MCCC

1: INTRODUCCIÓN

* ENTROPÍA

$I(\text{info que genera la fuente}) = H(F)$ Entropía fuente

$I(\text{info que ha atravesado el canal}) = H(F) - H(F/D)$ Entropia de salida / salida

$$\boxed{I = H(F) - H(F/D) = H(D) - H(D/F)} \quad [\text{bits/simb}]$$

$$\boxed{C = I_{max} = \max_{\{p(A_i)\}} [\,I\,]}$$ Capacidad del canal: info máx para todas las posibles fuentes

- CANAL SIN PERDIDA $\Rightarrow H(F/D) = 0 \Rightarrow C = \max\{H(F)\} = \log_2 m$
- CANAL DETERMINISTA $\Rightarrow H(D/F) = 0 \Rightarrow C = \max\{H(D)\} \leq \log_2 n$
  $= \Leftrightarrow$ símbolos de salida equiprobables
- CANAL SIN RUIDO $\Rightarrow H(F/D) = H(D/F) = 0 \Rightarrow C = \log_2 m = \log_2 n \Rightarrow m = n$
- CANAL SIMÉTRICO

$$\begin{array}{c} \\ A_1 \\ A_2 \end{array} \begin{array}{c} \begin{array}{cccc} B_1 & B_2 & B_3 & B_4 \end{array} \\ \begin{bmatrix} 1/3 & 1/3 & 1/6 & 1/6 \\ 1/6 & 1/8 & 1/3 & 1/3 \end{bmatrix} \end{array}$$

símbolos salida

símbolos entrada

Todas las filas contienen los mismos valores aunque esten en otro orden. Idem para columnas

$$H(D/A_i) = \sum_{j=1}^{n} p(B_j/A_i) \log_2 \frac{1}{P(B_j/A_i)} \overset{\text{canal simétrico}}{=} H$$

$$H(D/F) = \sum_{i=1}^{m} p(A_i)\, H(D/A_i) = H$$

$$\boxed{C = \max_{\{p(A_i)\}} [H(D) - H(D/F)] \overset{p(B_j)=\frac{1}{n}}{=} \log_2 n - H(D/F)}$$

- CANAL ARBITRARIO

1/ Calcular $\quad H(D/A_i) = \sum_{j=1}^{n} p(B_j/A_i) \log_2 \frac{1}{P(B_j/A_i)}$

2/ Resolver $\quad [P(B_j/A_i)] \cdot [Z_i]^{+} = [H(D/A_i)]^{+}$

3/ $C = \log_2 \left[\sum_{j=1}^{n} 2^{-z_i} \right]$

* CRITERIO DE DECISIÓN MAP

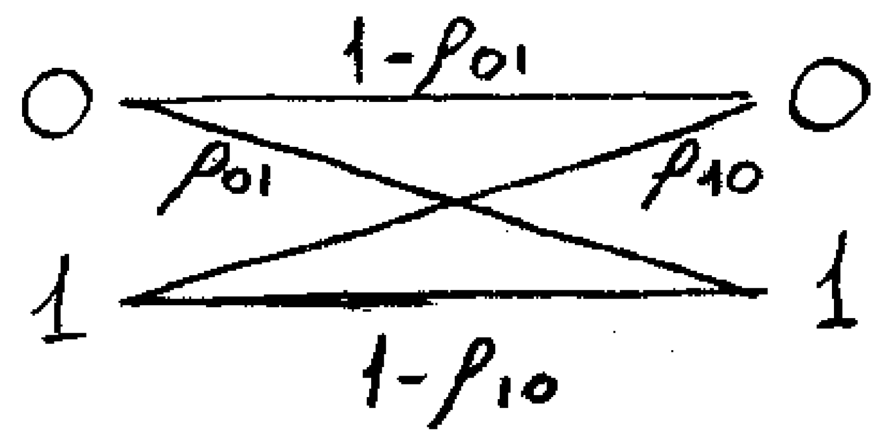
Recibido B_j escogemos A_i tq $\max_{A_i} \{ p(A_i/B_j) \}$

