Compresión de Datos sin Pérdida

Codificación Aritmética

Álvaro Martín

[1]Instituto de Computación,
Facultad de Ingeniería
almartin@fing.edu.uy

[2]PEDECIBA Informática

Motivación

- Sabemos cómo codificar un bloque $X_1, X_2, \ldots, X_n$ de forma ópitima si conocemos su distribución de probabilidad conjunta.
- Podríamos, por ejemplo, aplicar Huffman sobre el alfabeto $\mathcal{X}^n$.
- Pero el tamaño de $\mathcal{X}^n$ crece exponencialmente con n
- Buscamos un algoritmo de codificación con requerimientos de tiempo/memoria que escalen eficientemente con n.

Código de Shannon-Fano-Elias

- Consideramos el orden lexicográfico para secuencias de largo n, y definimos

$$F_n(x^n) = \sum_{y^n < x^n} P_n(y^n)\,. \tag{1}$$

- Identificamos cada secuencia x^n con un número real en

$$\left[F_n(x^n), F_n(x^n) + P_n(x^n)\right)$$

- Concretamente, usamos el punto medio del intervalo,

$$\bar{F}_n(x^n) = F_n(x^n) + \frac{1}{2}P_n(x^n)\,, \tag{2}$$

truncado a cierta precisión finita.

Código de Shannon-Fano-Elias

- Denotamos $\lfloor \cdot \rfloor_\ell$ al resultado de truncar la representación en base dos de un real a ℓ dígitos a la derecha de la coma.
- Identificamos a x^n mediante el real

$$\lfloor \bar{F}_n(x^n) \rfloor_{\ell(x^n)} \,, \tag{3}$$

donde

$$\ell(x^n) = \lceil -\log P_n(x^n) \rceil + 1 \,. \tag{4}$$

- Si no hay ambigüedad, omitimos x^n en la notación $\ell(x^n)$.
- Palabra de código $c(x^n)$ para x^n:

$$\bar{F}_n(x^n) = 0, \underbrace{c_1 c_2 \ \ldots \ c_\ell}_{c(x^n)} \, c_{\ell+1} c_{\ell+2} \ \ldots$$

Código de Shannon-Fano-Elias es instantáneo

- La diferencia entre $\bar{F}_n(x^n)$ y $\lfloor \bar{F}_n(x^n) \rfloor_\ell$ no excede $2^{-\ell}$,

$$\lfloor \bar{F}_n(x^n) \rfloor_\ell \geq \bar{F}_n(x^n) - 2^{-\ell} \, .$$

- Además, $2^{-\ell}$ no excede la mitad del tamaño del intervalo asociado a x^n. Como $\ell(x^n) \leq -\log P_n(x^n) + 2$, entonces

$$2^{-\ell} \leq \frac{1}{2} P_n(x^n) \, .$$

- Por lo tanto,

$$\left[\lfloor \bar{F}_n(x^n) \rfloor_\ell, \lfloor \bar{F}_n(x^n) \rfloor_\ell + 2^{-\ell} \right) \subseteq \left[F_n(x^n), F_n(x^n) + P_n(x^n) \right) .$$

- El intervalo de la izquierda cubre a todos los números de la forma

$$0, \underbrace{c_1 c_2 \, \ldots \, c_\ell}_{c(x^n)} \, c_{\ell+1} c_{\ell+2} \, \ldots \, c_m$$

- Como los intervalos son disjuntos, ninguna palabra puede ser prefijo de otra.

Código de Shannon-Fano-Elias: Cálculo de $\bar{F}_n(x^n)$

- Para $a \in \mathcal{X}$ definimos

$$C_n(a|x^{n-1}) = \sum_{b<a} P(b|x^{n-1}) \tag{5}$$

- Definimos también la recurrencia

$$\begin{aligned} F_0 &= 0\,, & (6)\\ F_n &= F_{n-1} + C_n(x_n|x^{n-1})P_{n-1}(x^{n-1})\,, & (7) \end{aligned}$$

  donde, por convención, $P_0(x^0) = 1$.

- La recurrencia (6)-(7) calcula $F_n(x^n)$, es decir, $F_n(x^n) = F_n$.

