Cơ sở lí thuyết thông tin

Chương 5: Mã tích chập
Thuật toán giải mã Viterbi

TS. Phạm Hải Đăng

Phần 1: Khái niệm cơ bản

- Định nghĩa Mã tích chập
  - Mã tích chập là 1 dạng mã tuyến tính.
  - Mã tích chập có cấu trúc giống 1 bộ lọc số - phép tích chập.
  - Bộ mã hóa tích chập có thể coi như 1 tập hợp các bộ lọc số - hệ thống tuyến tính, bất biến theo thời gian.
  - Đầu vào của bộ mã hóa tích chập là một dòng dữ liệu (data stream) biểu diễn dạng vector $m(x)=\left[m^{(1)}(x) \quad m^{(2)}(x) \quad \ldots\right]$

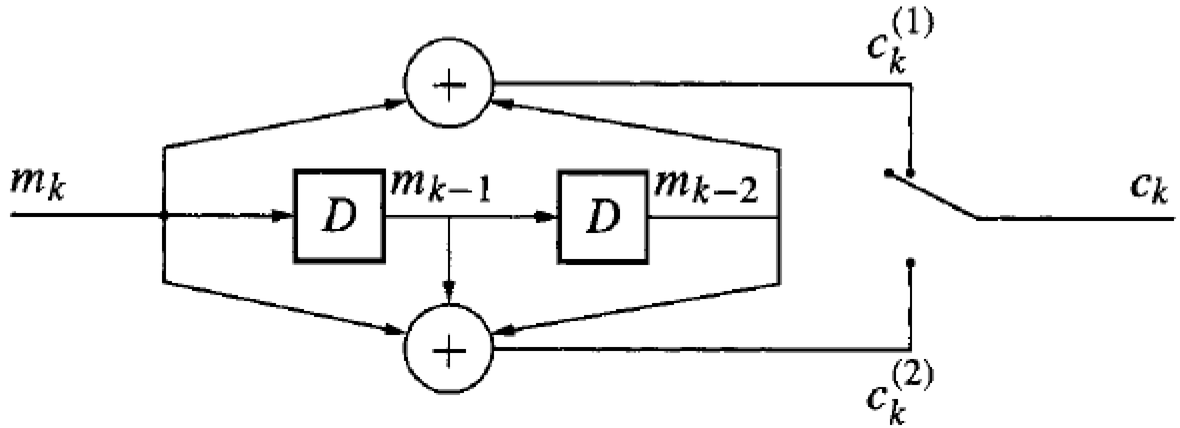
$$m^{(1)}(x)=m_0^{(1)}+m_1^{(1)}x+m_2^{(1)}x^2\ldots$$

$$m^{(2)}(x)=m_0^{(2)}+m_1^{(2)}x+m_2^{(2)}x^2\ldots$$

  - Tốc độ mã *R=k/n*
  - Chiều dài ràng buộc *K* (constraint length) là kích thước của thanh ghi (số lượng D-FF).

Phần 1: Khái niệm cơ bản

- Ví dụ: Mã tích chập có $R=1/2$



- Với đầu vào $\mathbf{m} = \{1, 1, 0, 0, 1, 0, 1\}$
- Đầu ra

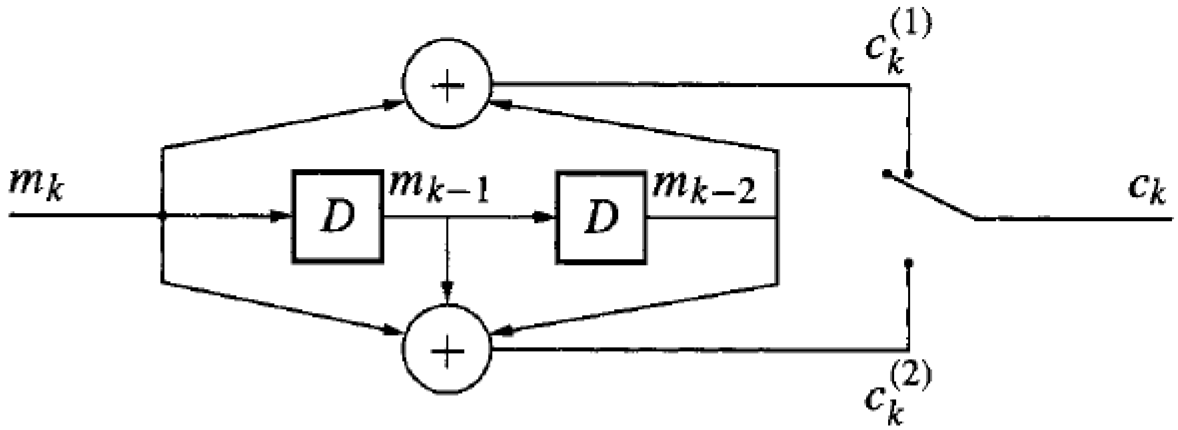
$$\mathbf{c}^{(1)} = \{1, 1, 1, 1, 1, 0, 0, 0, 1\}$$
$$\mathbf{c}^{(2)} = \{1, 0, 0, 1, 1, 1, 0, 1, 1\}$$

- Biểu diễn đầu ra dạng vector

$$\mathbf{c} = \{11, 10, 10, 11, 11, 01, 00, 01, 11\}$$

Phần 1: Khái niệm cơ bản

- Ví dụ: Mã tích chập có R=1/2



- Với đầu vào $\mathbf{m} = \{1, 1, 0, 0, 1, 0, 1\}$

Biểu diễn dạng đa thức $m(x) = 1 + x + x^4 + x^6$

- Đầu ra dạng đa thức

$$c^{(1)}(x) = m(x)g_1(x) = (1 + x + x^4 + x^6)(1 + x^2) = 1 + x + x^2 + x^3 + x^4 + x^8$$

$$c^{(2)}(x) = m(x)g_2(x) = (1 + x + x^4 + x^6)(1 + x + x^2) = 1 + x^3 + x^4 + x^5 + x^7 + x^8$$

Với đa thức sinh $g^{(1)}(x) = 1 + x^2$

$g^{(2)}(x) = 1 + x + x^2$

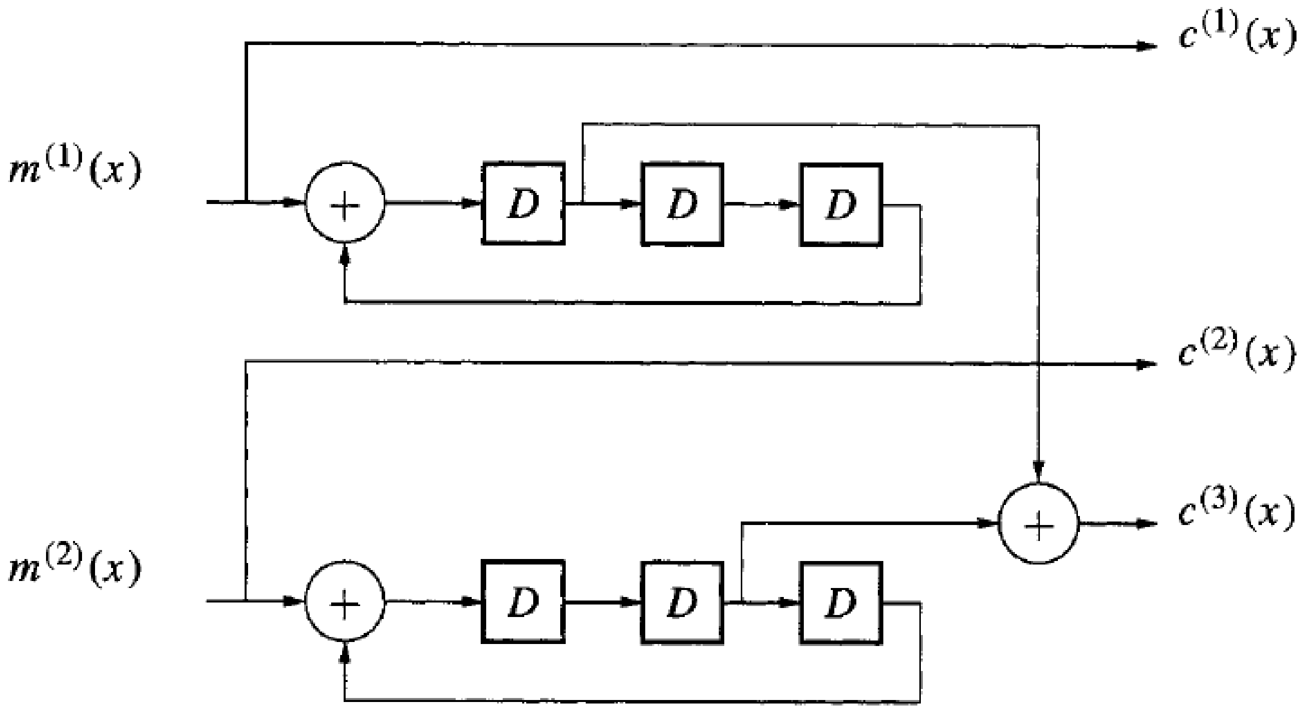
$$G_a(x) = [1 + x^2 \quad 1 + x + x^2]$$

