Brassard, Bratley 10.6

* Multiplicación de matrices.

¿ $C = AB$?

- Algoritmo seguro $n^3 \rightarrow n^{2.57}$ (Strassen)
- $C \neq AB \Rightarrow D = AB - C \neq 0 \Rightarrow \exists i : D[i,\cdot] \neq 0$
- $S \subseteq 1..n \qquad \Sigma_{(S)}(D) = \sum_{i \in S} D(i,\cdot)$
- $S \leftrightarrow S' \qquad S' = S \Delta \{i\} \Rightarrow \Sigma_{(S)}(D) \neq 0 \vee \Sigma_{(S')}(D) \neq 0$
- S elegido al azar prob $(i \in S) = 1/2 \Rightarrow$ prob $(\Sigma_{(S)}(D) \neq 0) \geq 1/2$
- $C = AB \Rightarrow \Sigma_S(D) = 0 \Rightarrow$ prob $(\Sigma_S(D) \neq 0) = 0$.
- $\Sigma_S(D) = \chi_S \cdot D = \chi_S \cdot (AB - C)$
- Estudiamos si $\chi_S AB = \chi_S C$ (tiempo n^2)

  Devolvemos falso si no son iguales

  cierto si son iguales (tras repetir k veces)

- Error sólo si $\neq$ y con probabilidad $\leq 1/2^k$.

---

* Test de primalidad.

- Tma. de Fermat primo $(n) \Rightarrow a^{n-1} \bmod n = 1 \quad \forall a \in 1..n-1$

  Contrarrecíproco.

- Elegimos a uniformemente y calculamos $a^{n-1} \bmod n$

  $\neq 1 \Rightarrow \neg$ primo (n)

  Demasiada prob de falsos testigos en algunos casos.

- impar $(n) \Rightarrow n-1 = 2^s \cdot t \quad s > 0$, impar (t)
- $B(n) = \{ a \in 2..n-2 \mid (a^t \bmod n \neq 1) \vee (\exists i \in 0..s-1 \; a^{2^i t} \bmod n = n-1) \}$
- Ext. Tma de Fermat primo $(n) \Rightarrow B(n) = 2..n-2$

  Falsos testigos fuertes $\neg$ primo $(n) \Rightarrow |B(n)| \leq \frac{n-9}{4}$

  Prob error (impar $(n) \wedge n > 3$) $\leq 1/4$

- Algoritmo 3/4 - correcto $\Rightarrow$ Amplificación ventaja estocástica
- Coste $O(\log n \cdot \log^2 n \cdot \log 1/\varepsilon)$

Amplificación de la ventaja estocástica

- Algoritmos no sesgados : pueden equivocarse dando cualquier respuesta.
- Mínima cota del error $< 1/2$. Ventaja estocásica $p - 1/2$
- Determinación del valor democrática tras k repeticiones
- Variable aleatoria de corrección $Pr[X_i = 1] \geq 1/2 + \varepsilon$

$$E(X_i) = 1/2 + \varepsilon \qquad Var(X_i) = 1/4 - \varepsilon^2$$

- Variable acumulada $X = \sum_{i=1}^{k} X_i$

$$Pr(X = i) = \binom{k}{i} (1/2 + \varepsilon)^i (1/2 - \varepsilon)^{k-i}$$

$$E(X) = (1/2 + \varepsilon) \cdot k \qquad Var(X) = (1/4 - \varepsilon^2) k$$

$Pr(X \leq k/2)$?

Tma. Central del Límite = Aproximación por la normal

$$Pr\left(X < E(X) - 1.645 \sqrt{Var(X)}\right) \sim 0.05$$

Tomamos k con $k/2 < E(X) - 1.645 \sqrt{Var(X)}$

$$k > 2.706 \left(\frac{1}{4\varepsilon^2} - 1\right)$$

Número de repeticiones k depende de $1/\varepsilon^2$ y de $\log(1/\delta)$ siendo δ el margen de error que nos damos.