Código de Shannon-Fano-Elias: Determinación de $c(x^n)$

- Si $P(b|x^{i-1})$ se puede calcular "eficientemente" para $b \in \mathcal{X}$, $i = 1 \ldots n$, entonces podemos calcular F_n eficientemente.
  Para cada i, $1 \leq i \leq n$,
  - $C_n(x_i|x^{i-1})$ se obtiene sumando no más de $|\mathcal{X}|$ términos de la forma $P(b|x^{i-1})$.
  - Habiendo calculado $P_{i-1}(x^{i-1})$ en el paso anterior, obtenemos $P_i(x^i)$ multiplicando por $P(x_i|x^{i-1})$.
- Como $\ell - 1 = \lceil -\log P_n(x^n) \rceil$, entonces

$$-\log P_n(x^n) \leq \ell - 1 < -\log P_n(x^n) + 1\,,$$

  de donde obtenemos $2^{-(\ell-1)} \leq P_n(x^n)$, y $2^{-(\ell-2)} > P_n(x^n)$.
- $P_n(x^n) = 0, \underbrace{000 \ldots 001}_{\ell-1} xxxx$

Código de Shannon-Fano-Elias: Decodificación

- Definimos G_0 como el número representado por la palabra de código recibida,

$$G_0 = \lfloor \bar{F}_n(x^n) \rfloor_\ell \,. \tag{8}$$

- Para $i > 0$, definimos

$$\tilde{x}_i = \text{máx} \left\{ b \in \mathcal{X} : C_i(b|\tilde{x}^{i-1}) P_{i-1}(\tilde{x}^{i-1}) \leq G_{i-1} \right\} , \tag{9}$$

y

$$G_i = G_{i-1} - C_i(\tilde{x}_i|\tilde{x}^{i-1}) P_{i-1}(\tilde{x}^{i-1}) \,, \tag{10}$$

donde el máximo en (9) es con respecto al orden lexicográfico sobre $\mathcal{X}$ y se demuestra que es sobre un conjunto no vacío.

Teorema: La secuencia $\tilde{x}^n$ definida por (8)-(10) coincide con x^n.

Código de Shannon-Fano-Elias: Idea de prueba de corrección

- Por inducción, usando que para $1 \leq i \leq n$

$$\lfloor \bar{F}_n(x^n) \rfloor_\ell \in \left[F_n(x^n), F_n(x^n) + P_n(x^n) \right) \subseteq \left[F_i(x^i), F_i(x^i) + P_i(x^i) \right) .$$

- Para $i = 1$, la ecuación (9) se reduce a

$$\tilde{x}_1 = \text{máx} \left\{ b \in \mathcal{X} : F_1(b) \leq \lfloor \bar{F}_n(x^n) \rfloor_\ell \right\} . \tag{11}$$

- Asumiendo que $\tilde{x}^{i-1} = x^{i-1}$, observamos que

$$G_{i-1} = \lfloor \bar{F}_n(x^n) \rfloor_\ell - F_{i-1} , \tag{12}$$

y (9) se convierte en

$$\tilde{x}_i = \text{máx} \left\{ b \in \mathcal{X} : F_i(x^{i-1} b) \leq \lfloor \bar{F}_n(x^n) \rfloor_\ell \right\} . \tag{13}$$

Codificación Aritmética

- Alfabeto de entrada $\mathcal{X} = \{1 \dots M\}$. Salida en base $D \geq 2$.
- $Q_i[m] \simeq P(X_i = m | x^{i-1})$ con J dígitos de precisión

$$Q_i[m] = \sum_{j=1}^{J} q_j D^{-j}\,, \quad 0 < Q_i[m] < 1\,, \quad \text{y} \quad \sum_{m=1}^{M} Q_i[m] = 1\,.$$

Q_i puede depender de x^{i-1} o $\tilde{x}^{i-1}$.