Phần 1: Khái niệm cơ bản

- Ví dụ: Mã tích chập dạng hệ thống có ma trận đa thức sinh

$$G_1(x) = \begin{bmatrix} 1 & 0 & \frac{x}{1+x^3} \\ 0 & 1 & \frac{x^2}{1+x^3} \end{bmatrix}$$

Biểu diễn dạng sơ đồ mạch



Phần 1: Khái niệm cơ bản

- Biểu diễn dạng tổng quan của đa thức bản tin và ma trận đa thức sinh

$$\mathbf{m}(x) = [m^{(1)}(x), m^{(2)}(x), \ldots, m^{(k)}(x)]$$

$$G(x) = \begin{bmatrix} g^{(1,1)}(x) & g^{(1,2)}(x) & \cdots & g^{(1,n)}(x) \\ g^{(2,1)}(x) & g^{(2,2)}(x) & \cdots & g^{(2,n)}(x) \\ \vdots & & & \\ g^{(k,1)}(x) & g^{(k,2)}(x) & \cdots & g^{(k,n)}(x) \end{bmatrix}$$

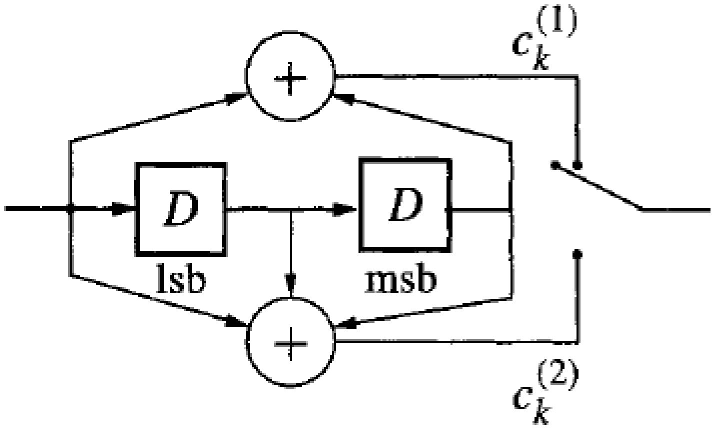
- Từ mã của mã tích chập

$$\mathbf{c}(x) = [c^{(1)}(x), c^{(2)}(x), \ldots, c^{(n)}(x)] = \mathbf{m}(x)G(x)$$

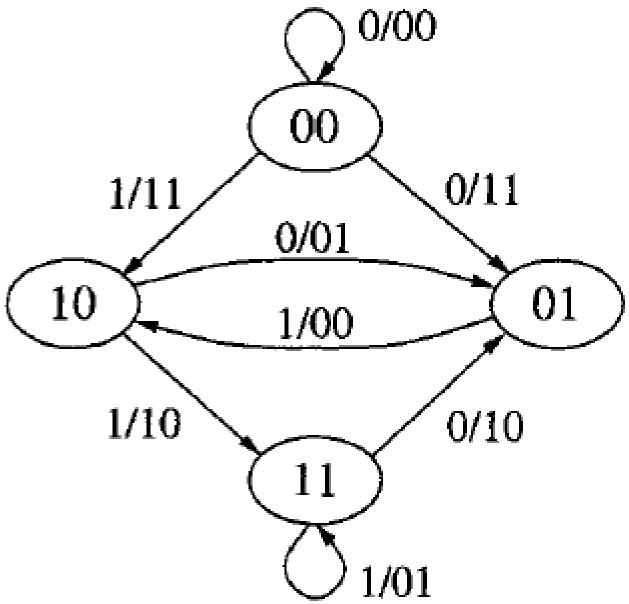
Phần 2: Biểu diễn sơ đồ trạng thái và sơ đồ lưới của mã tích chập

- Mã tích chập là một máy trạng thái (state machine), có thể biểu diễn bằng sơ đồ chuyển trạng thái
  - Giá trị D-FF là trạng thái (state). Số lượng trạng thái 2^K
  - Đầu vào là kích thích chuyển trạng thái
  - Mũi tên mô tả quá trình chuyển trạng thái, với giá trị đầu vào/đầu ra.

  Ví dụ: 0/00 – Đầu vào *m*=0, đầu ra *c*=[00]