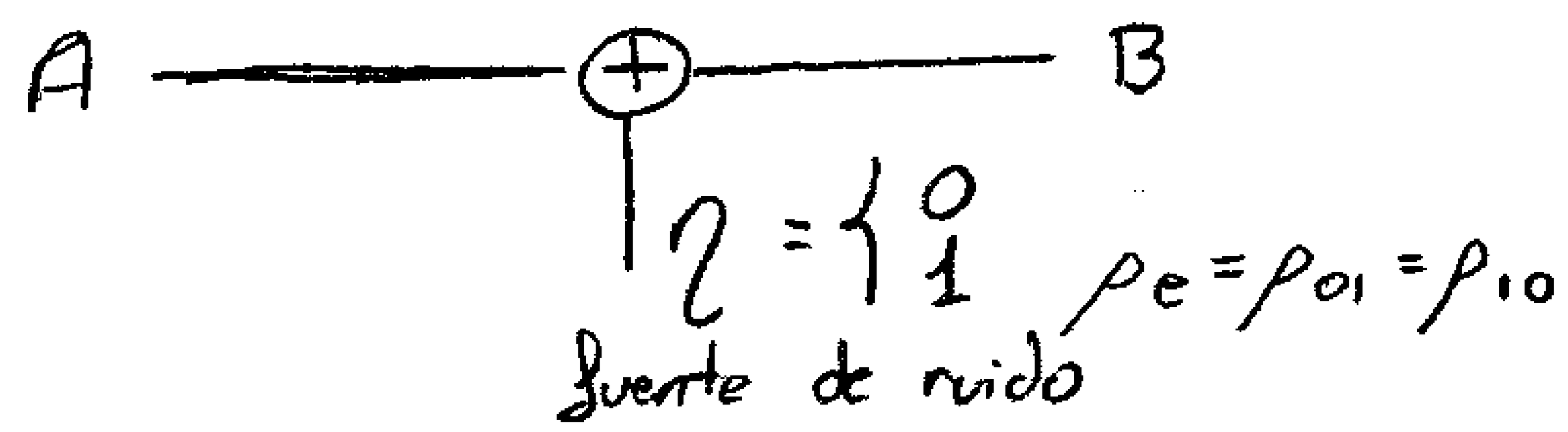
* CRITERIO DE DECISIÓN ML

Recibido B_j escogemos A_i tq $\max_{A_i} \{ p(B_j/A_i)\, p(A_i) \}$

* MODELOS DE CANAL

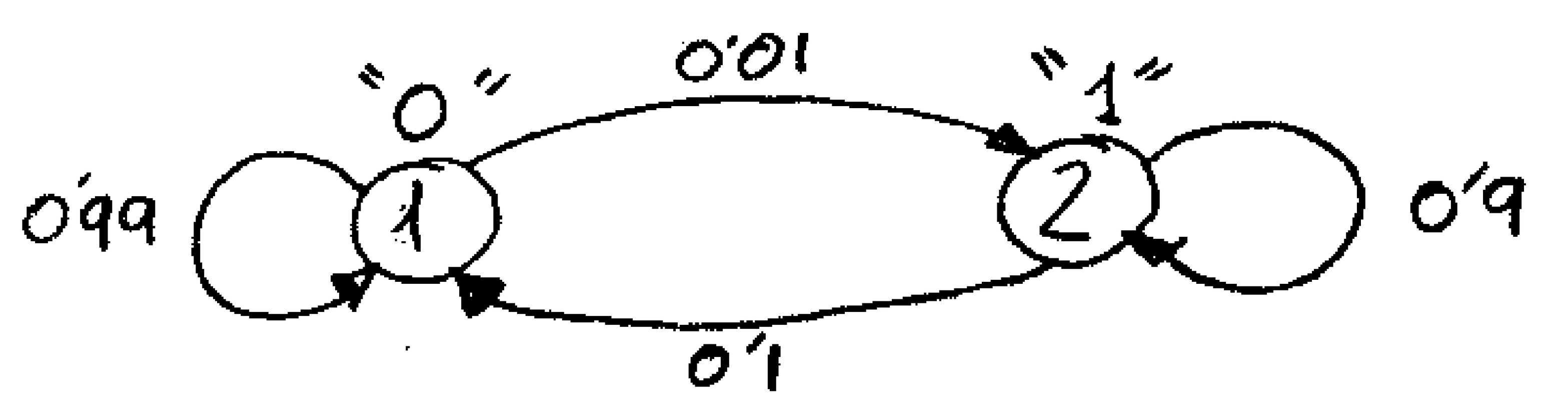
• Modelo canal simétrico





$p_e = \rho_{01} = \rho_{10}$

• Modelo cadena de Gilbert (Fuente con memoria)



