

## CI2612: Algoritmos y Estructuras de Datos II

Blai Bonet

Universidad Simón Bolívar, Caracas, Venezuela

## Algoritmos randomizados

© 2016 Blai Bonet

### Objetivos

- Hacer análisis probabilístico para calcular **tiempo promedio** de algoritmos determinísticos
- Utilizar **randomización** en el diseño de algoritmos
- Hacer análisis probabilístico para calcular **tiempo esperado** de algoritmos randomizados
- Diferencia entre tiempo promedio y tiempo esperado
- Algoritmos tipo Monte Carlo y Las Vegas

© 2016 Blai Bonet

### Problema de empleo (hiring problem)

Considere una compañía que desea contratar un nuevo asistente. La compañía contrata una agencia de empleo la cual envía un candidato cada día

La compañía entrevista al candidato y debe decidir si contratarlo o no después de la entrevista. La agencia de empleo cobra un monto pequeño por cada entrevista y un monto bastante mayor si se contrata

La compañía decide probar  $n$  días la estrategia de siempre contratar si el candidato es mejor que el asistente actual

¿Cuál es el costo promedio de esta estrategia de empleo?

© 2016 Blai Bonet

## Algoritmo de empleo

La estrategia de empleo se puede resumir con el siguiente algoritmo

```
1 Hire-Assistant(int n)
2   best = 0 % candidato 0 es un sentinel
3   for i = 1 to n do
4     Entrevistar al candidato i
5     if i es mejor a best then
6       best = i
7     Contratar al candidato i
```

El **costo promedio** basicamente depende del número promedio de candidatos contratados

## Análisis del algoritmo de empleo

Para analizar el costo promedio, asumimos que todos los candidatos tienen una **calificación diferente** y que son presentados a la compañía de forma **aleatoria**

Calculamos el **costo promedio** en que incurre el algoritmo utilizando variables aleatorias indicadoras

Sea  $X_i = \mathbb{I}\{\text{candidato } i \text{ es contratado}\}$  y  $X = \sum_{i=1}^n X_i$ . Queremos calcular  $\mathbb{E}[X]$  con respecto a la distribución sobre las posibles entradas

$$\begin{aligned}\mathbb{E}[X_i] &= \mathbb{P}(\text{candidato } i \text{ es contratado}) \\ &= \mathbb{P}(\text{candidato } i \text{ es mejor que los candidatos } 1, \dots, i-1) \\ &= \frac{1}{i}\end{aligned}$$

[los primeros  $i$  candidatos aparecen en cualquier order, el  $i$ -ésimo es el mejor con probabilidad  $\frac{1}{i}$ ]

Por lo tanto,  $\mathbb{E}[X] = \sum_{i=1}^n \mathbb{E}[X_i] = \sum_{i=1}^n \frac{1}{i} = \ln n + O(1)$

## Algoritmos randomizados (aleatorizados)

Se dice que un algoritmo es randomizado cuando su ejecución no solo depende de la entrada sino también de los valores producidos por un **generador de números aleatorios**

Asumiremos que todo algoritmo tiene a su disposición una rutina **Random(a,b)** para generar números aleatorios

Una llamada a **Random(a,b)** retorna un número en  $\{a, a+1, \dots, b\}$  seleccionado de forma **aleatoriamente uniforme**

**Random(0,1)** retorna 0 con probabilidad  $\frac{1}{2}$  y 1 con probabilidad  $\frac{1}{2}$ .  
**Random(4,9)** retorna un entero en  $\{4, 5, 6, 7, 8, 9\}$  cada uno con probabilidad  $\frac{1}{6}$

Cada entero generado por **Random** es **independiente** de todos los enteros generados anteriormente

## Espacio de probabilidad para algoritmos randomizados

El espacio de probabilidad  $(\Omega, \mathcal{F}, \mathbb{P})$  asociado a una **ejecución** de un algoritmo randomizado es el espacio donde cada par de eventos  $A$  y  $B$  asociados a **llamadas distintas** a **Random** son independientes:

$$\mathbb{P}(A \cap B) = \mathbb{P}(A) \times \mathbb{P}(B)$$

E.g., si el algoritmo realiza  $n$  llamadas a **Random(0,1)** y solo esas llamadas a **Random** durante su ejecución, el algoritmo basicamente “lanza  $n$  monedas insesgadas e independientes”