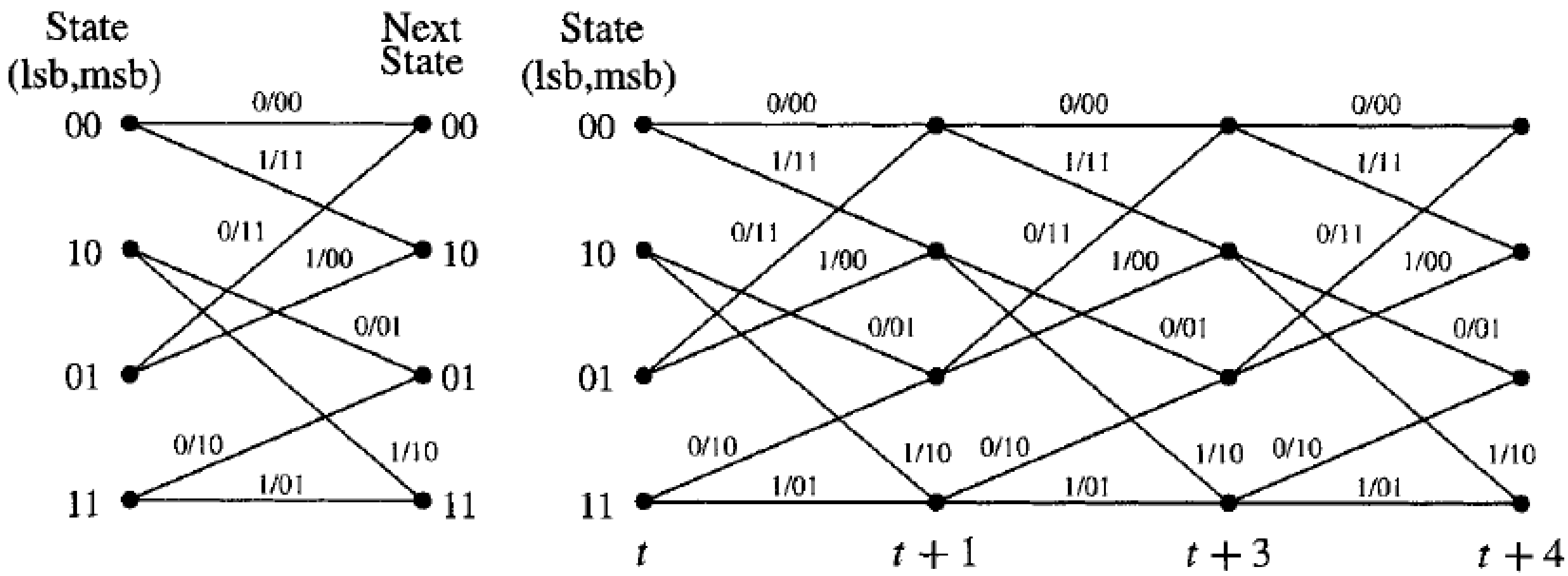
Bộ mã hóa tích chập R=1/2



Bộ mã hóa tích chập R=1/2

Phần 2: Biểu diễn sơ đồ trạng thái và sơ đồ lưới của mã tích chập

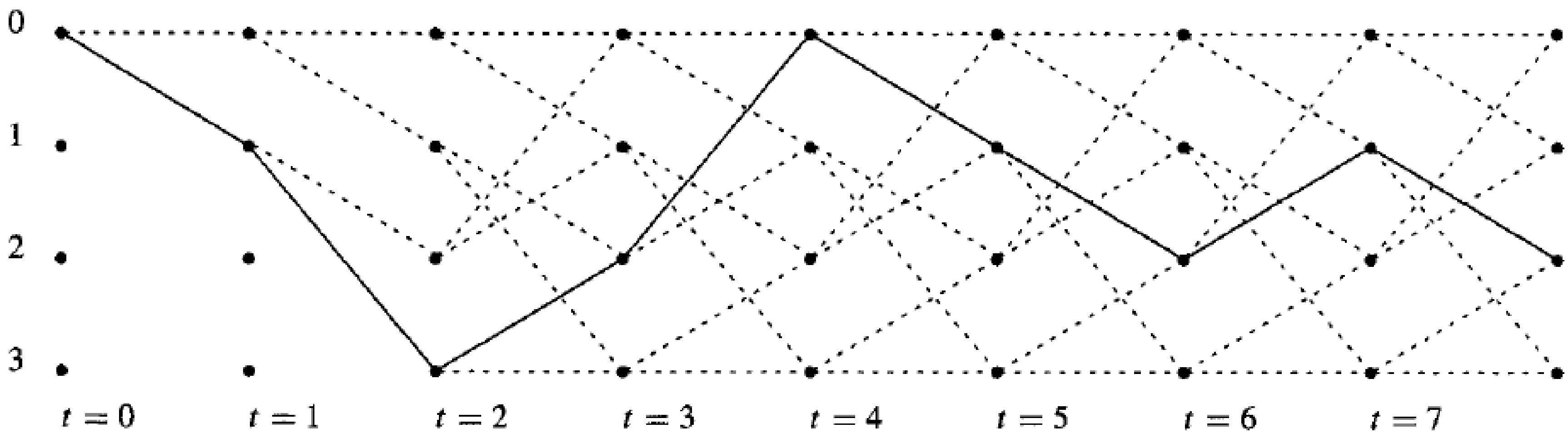
- Từ sơ đồ chuyển trạng thái, có thể chuyển sang sơ đồ lưới



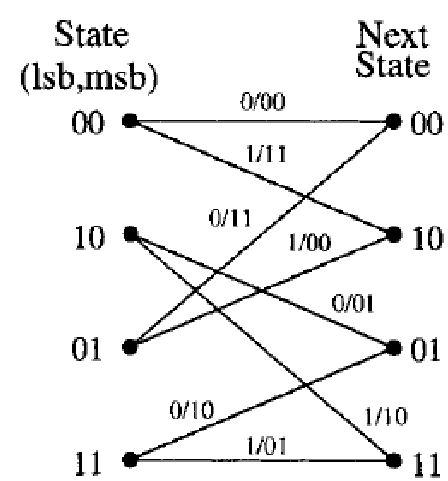
Phần 3: Thuật toán giải mã Viterbi

Sơ đồ lưới của mã tích chập $G(x) = \begin{bmatrix} 1+x^2 & 1+x+x^2 \end{bmatrix}$

Đầu vào m=[1,1,0,0,1,0,1,0]

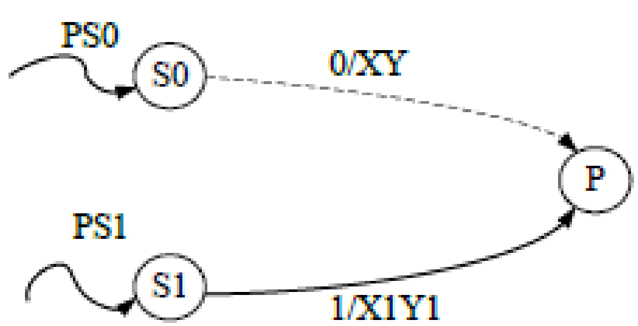


t	Input m_k	Output $\mathbf{c}_t$	State Ψ_{t+1}
0	1	11	1
1	1	10	3
2	0	10	2
3	0	11	0
4	1	11	1
5	0	01	2
6	1	00	1
7	0	01	2



Phần 3: Thuật toán giải mã Viterbi

- Thuật toán giải mã Viterbi thuộc lớp thuật toán giải mã ML (Maximum Likelihood).
- Thuật toán Viterbi là thuật toán tìm đường ngắn nhất, với quãng đường được tính toán là tổng khoảng cách Hamming của các nhánh trung gian.
  - *P* là trạng thái (state) đích, *S* trạng thái trung gian.
  - *P*0 là tổng khoảng cách quãng đường tới state *P* với bit đầu vào giá trị ‘0’, đi qua state *S*0. *BR*0 là khoảng cách Hamming (đầu ra) của nhánh *S*0-*P*
  - *P*1 là tổng khoảng cách quãng đường tới state *P* với bit đầu vào giá trị ‘1’, đi qua state *S*1. *BR*1 là khoảng cách Hamming (đầu ra) của nhánh *S*1-*P*



Algorithm 1 Path metric calculation in the conventional Viterbi algorithm

$P0 = PS0 + BR0$
$P1 = PS1 + BR1$

Phần 3: Thuật toán giải mã Viterbi

Ví dụ: mã tích chập $G(x) = \left[1 + x^2 \quad 1 + x + x^2\right]$

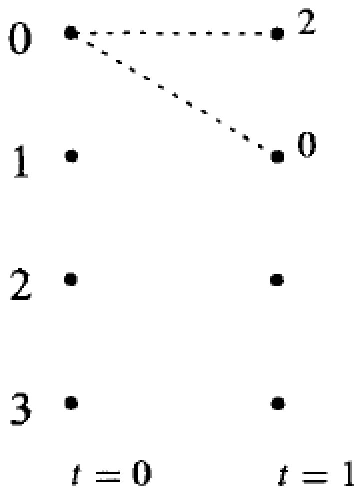
Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ 00\ 10\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit ‘0’).

Tại t=1. Khoảng cách Hamming giữa đầu ra [11] và nhánh 0-0 và 0-1 lần lượt là 2 và 0

$\mathbf{r}_0 = 11$



Phần 3: Thuật toán giải mã Viterbi

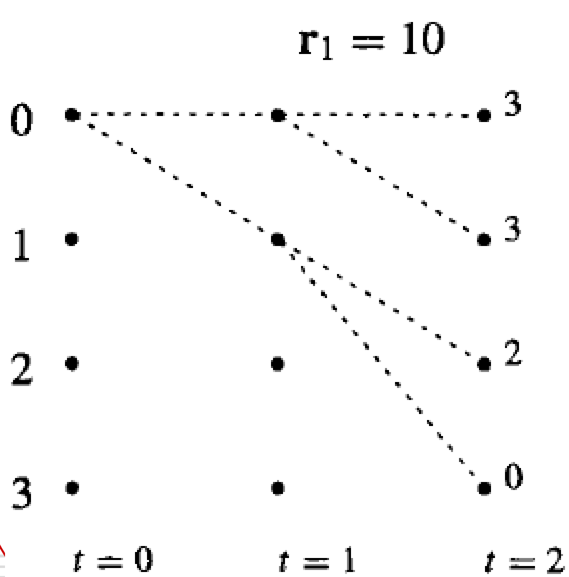
Ví dụ: mã tích chập $G(x) = \begin{bmatrix} 1+x^2 & 1+x+x^2 \end{bmatrix}$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit ‘0’).

