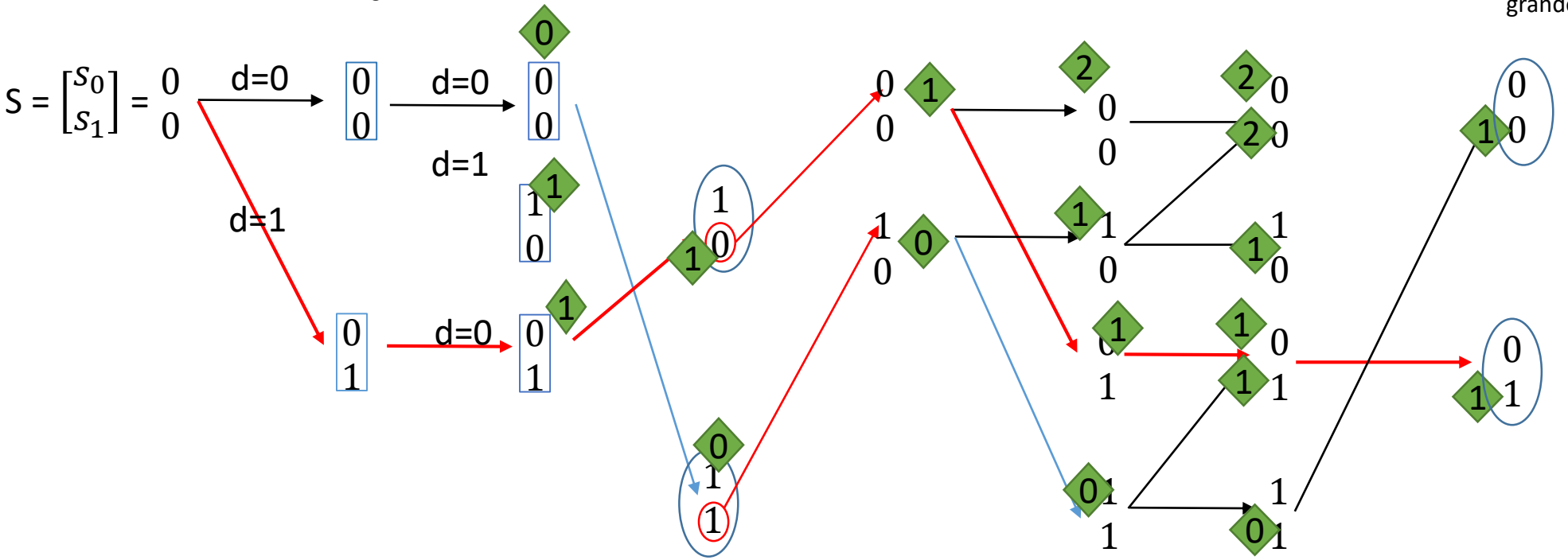
X = 0 0 1 1 0 0

Si m=[1 0] seulement on a deux choix pour Y avec distance de Hamming = 1

Y = 0 0 1 1 0 1

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Rejet des chemins convergent vers un même état et présentant une plus grande distance de Hamming



X = 0 0 1 1 0 0

Si m=[1 0] seulement on a deux choix pour Y avec distance de Hamming = 1

Y = 1 0 1 1 0 0