$$\left.\begin{array}{l} p(1) = p(1/1)\,p(1) + p(1/2)\,p(2) \\ p(1) + p(2) = 1 \end{array}\right\} \text{Resolver sistema}$$

$$H(F) = H(F/1)\,p(1) + H(F/2)\,p(2)$$

$$H(F/S_i) = \sum_{j=1} P(E_j/S_i) \log_2 \frac{1}{P(E_j/S_i)}$$

* Capacidad con una fuente de error

$$C = C_{max} - H(F_{error})$$

* Prob 'i' errores en un vector de 'n' componentes

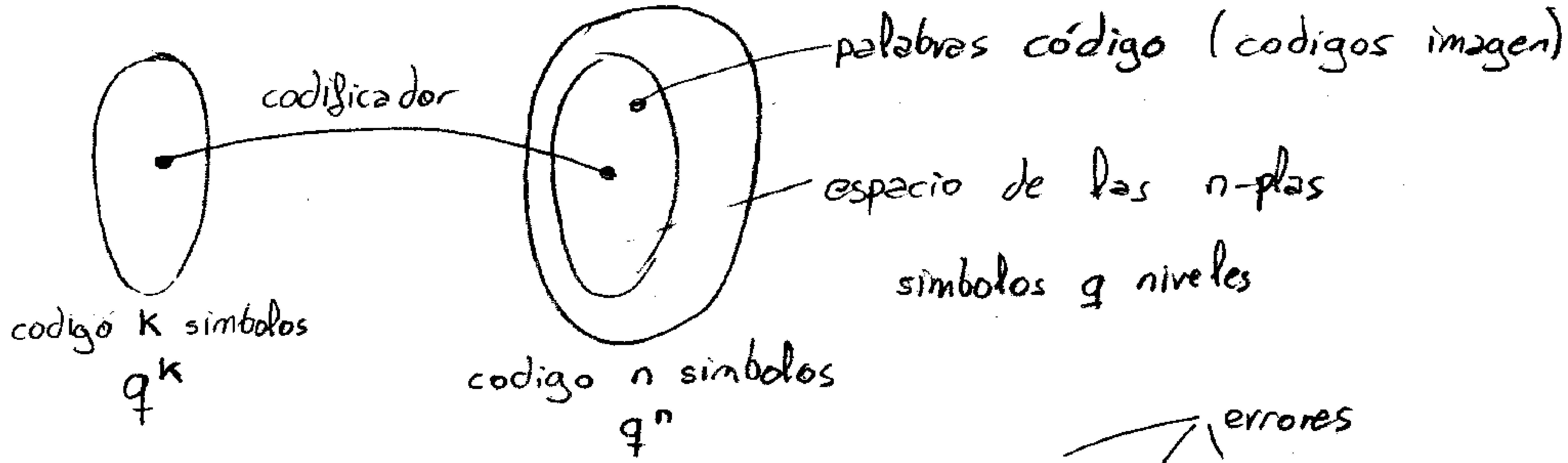
$$P = \binom{n}{i} p_e^{\,i} (1-p_e)^{n-i}$$

* Si corrige c errores $\quad P_{Be} = \sum_{i=c}^{n} \binom{n}{i} p_e^{\,i} (1-p_e)^{n-i} \simeq \binom{n}{c} p_e^{\,c} (1-p_e)^{n-c}$