Tại t=2, tính các khoảng cách Hamming tới các state



Phần 3: Thuật toán giải mã Viterbi

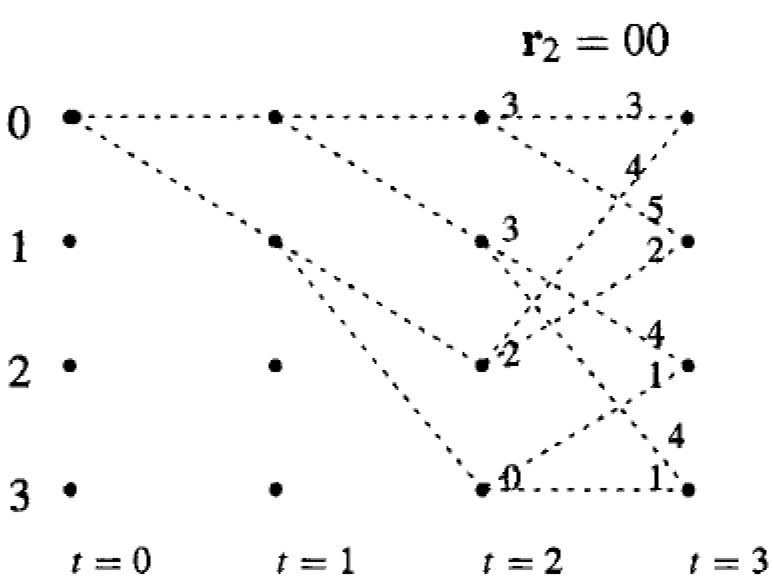
Ví dụ: mã tích chập $G(x) = \left[1 + x^2 \quad 1 + x + x^2\right]$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit ‘0’).

Tại t=3, tính các khoảng cách Hamming tới các state



Phần 3: Thuật toán giải mã Viterbi

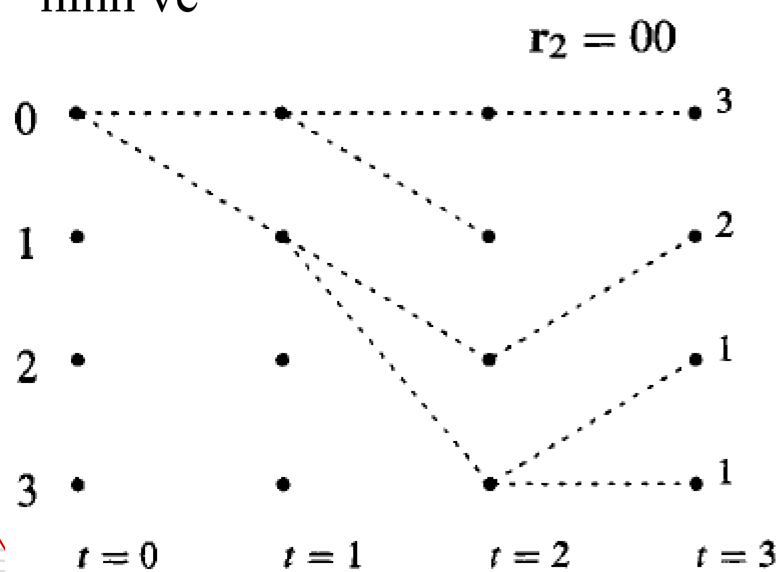
Ví dụ: mã tích chập $G(x) = \begin{bmatrix} 1+x^2 & 1+x+x^2 \end{bmatrix}$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit ‘0’).

Tại *t*=3: xuất hiện 2 tuyến đường cùng tới 1 trạng thái. So sánh là loại bỏ tuyến đường có khoảng cách Hamming lớn. Tuyến đường giữ lại được biểu diễn như hình vẽ



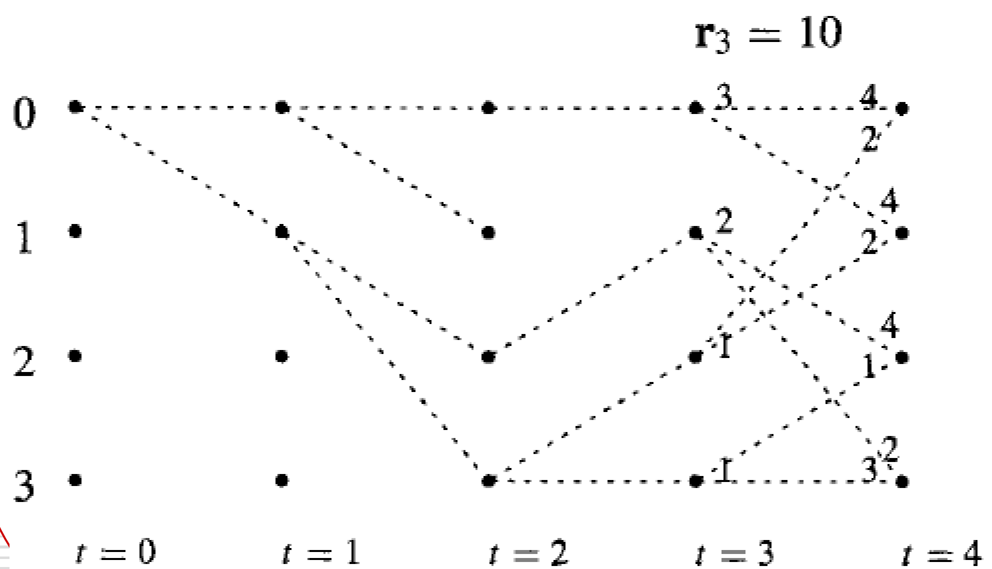
Ví dụ: mã tích chập $G(x) = \left[1 + x^2 \quad 1 + x + x^2\right]$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit '0').

Tại t=4: Mở rộng sơ đồ lưới, tính khoảng cách Hamming



Phần 3: Thuật toán giải mã Viterbi

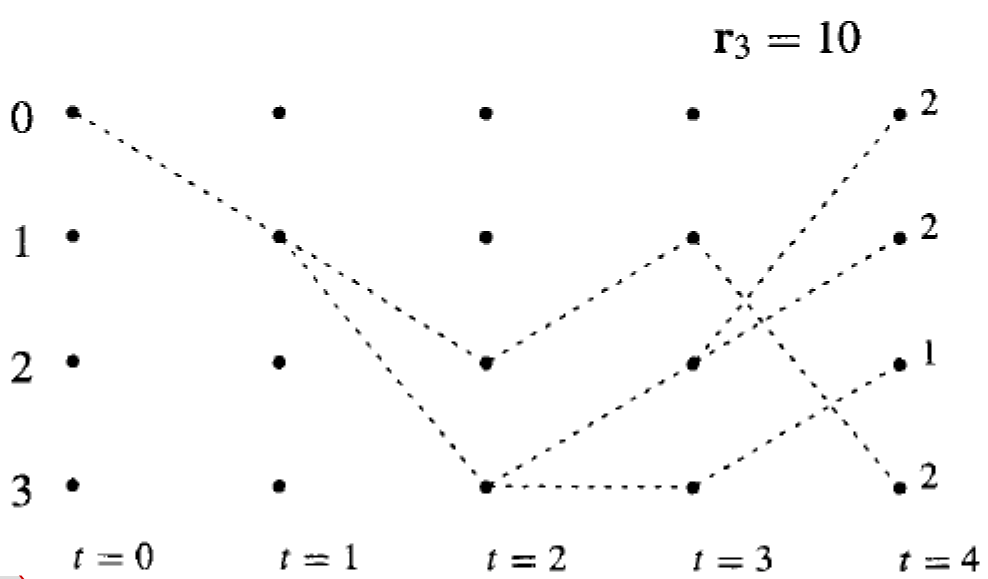
Ví dụ: mã tích chập $G(x) = \begin{bmatrix} 1+x^2 & 1+x+x^2 \end{bmatrix}$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit ‘0’).