- $C_i[m] = \sum_{j<m} Q_i[j]$ (acumulativa).
- $T = \sum_{j=0}^{K-1} t_j D^{-\tau-j}$: ancho del intervalo con K dígitos de precisión y representación de punto flotante

$$T = t_0, t_1 t_2 \dots t_{K-1} \times D^{-\tau}\,, \quad t_0 > 0\,. \tag{14}$$

Se cumple que

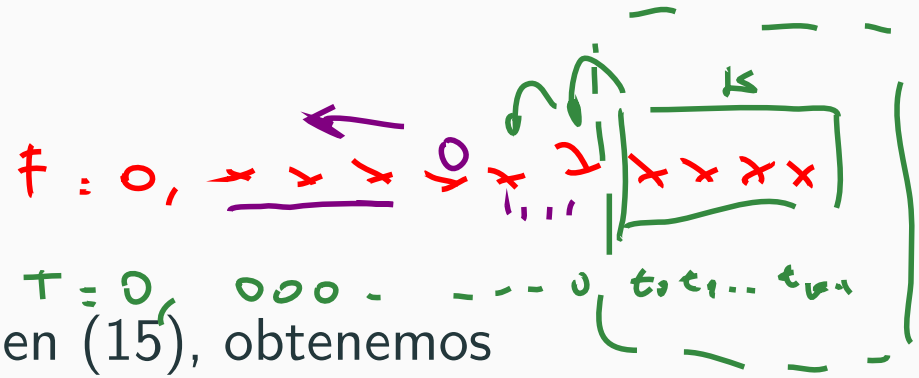
$$D^{-\tau} \leq T < D^{-(\tau-1)}\,. \tag{15}$$

Codificación Aritmética: Codificador

1. Calcular F_n y T_n:

$$F_0 = 0\,, T_0 = 1 \tag{16}$$
$$F_i = F_{i-1} + T_{i-1} C_i[x_i] \tag{17}$$
$$T_i = \left\lfloor T_{i-1} Q_i[x_i] \right\rfloor_K \tag{18}$$

2. $L = \tau_n + 1$
3. $W = \left\lfloor F_n \right\rfloor_L + D^{-L}$
4. Emitir L dígitos de W



Observación: Tomando logaritmo en (15), obtenemos $\tau_n \geq -\log_D T_n > \tau_n - 1$, de modo que $\tau_n = \lceil -\log_D T_n \rceil$. El cálculo de L es análogo al cálculo de ℓ en el código de Shannon-Fano-Elias.

Codificación Aritmética: Decodificador

$G_0 = 0, w_1 w_2 w_3 \ldots w_L w_1' w_2' \ldots w_i'$

el número que representa !?

1. Sea G_0 la secuencia de entrada truncada al máximo valor posible de L (ver Práctico).
2. Sea $U_0 = 1$.
3. Calcular $\tilde{x}_i$, $i = 1 \ldots n$:

$$\tilde{x}_i = \text{máx}\left\{ b \in \mathcal{X} : C_i[b] \leq \frac{G_{i-1}}{U_{i-1}} \right\} \quad (19)$$