En dicho caso,  $\Omega = \{H, T\}^n$  y la medida satisface (entre otras cosas):

$$\mathbb{P}(\{\omega \in \Omega : \omega_i = H\}) = \frac{1}{2} \quad \text{para todo } i = 1, 2, \dots, n$$

## Análisis de algoritmos randomizados

Al hacer el análisis de algoritmos randomizados se debe considerar todas los posibles valores retornados por las llamadas al generador

El algoritmo es correcto ssi es correcto para cualquier valor de los enteros aleatorios

Para el desempeño, calculamos el **tiempo esperado de ejecución** con respecto a la distribución de probabilidad sobre los números aleatorios generados

## Algoritmo randomizado para empleo

Para randomizar el algoritmo cambiamos el modelo y asumimos que la agencia envía a la compañía la lista de los  $n$  candidatos a ser entrevistados

Una manera fácil de randomizar el algoritmo es **permutar aleatoriamente** la lista de candidatos antes de iniciar las entrevistas

**Input:** arreglo  $A$  con candidatos a entrevistar

---

```
1 Randomized-Hire-Assistant(array A)
2   Permutar de forma aleatoria el arreglo A
3   best = 0                                % candidato 0 es un sentinel
4   for i = 1 to A.length do
5     Entrevistar al candidato A[i]
6     if A[i] es mejor a best then
7       best = A[i]
8     Contratar al candidato A[i]
```

---

Por la randomización, el **costo esperado** es igual al **costo promedio** de **Hire-Assistant**; i.e. esperamos realizar  $O(\log n)$  contrataciones

## Sobre la generación de enteros aleatorios

Hasta ahora hemos supuesto que tenemos a nuestra disposición el generador **Random(a,b)**

¿Qué hacemos si no lo tenemos o tenemos algo mas débil?

- Si no tenemos un generador genuino de aleatoriedad, podemos utilizar un **generador de números pseudo-aleatorios**
- Si solo tenemos monedas sesgadas con **Biased-Random(0,1)**, utilizamos **Biased-Random(0,1)** para implementar **Random(0,1)** (Ejercicio 5.1-2)
- Si solo tenemos el generador **Random(0,1)** (i.e. solo podemos “lanzar monedas insesgadas”), utilizamos **Random(0,1)** para implementar **Random(a,b)** (Ejercicio 5.1-3)

## Solo podemos lanzar monedas sesgadas

Considere la rutina **Biased-Random(0,1)** que retorna 0 con probabilidad  $p$  y retorna 1 con probabilidad  $1 - p$  donde  $p$  es fijo

---

```
1 Random(0,1)
2   while true do
3     x = Biased-Random(0,1)
4     y = Biased-Random(0,1)
5     if x == 0 & y == 1 then return 0
6     if x == 1 & y == 0 then return 1
```

---

En una iteración, **Random(0,1)** retorna 0 con probabilidad  $p(1 - p)$  y retorna 1 con probabilidad  $(1 - p)p$ . Ambas probabilidades son iguales por lo que **Random(0,1)** es un generador uniforme sobre  $\{0, 1\}$

## Tiempo esperado de ejecución

Sea  $T$  la v.a. para el tiempo de ejecución (en unidades de tiempo) de  $\text{Random}(0,1)$ . Queremos calcular  $\mathbb{E}[T]$

Como  $T$  es entero y  $T \geq 0$ , utilizamos  $\mathbb{E}[T] = \sum_{t \geq 1} \mathbb{P}(T \geq t)$

Una iteración **falla** si  $x = y$  (ambos 1 o ambos 0). La probabilidad de que eso suceda es  $r = p^2 + (1-p)^2$