Tại *t*=4: Loại bỏ nhánh có khoảng cách Hamming lớn



Phần 3: Thuật toán giải mã Viterbi

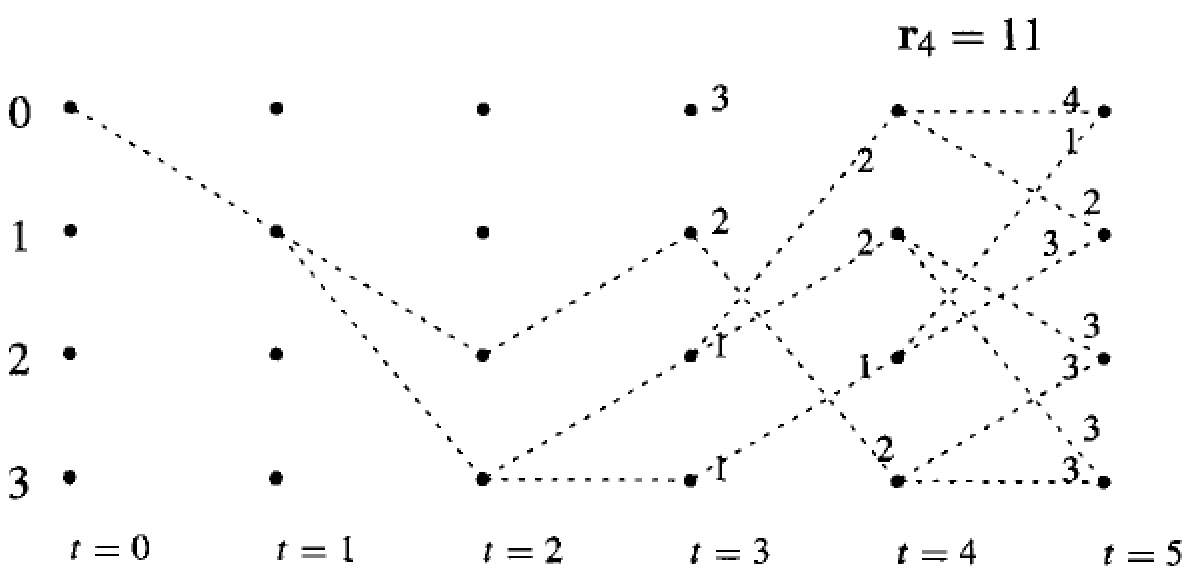
Ví dụ: mã tích chập $G(x) = \left[1 + x^2 \quad 1 + x + x^2\right]$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit ‘0’).

Tại *t*=5: Mở rộng sơ đồ lưới, tính khoảng cách Hamming



Phần 3: Thuật toán giải mã Viterbi

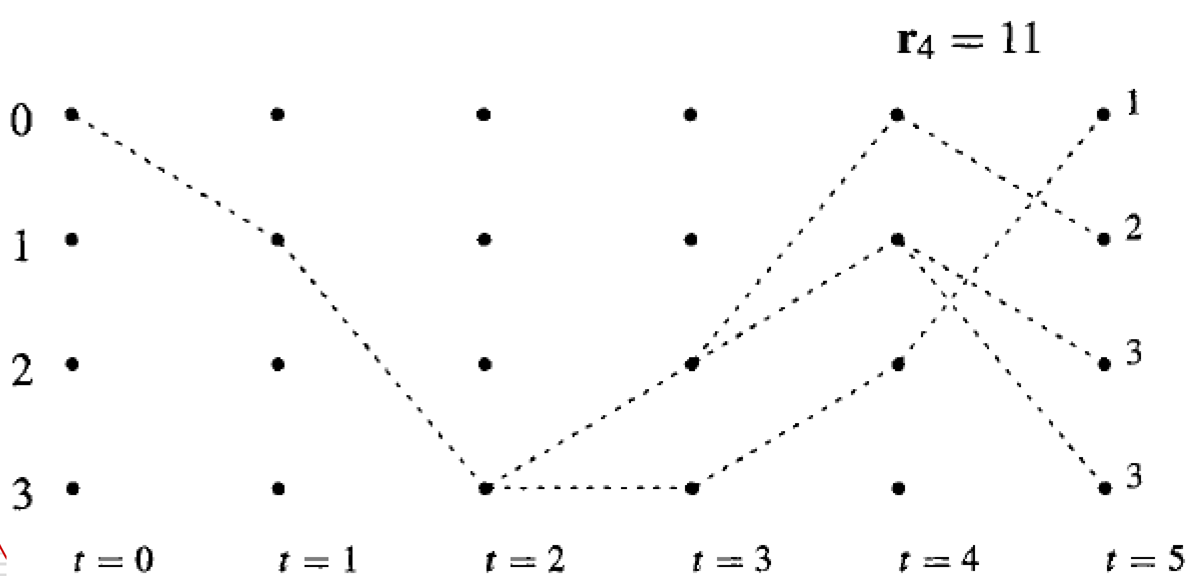
Ví dụ: mã tích chập $G(x) = \left[1 + x^2 \quad 1 + x + x^2 \right]$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ 00\ 10\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit ‘0’).

Tại *t*=5: Loại bỏ nhánh có khoảng cách Hamming lớn



Phần 3: Thuật toán giải mã Viterbi

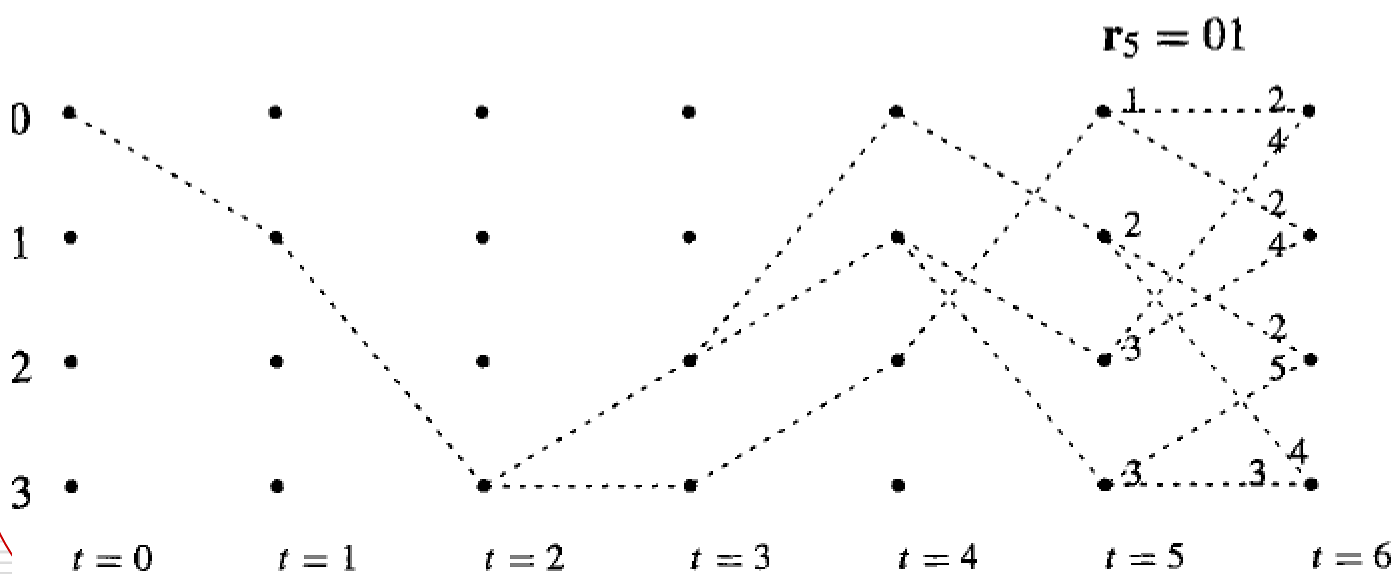
Ví dụ: mã tích chập $G(x) = \left[1 + x^2 \quad 1 + x + x^2\right]$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit ‘0’).