$$G_i = G_{i-1} - U_{i-1} C_i[\tilde{x}_i] \quad (20)$$

$$U_i = \left\lfloor U_{i-1} Q_i[\tilde{x}_i] \right\rfloor_K \quad (21)$$

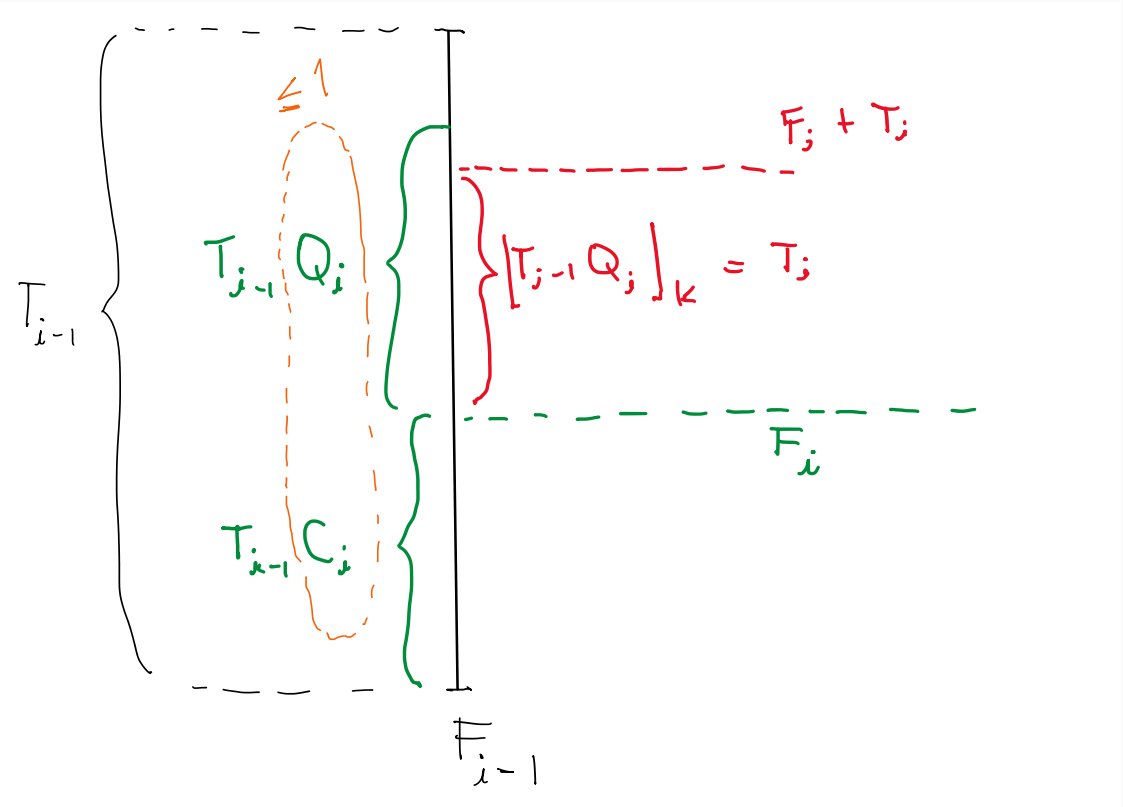
4. Devolver $\tilde{x}^n$

Codificación Aritmética - Intervalos anidados

Lemma

Para todo par de enteros i, k tales que $i \geq k \geq 0$ se cumple que

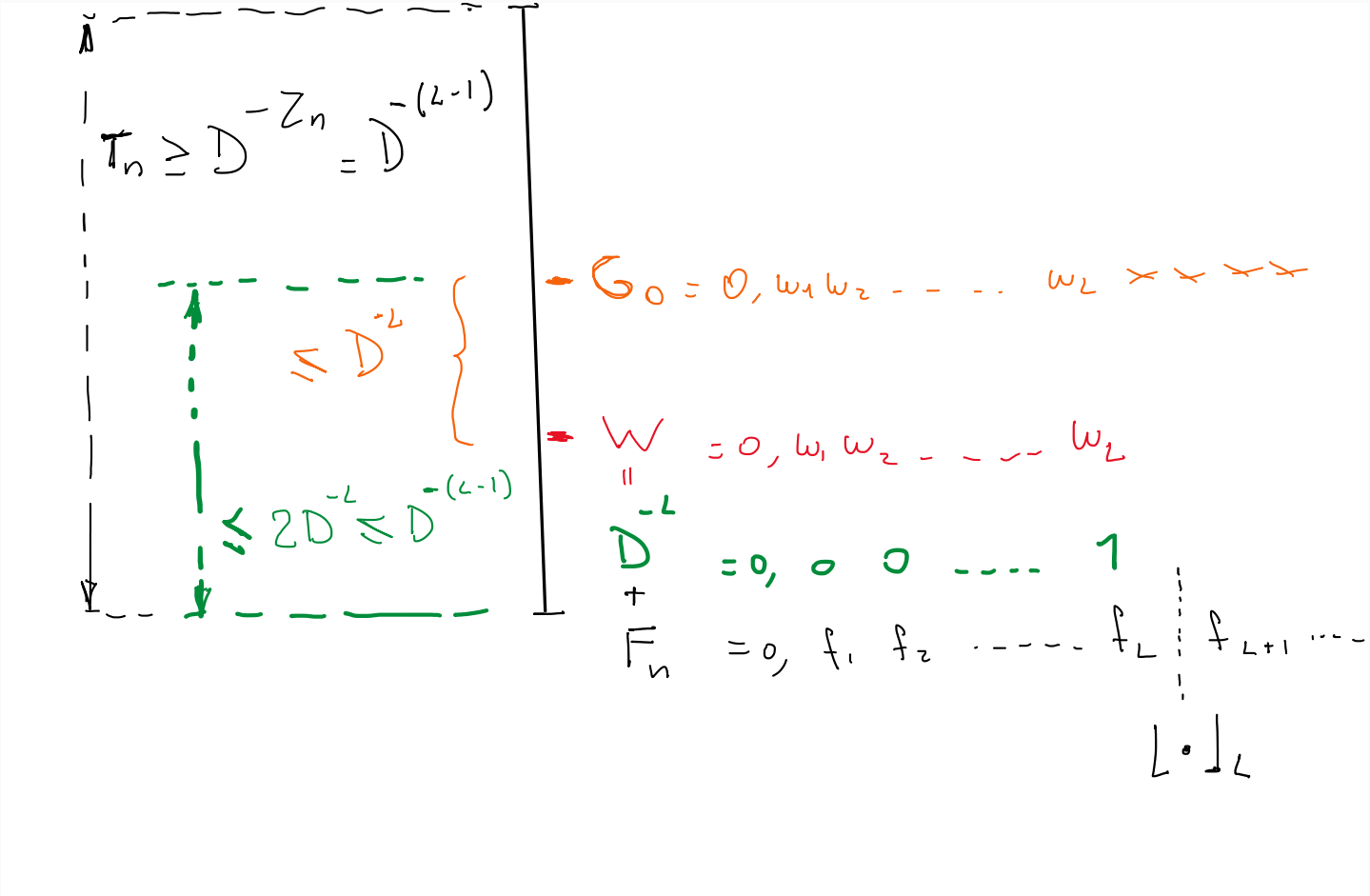
$$\Big[F_i, F_i + T_i\Big) \subseteq \Big[F_k, F_k + T_k\Big). \tag{22}$$