$T \geq t$  ssi existen  $t-1$  fallas sucesivas desde el inicio. Como cada iteración es independiente de las otras,  $\mathbb{P}(T \geq t) = r^{t-1}$

Calculamos:  $\mathbb{E}[T] = \sum_{t \geq 1} \mathbb{P}(T \geq t) = \sum_{t \geq 1} r^{t-1} = \sum_{t \geq 0} r^t = \frac{1}{1-r}$

E.g., si  $p = \frac{1}{2}$  entonces  $r = \frac{1}{2}$  y  $\mathbb{E}[T] = 2$ . Si  $p = 0.99$  entonces  $r = 0.9802$  y  $\mathbb{E}[T] = 50.505$

## Solo podemos lanzar monedas

Mostramos como implementar  $\text{Random}(0,b)$  utilizando  $\text{Random}(0,1)$  (implementar  $\text{Random}(a,b)$  usando  $\text{Random}(0,1)$  se deja como ejercicio)

La idea es **generar los bits** del número aleatorio con  $\text{Random}(0,1)$

---

```
1 Random(0,b)
2   n = ⌈log(b+1)⌉
3   while true do
4     x = 0
5     for i = 1 to n do
6       x = 2 * x + Random(0,1)
7     if x <= b then return x
```

---

En una iteración,  $\text{Random}(0,b)$  retorna un  $x \in [0, b]$  si  $x \leq b$ . En otro caso, itera. Como la probabilidad es igual para cualquier  $x$  retornado, la generación es uniforme

## Permutaciones aleatorias de arreglos

Muchos algoritmos randomizados **permutan la entrada** de forma uniforme. Si la entrada es un arreglo, esto equivale a permutar el arreglo de forma tal que cualquier permutación es **equiprobable**

Veremos dos formas de permutar un arreglo  $A$ :

- permutación por ordenamiento
- permutación por intercambio

## 1er Método: Permutación por ordenamiento

La idea es generar una **prioridad** para cada elemento del arreglo y luego ordenar el arreglo utilizando las prioridades como **claves para el ordenamiento**

**Input:** arreglo  $A$  con  $n$  elementos

**Output:** arreglo  $A$  permutado

---

```
1 Permute-By-Sorting(array A)
2   n = A.length
3   let P be new array[n]
4   for i = 1 to n do
5     P[i] = Random(1,n^3)
6   Ordenar A usando P como las claves de los elementos en A
```

---

Si todas las prioridades son distintas, las claves son una permutación uniforme de prioridades y los elementos en  $A$  son permutados de forma uniforme

## Permutación por ordenamiento

¿Por qué las prioridades (claves) se generan en el rango  $\{1, 2, \dots, n^3\}$ ?

Porque con gran probabilidad todas las prioridades serán distintas (serán distintas con **probabilidad al menos**  $1 - \frac{1}{n}$ )

Sea  $p_i$  la v.a. que denota la prioridad del elemento  $A[i]$

$\mathbb{P}(\text{las prioridades no son únicas})$

$$\begin{aligned} &= \mathbb{P}(\exists i, j : p_i = p_j) \\ &\leq \sum_{1 \leq i < j \leq n} \mathbb{P}(p_i = p_j) \quad (\text{cota de unión}) \\ &= \sum_{1 \leq i < j \leq n} \sum_{k=1}^{n^3} \mathbb{P}(p_i = k, p_j = k) \\ &= \sum_{1 \leq i < j \leq n} \sum_{k=1}^{n^3} \mathbb{P}(p_i = k) \times \mathbb{P}(p_j = k) \\ &= \sum_{1 \leq i < j \leq n} \sum_{k=1}^{n^3} \frac{1}{n^3} \times \frac{1}{n^3} \\ &= \sum_{1 \leq i < j \leq n} \frac{1}{n^3} = \binom{n}{2} \frac{1}{n^3} < \frac{1}{n} \end{aligned}$$

## 2do Método: Permutación por intercambio

El segundo método es más simple. Consiste en intercambiar cada elemento  $A[i]$  con un elemento al azar en  $A[i \dots n]$