Tại *t*=6: Mở rộng sơ đồ lưới, tính khoảng cách Hamming



Phần 3: Thuật toán giải mã Viterbi

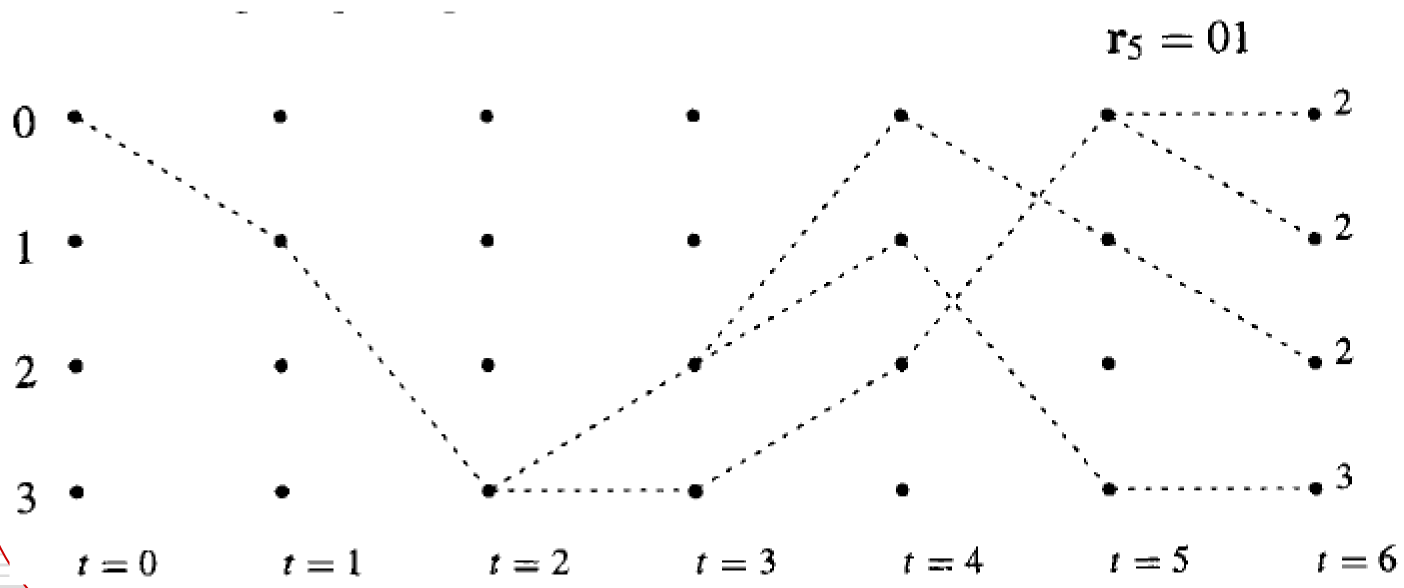
Ví dụ: mã tích chập $G(x) = \begin{bmatrix} 1+x^2 & 1+x+x^2 \end{bmatrix}$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit ‘0’).

Tại *t*=6: Loại bỏ nhánh có khoảng cách Hamming lớn



Phần 3: Thuật toán giải mã Viterbi

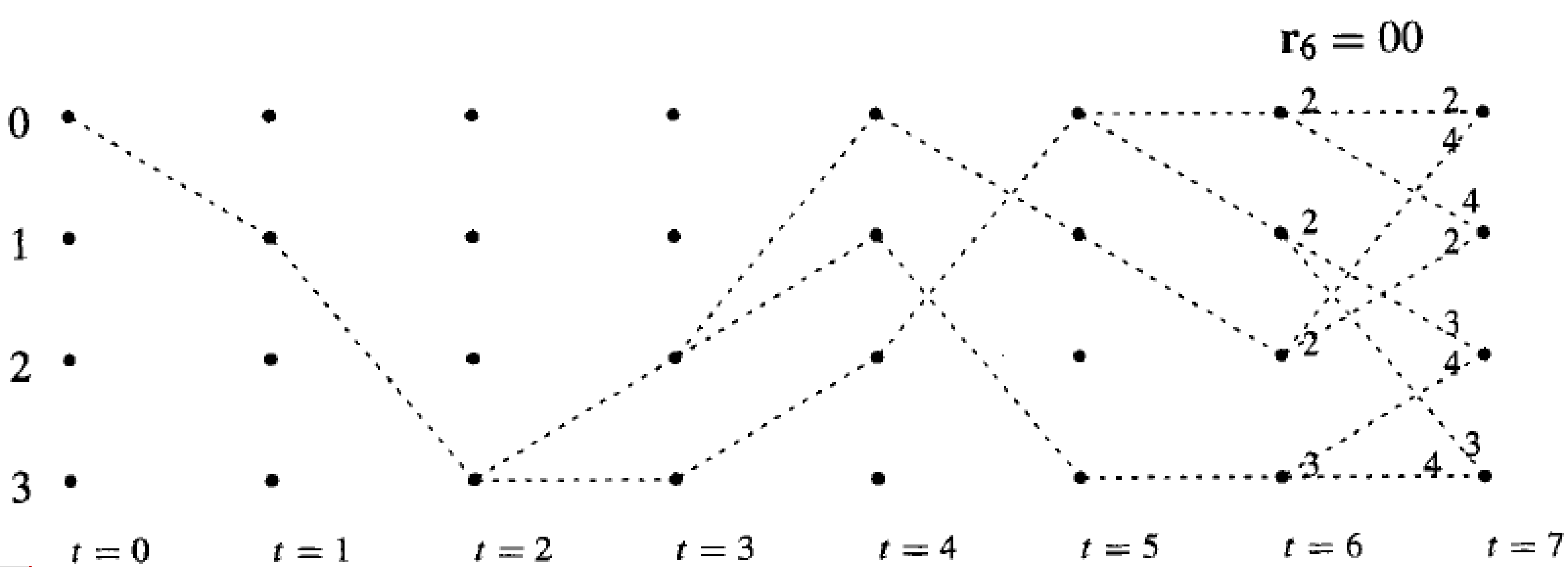
Ví dụ: mã tích chập $G(x) = \begin{bmatrix} 1+x^2 & 1+x+x^2 \end{bmatrix}$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit ‘0’).