Codificación Aritmética - $G_0 \in \left[F_n, F_n + T_n\right)$

Lemma

Para todo i, $0 \leq i \leq n$, *se cumple* $G_0 \in \left[F_i, F_i + T_i\right)$.



Codificación Aritmética - Corrección ($\tilde{x}^n = x^n$)

- Probamos por inducción en i que para cada i, $1 \leq i \leq n$,

$$U_i = T_i \,, \tag{23}$$

$$U_{i-1}\, C_i[x_i] \leq G_{i-1} < U_{i-1}\Big(C_i[x_i] + Q_i[x_i] \Big) \,. \tag{24}$$

- Observar que (24) implica que en (19) el decodificador selecciona el símbolo $\tilde{x}_i = x_i$.
- Para $i = 1$, (24) es

$$\underbrace{U_0}_{1}\, \underbrace{C_1[x_1]}_{F_1} \leq G_0 < \underbrace{U_0}_{1} \Big(\underbrace{C_1[x_1]}_{F_1} + \underbrace{Q_1[x_1]}_{\geq T_1} \Big) \,, \tag{25}$$

que se verifica por el lema anterior, implicando que $\tilde{x}_1 = x_1$ y, en consecuencia, $U_1 = T_1$.

Codificación Aritmética - Corrección ($\tilde{x}_i = x_i,\ i > 1$)

- Para $i > 1$, asumiendo la hipótesis de inducción, obtenemos

$$G_{i-1} = G_0 - \sum_{j=1}^{i-1} C_j[\tilde{x}_j]\, U_{j-1} = G_0 - \sum_{j=1}^{i-1} C_j[x_j]\, T_{j-1} = G_0 - F_{i-1}\,.$$