**Input:** arreglo  $A$  con  $n$  elementos

**Output:** arreglo  $A$  permutado

---

```
1 Permute-By-Swap(array A)
2   n = A.length
3   for i = 1 to n do
4     Intercambiar A[i] con A[Random(i,n)]
```

---

Claramente el algoritmo corre en tiempo  $\Theta(n)$

## Correctitud de permutación por intercambio

### Invariante:

*Al comienzo de cada iteración, el subarreglo  $A[1 \dots i-1]$  contiene una  $(i-1)$ -permutación con probabilidad uniforme*

**Inicialización:** en la primera iteración,  $i = 1$  y el invariante dice que  $A[1 \dots 0]$  contiene una 0-permutación con probabilidad uniforme. En dicha iteración,  $A[1 \dots 0]$  es la única 0-permutación válida, la permutación vacía

## Correctitud de permutación por intercambio

### Invariante:

*Al comienzo de cada iteración, el subarreglo  $A[1 \dots i-1]$  contiene una  $(i-1)$ -permutación con probabilidad uniforme*

**Mantenimiento:** asuma que estamos por comenzar la  $i$ -ésima iteración y que el invariante es cierto. Sea  $\langle x_1, x_2, \dots, x_{i-1} \rangle$  la permutación en  $A[1 \dots i-1]$  y  $E_{i-1}$  el evento  $A[1 \dots i-1] = \langle x_1, \dots, x_{i-1} \rangle$ . Por el invariante,  $\mathbb{P}(E_{i-1}) = 1/\binom{n}{i-1}(i-1)! = (n-i+1)/n!$

La iteración intercambia  $A[i]$  con  $A[j]$  para  $j = \text{Random}(i, n)$ . Denote  $A[1 \dots i] = \langle x_1, \dots, x_i \rangle$  al final de la iteración y sea  $E_i$  el evento para el cual el algoritmo construye  $\langle x_1, \dots, x_i \rangle$  y  $S$  el evento de escoger el índice  $j$  para intercambiar con  $A[i]$

$$\mathbb{P}(E_i) = \mathbb{P}(S \cap E_{i-1}) = \mathbb{P}(S|E_{i-1}) \times \mathbb{P}(E_{i-1}) = \frac{1}{n-i+1} \times \frac{(n-i+1)!}{n!} = \frac{(n-i)!}{n!}$$

## Correctitud de permutación por intercambio

### Invariante:

Al comienzo de cada iteración, el subarreglo  $A[1 \dots i - 1]$  contiene una  $(i - 1)$ -permutación con probabilidad uniforme

**Terminación:** el lazo termina cuando  $i = n + 1$ . Al finalizar el invariante dice que la permutación en  $A[1 \dots n]$  es una  $n$ -permutación cualquiera con probabilidad  $\frac{1}{n!}$

Entonces podemos concluir que el **algoritmo es correcto**

## Verificación probabilística de productos de matrices

Queremos diseñar un algoritmo que dadas tres matrices cuadradas con coeficientes en los enteros  $A$ ,  $B$  y  $C$ , verifique si  $A \times B = C$

(Nota: la restricción a matrices cuadradas no es necesaria)

Una forma es calcular el producto  $A \times B$  y comparar con  $C$ . Pero queremos un algoritmo mas eficiente

Veremos que la verificación puede hacerse en tiempo  $O(n^2)$  con gran precisión utilizando un **algoritmo randomizado**

**IDEA:** generar un vector aleatorio  $z$ , computar  $A \times (B \times z)$  y  $C \times z$ , y comparar los resultados. Si  $A \times B = C$ , ambos resultados son iguales. Si  $A \times B \neq C$ , **esperamos** que ambos resultados sean diferentes

## Algoritmo de Freivalds (1977)

**Input:** matrices  $A$ ,  $B$  y  $C$  de dimensión  $n \times n$

**Output:** **true** si  $A \times B = C$ , **false** en otro caso

```
1 Verify-Product(matrix A, matrix B, matrix C)
2   n = A.nrows
3   let z be new matrix[n][1]      % vector columna de dimensión n x 1
4   for i = 1 to n do
5     z[i] = Random(0,1)           % construimos vector aleatorio
6   y = B x z
7   x1 = A x y
8   x2 = C x z
9   return x1 == x2                % chequea si A x (B x z) = C x z
```