Tại *t*=7: Mở rộng sơ đồ lưới, tính khoảng cách Hamming



Phần 3: Thuật toán giải mã Viterbi

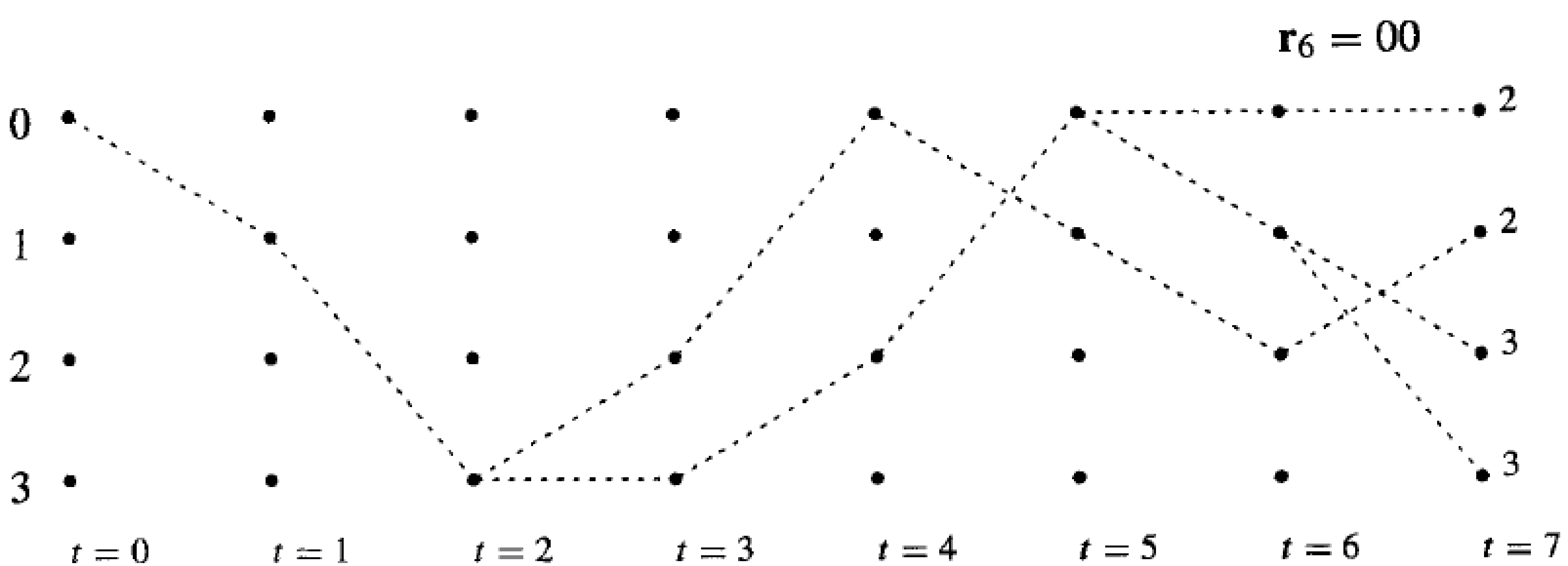
Ví dụ: mã tích chập $G(x) = \begin{bmatrix} 1+x^2 & 1+x+x^2 \end{bmatrix}$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit ‘0’).

Tại *t*=7: Loại bỏ nhánh có khoảng cách Hamming lớn



Phần 3: Thuật toán giải mã Viterbi

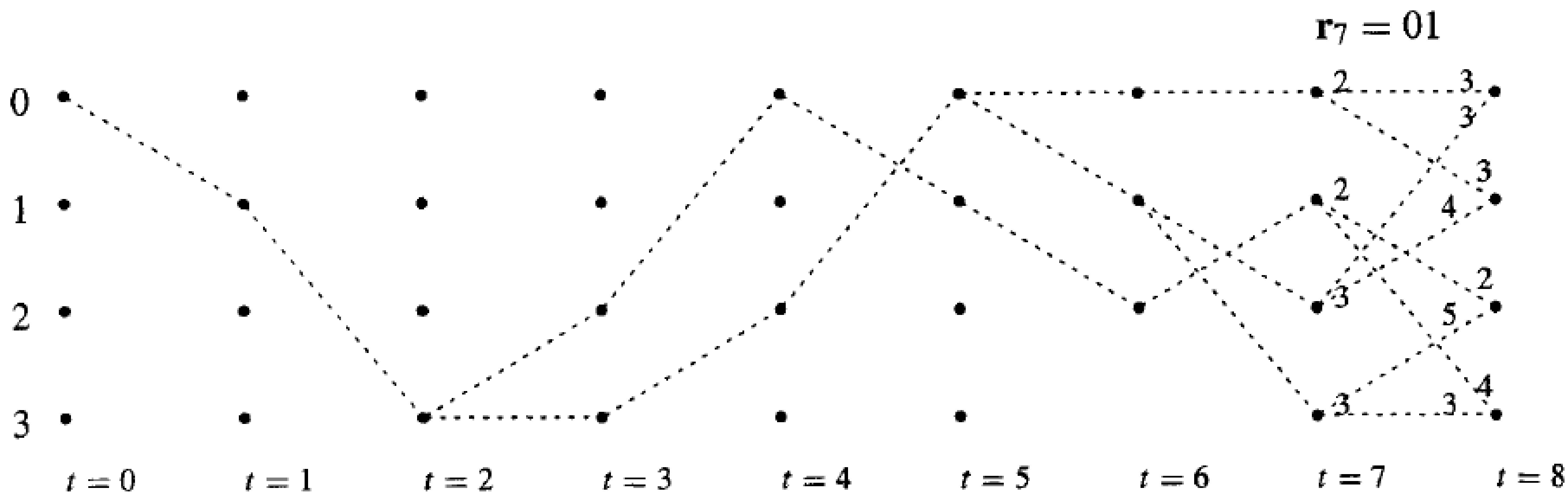
Ví dụ: mã tích chập $G(x) = \begin{bmatrix} 1+x^2 & 1+x+x^2 \end{bmatrix}$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit ‘0’).

Tại *t*=8: Mở rộng sơ đồ lưới, tính khoảng cách Hamming



Phần 3: Thuật toán giải mã Viterbi

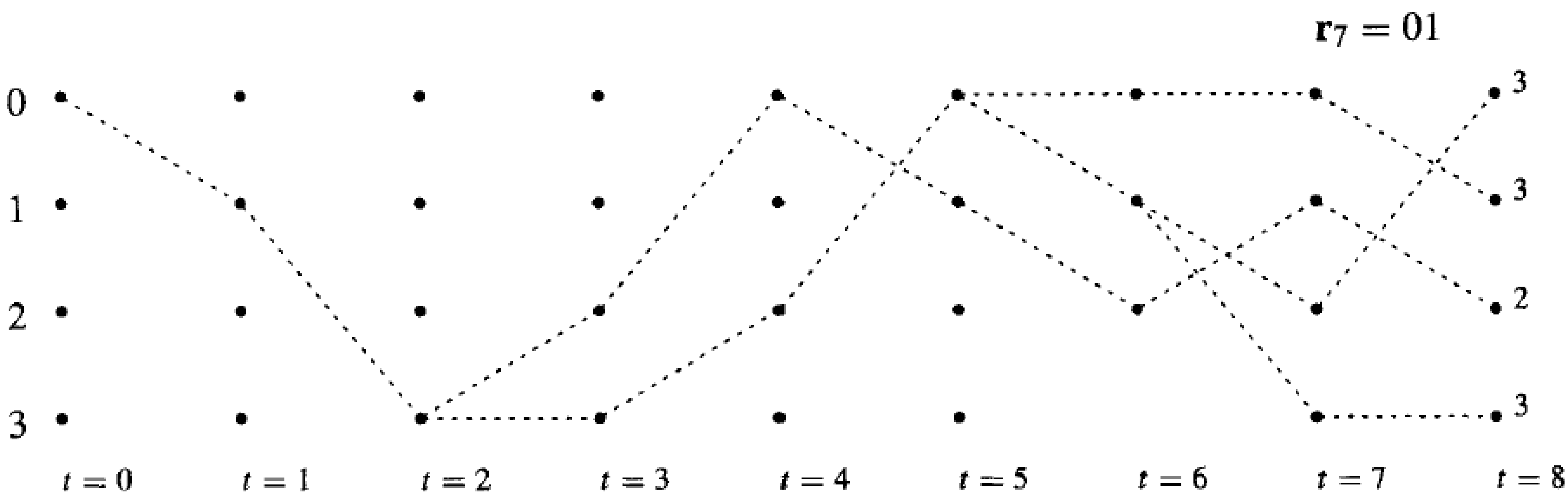
Ví dụ: mã tích chập $G(x) = \left[1 + x^2 \quad 1 + x + x^2\right]$

Đầu vào m=[1,1,0,0,1,0,1,0]

Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

Xuất phát từ trạng thái 0 (giá trị các D-FF được reset về giá trị bit '0').