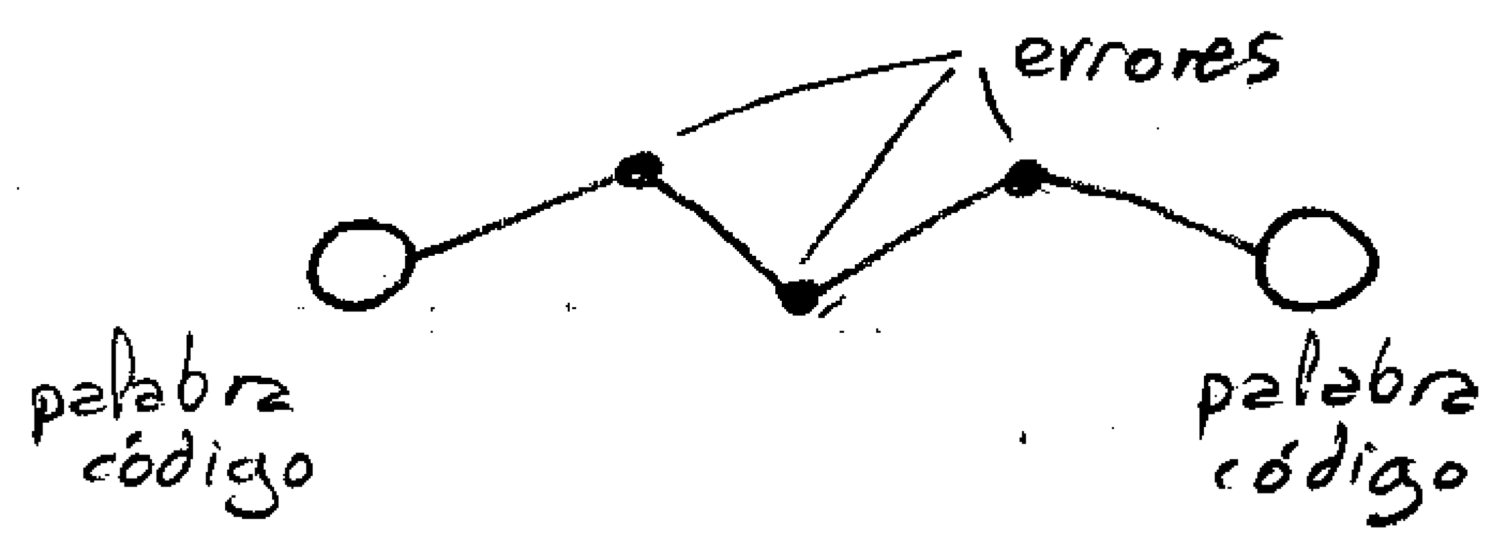
* P. error final al user $\Rightarrow P_{e,final} = \dfrac{\#\text{bits err}}{\#\text{bits tot}} = \dfrac{\#\text{bits err bloq} \cdot \#\text{bloq err}}{\#\text{bits bloq} \cdot \#\text{bloq tot}}$ → P_{Be}

=

12: TEORIA DE LA CODIFICACIÓN ALGEBRAICA



- Distancia mínima del código



Distancia mínima entre dos palabras còdigo.

- Capacidad correctora $\quad c = \left[\frac{d-1}{2}\right]$
- Capacidad detectora $\quad \delta = d - 1$
- Capacidad correctora de borrones (Soft Decision) $= 2c$

$\Rightarrow$ Se pueden corregir t errores y $\left|\begin{array}{ll} s \text{ borrones} & \Leftrightarrow 2t + s < \delta \\ \text{detectar } r \text{ más} & \Leftrightarrow 2t + r < \delta \end{array}\right.$

- Códigos perfectos $\Rightarrow$ si # errores $> c$ siempre se equivoca

* CÓDIGOS LINEALES (Sistemáticos)

Matriz generadora $\quad G = \left[Id_k | P\right]_{n \times K}$

Matriz de comprovación $\quad H = \left[-P^T | Id_r\right]_{n \times r}$

Prop:
- Todas columnas diferentes
- Ninguna columna $\vec{0}$

$\vec{u}$ código a enviar
$\vec{v}$ codificación del código (palabra código) $\quad \vec{v} = \vec{u} \cdot \overline{G}$; $\vec{v} \cdot \vec{H}^T = \vec{0}$
$\vec{z}$ código recibido $\quad \vec{z} = \vec{v} + \vec{e}$; $\vec{s} = \vec{e} \cdot \vec{H}^T$

* CÓDIGOS HAMMING (1-PERFECTOS)

$$\boxed{n = 2^r - 1}$$

* CÓDIGOS NO NECESARIAMENTE LINEALES

• Cota de Hamming

$$\boxed{q^k \sum_{i=0}^{c} \binom{n}{i} (q-1)^i \leq q^n} \leq q^n \sum_{i=0}^{\ell} \binom{n}{i} (q-1)^i$$