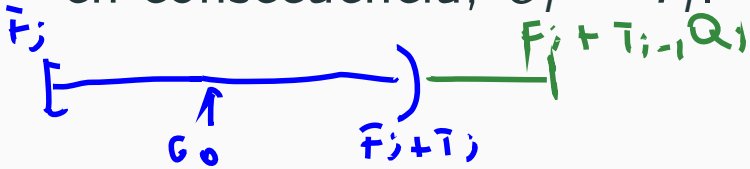
- Entonces, (24)

$$\underbrace{U_{i-1}}_{T_{i-1}}\, C_i[x_i] \leq \underbrace{G_{i-1}}_{G_0 - F_{i-1}} < \underbrace{U_{i-1}}_{T_{i-1}} \Big(C_i[x_i] + Q_i[x_i] \Big)\,,$$

es equivalente a

$$\underbrace{F_{i-1} + T_{i-1}\, C_i[x_i]}_{F_i} \leq G_0 < \underbrace{F_{i-1} + T_{i-1}\, C_i[x_i]}_{F_i} + \underbrace{T_{i-1}\, Q_i[x_i]}_{\geq T_i}\,, \qquad (*)$$

que se verifica por el lema anterior, implicando que $\tilde{x}_i = x_i$ y, en consecuencia, $U_i = T_i$.



Como $G_0 \in [F_i,\ F_i + T_i)$
$\Rightarrow$ G_0 cumple $(*)$

Cota inferior para el ancho de intervalos

Lemma

Para todo $i = 1 \dots n$ se cumple

$$T_{i-1} Q_i[x_i] \left(1 - D^{1-K}\right) \leq T_i \,, \tag{26}$$

Demostración.

$$T_i = \overbrace{0, \underbrace{00 \dots 0 t_0}_{\tau_i} \underbrace{t_1 \dots t_{K-1}}_{K-1} \Big| \underbrace{tt \dots t}_{\text{truncado}}}^{T_{i-1} Q_i[x_i]}$$

$$T_{i-1} Q_i[x_i] - T_i \leq D^{-(\tau_i + K - 1)} = D^{1-K} D^{-\tau_i} \leq D^{1-K} T_{i-1} Q_i[x_i] \,.$$

□

Largo de código en función de Q y K

Theorem

El largo de código $L(x^n)$ para cualquier secuencia x^n satisface

$$\frac{L(x^n)}{n} \leq -\frac{\log_D Q(x^n)}{n} + \frac{2}{n} + \nu_D(K)\,, \tag{27}$$

y $\nu_D(K) = -\log_D\left(1 - D^{1-K}\right)$ decrece exponencialmente con K.

Demostración de (27).
Tomando logaritmos sobre (26) obtenemos

$$\log_D T_{i-1} - \log_D T_i \leq -\log_D Q_i[x_i] + \nu_D(K)\,. \tag{28}$$

Sumando para $i = 1 \ldots n$ y recordando que $T_0 = 1$, obtenemos

$$\underbrace{-\log_D T_n}_{\geq L-2} \leq -\log_D Q(x^n) + n\nu_D(K)\,, \tag{29}$$

Esperanza de largo de código

Corollary
Sea P una distribución de probabilidad sobre $\mathcal{X}^n$ y X^n una secuencia aleatoria generada según P. Entonces, el largo medio de código normalizado satisface

$$\frac{E[L(X^n)]}{n} \leq \frac{H_D(X^n)}{n} + \frac{D_D(P||Q)}{n} + \frac{2}{n} + \nu_D(K)\,. \tag{30}$$

Precisión numérica para la representación de Q

Theorem
Sea P una distribución de probabilidad sobre $\mathcal{X}^n$ tal que todas las secuencias tienen probabilidad positiva y sea

$$P_{\text{mín}} = \min_{x^i \in \mathcal{X}^i, 1 \leq i \leq n} \{P(x_i|x^{i-1})\}.$$

Entonces, para todo δ, $0 < \delta < 1$, si la cantidad de dígitos de precisión usados en la representación de $Q_i[m]$ satisface

$$J \geq \lceil -\log_D P_{\text{mín}} - \log_D \delta + 1 \rceil,$$

entonces existe una elección de $Q_i[\cdot]$ tal que

$$\frac{D_D(P||Q)}{n} < \delta$$

.

Precisión numérica para la representación de Q

La demostración es constructiva. Definimos

- $Q_i[a] = \lfloor P(a|x^{i-1}) \rfloor_J$ para $a < M$,
- $Q_i[M] = 1 - \sum_{a<M} Q_i[a]$