- El algoritmo corre en tiempo  $\Theta(n^2)$
- Si  $A \times B = C$ , **Verify-Product**( $A, B, C$ ) retorna **true**
- Si  $A \times B \neq C$ , **Verify-Product**( $A, B, C$ ) puede o no retornar **false** (i.e. el algoritmo puede cometer errores)

## Errores en algoritmos randomizados

El algoritmo de Freivalds es un ejemplo de algoritmo **Monte Carlo**: un algoritmo randomizado que puede cometer errores

Algoritmos randomizados que siempre hacen lo correcto se conocen como tipo **Las Vegas**

- **Permute-By-Sorting**( $A$ ) es un algoritmo tipo Monte Carlo
- **Permute-By-Swap**( $A$ ) es un algoritmo tipo Las Vegas
- **Verify-Product**( $A, B, C$ ) es un algoritmo tipo Monte Carlo

## Error en algoritmo de Freivalds

Si  $A \times B = C$ , el algoritmo siempre retorna **true** y no existe error

Si  $A \times B \neq C$ , el algoritmo erra cuando  $(A \times B) \times z = C \times z$  donde  $z \in \{0, 1\}^n$  es el vector aleatorio construido por el algoritmo

Sea  $D = A \times B - C = (d_{ij})$ . Como  $A \times B \neq C$ , debe existir un coeficiente en  $D$  distinto de 0. Sea  $d_{ij} \neq 0$  y defina  $x = D \times z$  dado por

$$x_i = \sum_{k=1}^n d_{ik} z_k = d_{i1} z_1 + d_{i2} z_2 + \dots + d_{in} z_n = d_{ij} z_j + y$$

Calculamos,

$$\mathbb{P}(x_i = 0 | y = 0) = \mathbb{P}(d_{ij} z_j = 0) = \mathbb{P}(z_j = 0) = \frac{1}{2}$$

$$\mathbb{P}(x_i = 0 | y \neq 0) = \mathbb{P}(z_j = 1 \wedge d_{ij} = -y) \leq \mathbb{P}(z_j = 1) = \frac{1}{2}$$

## Error en algoritmo de Freivalds

Si  $A \times B = C$ , el algoritmo siempre retorna **true** y no existe error

Si  $A \times B \neq C$ , el algoritmo erra cuando  $(A \times B) \times z = C \times z$  donde  $z \in \{0, 1\}^n$  es el vector aleatorio construido por el algoritmo

Sea  $D = A \times B - C = (d_{ij})$ . Como  $A \times B \neq C$ , debe existir un coeficiente en  $D$  distinto de 0. Sea  $d_{ij} \neq 0$  y defina  $x = D \times z$  dado por

$$x_i = \sum_{k=1}^n d_{ik} z_k = d_{i1} z_1 + d_{i2} z_2 + \dots + d_{in} z_n = d_{ij} z_j + y$$

Finalmente,

$$\begin{aligned} \mathbb{P}(x_i = 0) &= \mathbb{P}(x_i = 0, y = 0) + \mathbb{P}(x_i = 0, y \neq 0) \\ &= \mathbb{P}(x_i = 0 | y = 0) \mathbb{P}(y = 0) + \mathbb{P}(x_i = 0 | y \neq 0) \mathbb{P}(y \neq 0) \\ &\leq \frac{1}{2} [\mathbb{P}(y = 0) + \mathbb{P}(y \neq 0)] = \frac{1}{2} \end{aligned}$$

$$\mathbb{P}(\text{error}) = \mathbb{P}(x_1 = 0 \wedge x_2 = 0 \wedge \dots \wedge x_n = 0) \leq \mathbb{P}(x_i = 0) \leq \frac{1}{2}$$