Tại *t*=8: Loại bỏ nhánh có khoảng cách Hamming lớn



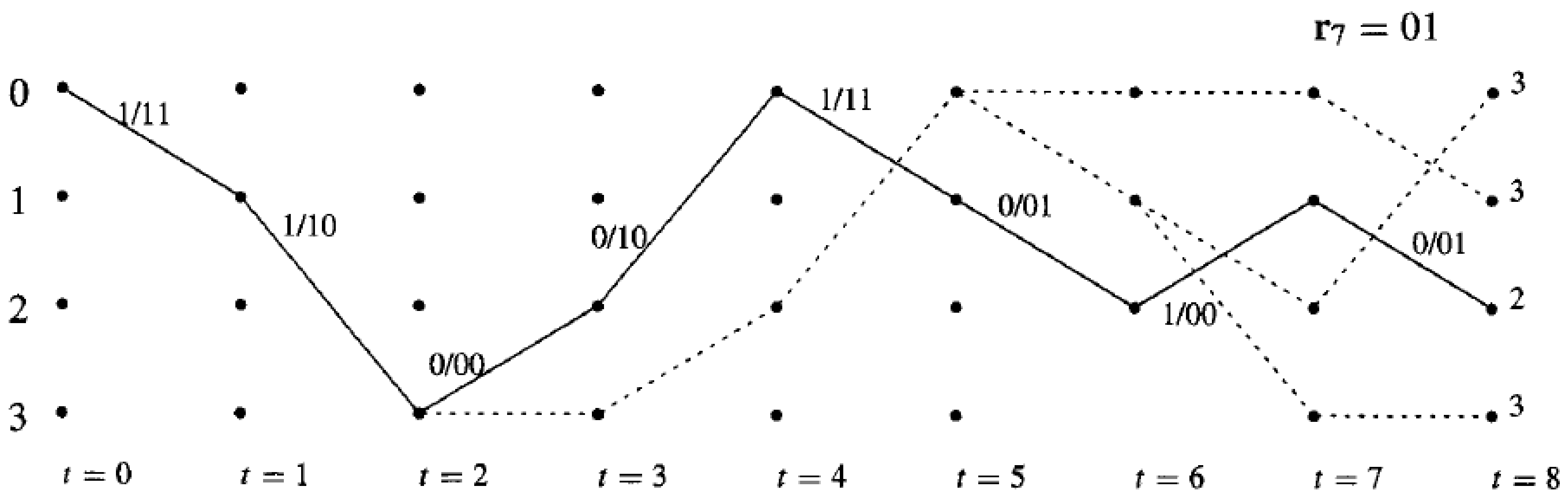
Phần 3: Thuật toán giải mã Viterbi

Ví dụ: mã tích chập $G(x) = \begin{bmatrix} 1+x^2 & 1+x+x^2 \end{bmatrix}$

Đầu vào m=[1,1,0,0,1,0,1,0]

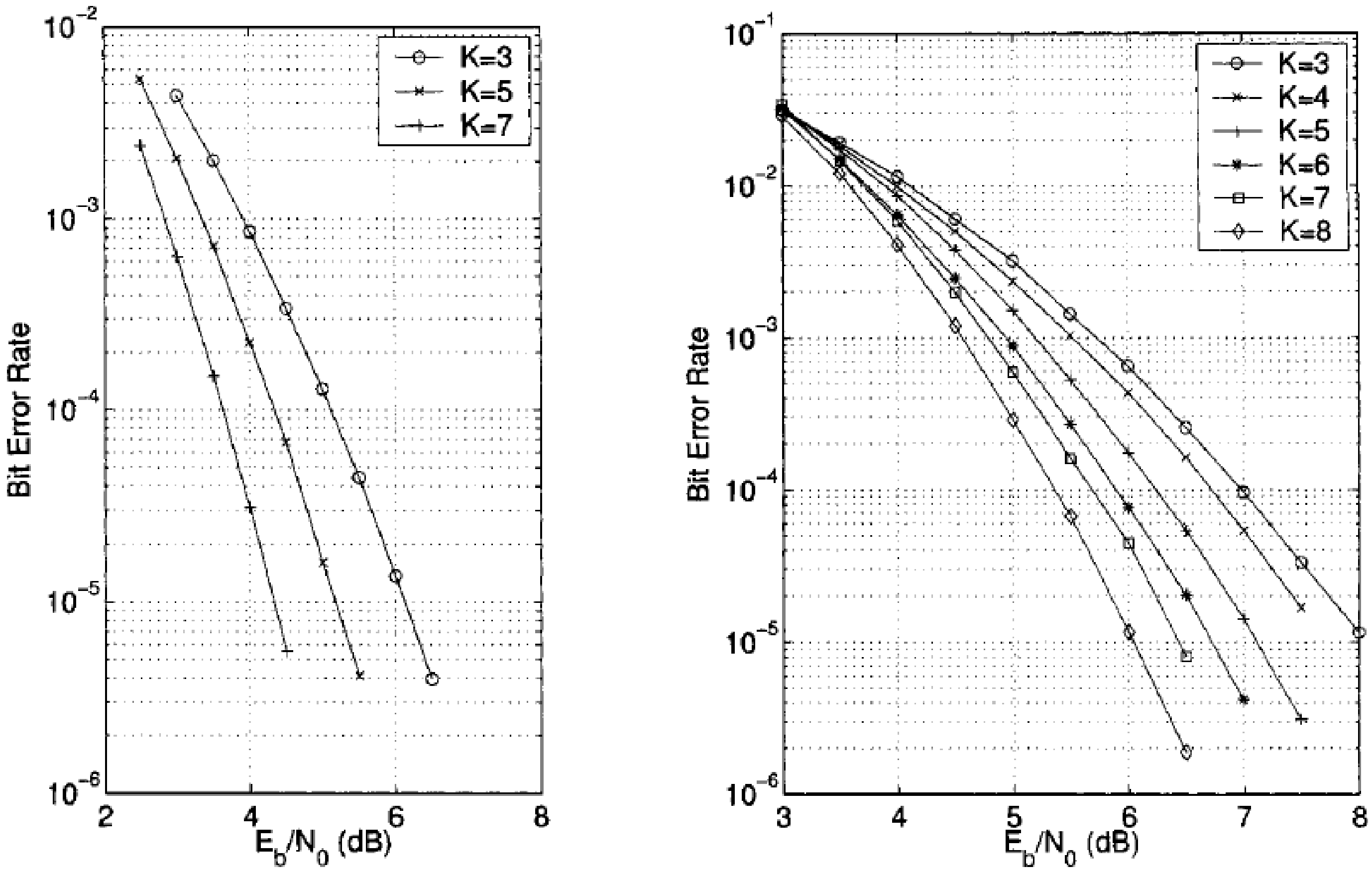
Từ mã thu được $\mathbf{r} = [11\ 10\ \underline{0}0\ 1\underline{0}\ 11\ 01\ 00\ 01\ \ldots] = [\mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4, \mathbf{r}_5, \mathbf{r}_6, \mathbf{r}_7, \ldots]$

- Lựa chọn tuyến đường ngắn nhất – Survival Path
- Đầu vào của tuyến đường ngắn nhất chính là thông tin cần giải mã-sửa lỗi.



Phần 3: Thuật toán giải mã Viterbi

- So sánh khả năng sửa lỗi của mã tích chập với các độ dài ràng buộc khác nhau, và phương pháp giải mã 1-bit (Khoảng cách Hamming) và 3-bit (khoảng cách Euclid).



(a) 8-level quantization, $K = 3, 5, 7$.

(b) 1-bit (hard) quantization, $K = 3$ through 8.