• Cota de Gilvert-Varshamon

$$\boxed{q^k \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i}}$$

• Cota de Singleton (Códigos lineales)

$$\boxed{d \leq r + 1}$$

* REPRESENTACIÓN POLINÓMICA

• Códigos cíclicos

$V(D)$: palabra código
$U(D)$: datos
$g(D)$: pol. generador

$\vec{V} \doteq (V_{n-1}, V_{n-2}, \ldots, V_2, V_1, V_0)$
$\vec{V}^r = (V_{n-2}, V_{n-3}, \ldots, V_1, V_0, V_{n-1})$

$$V^r(D) = D \cdot V(D) - V_{n-1}(D^n - 1) \Rightarrow \boxed{V^i(D) = D^i \cdot V(D) \bmod (D^n - 1)}$$

$$\boxed{V(D) \equiv q(D) \cdot g(D)} \qquad g(D) \text{ divide } D^n - 1$$

- Códigos Hammig $H(n,K,r)$

$$(D^n + 1) = (D+1)\, g(D)\, g^+(D)$$

$$(D^7+1) = (D+1)(D^3+D+1)(D^3+D^2+1)$$

Polinomio de comprovación $\Rightarrow$ $h(D) = \dfrac{D^n+1}{g(D)}$

- BCH $m, t \Rightarrow GF(2^m)$

$n = 2^m - 1$; $r = 2t$

$g(D) = m_1(D)\, m_3(D) \cdots m_{2t-1}(D)$

$m_1(D) = (D+\alpha)(D+\alpha^2)(D+\alpha^{2^2}) \cdots$

$m_3(D) = (D+\alpha^3)(D+\alpha^{3^2})(D+\alpha^{3^{2^2}}) \cdots$

Todos los terminos no repetidos $(D+(\alpha^i)^{2\cdot 2\cdot 2\cdots})$

- Corrección : Idem R-S

$S_1 = w(\alpha)$ $\quad S_2 = w(\alpha^2)$ $\quad \ldots \quad S_r = w(\alpha^r)$

$$\begin{bmatrix} S_1 & S_2 & \cdots & S_n \\ S_2 & & & \\ S_3 & & & \\ \vdots & & & \\ S & & & \end{bmatrix} \begin{bmatrix} L \\ \\ \\ L_2 \\ L_1 \end{bmatrix} = \begin{bmatrix} S_{n+1} \\ \vdots \\ \\ \\ S_r \end{bmatrix}$$

Para saber num errores $\begin{vmatrix} S_1 & S_2 & \cdots \\ S_2 & \cdots & \cdots \\ \vdots & & \end{vmatrix} \neq 0$ si es 0 quitamos las úlimas filas y columnas.

- Reed-Solomon

$$g(D) = (D+\alpha)(D+\alpha^2)(D+\alpha^3)\cdots(D+\alpha^r)$$

$$v(D) = u(D)D^r + u(D)D^r \bmod g(D)$$

Corrección

$S_1 = w(\alpha) \quad S_2 = w(\alpha^2) \ \ldots \ S_r = w(\alpha^r)$

$S(D) = S_1 + S_2 D + S_3 D^2$

- Algoritmo de Euclides $\xrightarrow{\text{hasta grado } \leq t} \mathcal{E}(D), \ L(D)$
- Pos errores $L(1/\alpha^{pos}) = 0$
- Valor errores $\mathcal{E} = \left. \dfrac{\mathcal{E}(D)}{L'(D)} \right|_{D = 1/\alpha^{pos}}$

Con borrones

$L(D) = L_B(D) \cdot L_E(D)$

$L_B(D) = (D+\alpha^{pos1})(D+\alpha^{pos2})\cdots$

$\hat{S}(D) = S(D) \cdot L_B(D) \bmod D^r$

- Obtenemos $\mathcal{E}(D)$ y $L_E(D)$ mediante Euclides (hasta grado $\leq t + \frac{\#borr}{2}$) a partir $\hat{S}(D)$
- Continuamos como en el caso normal

Alg. Euclides

	$d_1 = D^r / S(D)$	$d_2 = S(D)/r_1$		
D^r	$S(D)$	$r_1 = D^r \% S(D)$	$r_2 = S(D) \% r_1$	$= \mathcal{E}(D)$

	d_1	d_2		
0	1	$t_1 = d_1 \cdot 1 + 0$	$t_2 = d_2 \cdot t_1 + 1$	$= L(D)$