## Amplificación mediante ejecuciones independientes

La **garantía**  $\mathbb{P}(\text{error}) \leq \frac{1}{2}$  para el algoritmo de Freivalds parece pobre, aunque la garantía es **independiente** de la dimensión  $n \times n$

Podemos **amplificar** esta garantía corriendo el algoritmo de Freivalds múltiples veces

Si corremos el algoritmo de Freivalds  $k$  veces sobre la misma entrada y retornamos **true** ssi todas las corridas devuelven **true**, entonces obtenemos un algoritmo cuya probabilidad de error es  $\leq \frac{1}{2^k}$

Para **constante**  $k$  moderada, e.g.  $k = 50$ , obtenemos un **algoritmo confiable de verificación** que corre en tiempo  $\Theta(kn^2) = \Theta(n^2)$

**No se conoce ningún algoritmo determinístico que realice la verificación del producto en tiempo  $O(n^2)$**

## Resumen

- Un algoritmo es randomizado cuando hace llamadas a un generador de números aleatorios: **Random(p, q)**
- Diferencia entre tiempo promedio de un algoritmo determinístico y tiempo esperado de un algoritmo randomizado (también podemos hablar de tiempo promedio de un algoritmo randomizado y aquí hablamos del tiempo esperado cuando promediamos sobre la aleatorización dentro del algoritmo y la aleatorización de las entradas)
- Análisis probabilístico para calcular tiempos promedio y esperado de algoritmos
- Algoritmo de Freivalds y poder de la randomización

## Ejercicios (1 de 4)

1. (5.1-2) Implemente el procedimiento `Random(a,b)` utilizando el procedimiento `Random(0,1)`. Calcule el tiempo esperado de `Random(a,b)` en función de  $a$  y  $b$ .
2. (5.2-1) Para `Hire-Assistant`, asumiendo que los candidatos se presentan en orden aleatorio, ¿cuál es la probabilidad de que solo se contrate a un candidato? ¿cuál es la probabilidad que se contraten los  $n$  candidatos?
3. (5.2-1) Para `Hire-Assistant`, asumiendo que los candidatos se presentan en orden aleatorio, ¿cuál es la probabilidad de que solo se contraten a dos candidatos?
4. Obtenga una versión Las Vegas del algoritmo `Permute-By-Sorting` para permutar arreglos

## Ejercicios (2 de 4)

5. (5.3-2) ¿Cuál es el problema con el siguiente algoritmo para permutar de forma aleatoria un arreglo  $A$ ?

---

```
1 Permute-Without-Identity(array A)
2   n = A.length
3   for i = 1 to n-1 do
4     Intercambiar A[i] con A[Random(i+1,n)]
```

---

6. (5.3-3) ¿Produce el siguiente algoritmo una permutación aleatoria uniforme?

---

```
1 Permute-With-All(array A)
2   n = A.length
3   for i = 1 to n do
4     Intercambiar A[i] con A[Random(1,n)]
```

---

## Ejercicios (3 de 4)

7. (5.3-7) Suponga que queremos crear un subconjunto aleatorio uniforme de tamaño  $m$  a partir de un conjunto de  $m$  elementos (cada subconjunto debe tener probabilidad de ser retornado igual a  $1/\binom{n}{m}$ ). Una forma de hacerlo es generar una permutación aleatoria uniforme de los  $n$  elementos y retornar los primeros  $m$  elementos. Esto requiere generar  $n$  números aleatorios y puede ser ineficiente cuando  $m \ll n$ . Muestre que el siguiente algoritmo recursivo construye un  $m$ -subconjunto aleatorio uniforme de  $\{1, 2, \dots, n\}$  generando solo  $m$  números aleatorios

---

```
1 Random-Sample(int m, int n)
2   if m == 0 then
3     return {}
4   else
5     S = Random-Sample(m-1, n-1)
6     i = Random(1,n)
7     if i ∈ S then
8       return S ∪ {n}
9     else
10      return S ∪ {i}
```

---

## Ejercicios (4 de 4)

8. Solucionar problema 5-2 del libro