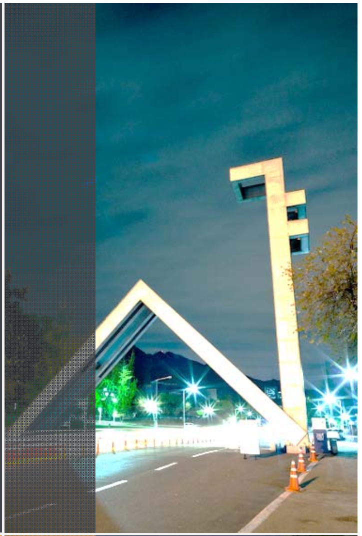
Seoul
National
University



Introduction

Date

Name: Chong-kwon Kim

SCONE

Lab.

Simpson's Paradox

- Bob's GPAs in both Spring semester and Fall semester are better than Alice's GPAs in the same semesters. However, Alice's GPA is higher than Bob's.

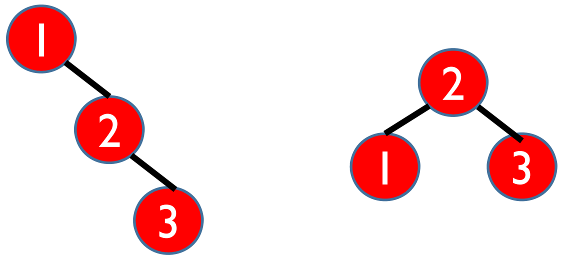
	'18 Spring		'18 Fall		'18	
	GPA	Credits	GPA	Credits	GPA	Credit
Alice	3.5	5	4.0	20		25
Bob	3.7	20	4.1	5		25

- Do not believe anything blindly. Doubt everything.

Descartes Said "Cogito, ergo sum"
Originally, "Dubito, ergo cogito, ergo sum"

Computing & Probability

- Computer Science broadly uses the knowledge of probability & statistics in developing algorithms
  - Machine learning
  - Big data analyses
  - Networks, systems, ..
- Randomized algorithms
  - Use randomness in performing their procedures
  - Example: Select pivot elements randomly (Quick sort)
- Probabilistic analysis of algorithms
  - The performance of many algorithms depends on input
  - Average (or worst case) performance considering input probability
  - Example: BST (Binary Search Tree)



Probability Space

Sample Spaces (Ω)

- Set of all possible outcomes of an experiment (random process)
- Examples
  - Coin flip: Ω = {Head, Tails}
  - Flipping two coins: Ω = {(H, H), (H, T), (T, H), (T, T)}
  - Roll of 6-sided die: Ω = {1, 2, 3, 4, 5, 6}
  - # CacaoTalk msgs in a day: $\Omega = \{x \mid x \in \mathbf{Z}, x \geq 0\}$
  - Hearthstone hrs. in day: $\Omega = \{x \mid x \in \mathbf{R}, 0 \leq x \leq 24\}$

Event (E)

- Subset of Ω ($E \subseteq \Omega$)
- Examples
  - Coin flip is head: E = {Head}
  - At leat one head on 2 coin flips: E = {(H, H), (H, T), (T, H)}
  - Roll of die is 3 or less: E = {1, 2, 3}
  - # CacaoTalk msgs in a day ≤200: $E = \{x \mid x \in \mathbf{Z}, 0 \leq x \leq 200\}$
  - Wasted time (≥ 5 hrs.): $E = \{x \mid x \in \mathbf{R}, 5 \leq x \leq 24\}$

Axioms of Probability

- **Probability function**, Pr: $E \rightarrow \mathbf{R}$
  - Relative frequency of event

$$\Pr(E) = \lim_{n\to\infty} \frac{n(E)}{n}$$

- **Axioms of Probability**

A1: $0 \le \Pr(E) \le 1$

A2: $Pr(\Omega) = 1$

A3: If E_1 and E_2 are mutually exclusive ($E_1 \cap E_2 = \emptyset$),

then $Pr(E_1 \cup E_2) = Pr(E_1) + Pr(E_2)$

→For any sequence of pairwise mutually disjoint events $E_1, E_2, \cdots, E_n$

$$Pr(\cup_{i=1}^{n} E_i) = \sum_{i=1}^{n} Pr(E_i)$$

Lemmas

- From the axioms, we can easily derive following Lemmas
- Lemma 1.0
  - If $E \subseteq F$ then $\Pr(E) \le \Pr(F)$
  - $\Pr(\bar{E}) = 1 - \Pr(E)$
- Lemma 1.1
  - For any events E_1 & E_2
    $Pr(E_1 \cup E_2) = Pr(E_1) + Pr(E_2) - Pr(E_1 \cap E_2)$
- Lemma 1.2:
  - For any sequence of events E_i
  - $Pr(\bigcup_{i\ge1} E_i) \le \sum_{i\ge1} Pr(E_i)$
- Lemma 1.3: *Inclusion-exclusion principle*
  - $Pr(\bigcup_{i=1}^{n} E_i) = \sum_{i=1}^{n} Pr(E_i) - \sum_{i<j} Pr(E_i \cap E_j) + \cdots$
    $(-1)^{l+1} \sum_{i_1<i_2<\cdots<i_l} Pr(\bigcap_{r=1}^{l} E_{i_r}) + \cdots$

Equally Likely Outcomes

- Some sample spaces consist of equally likely outcomes
- Examples
  - (Fair) Coin flip: Ω = {Head, Tails}
  - Flipping two coins: Ω = {(H, H), (H, T), (T, H), (T, T)}
  - Roll of 6-sided die: Ω = {1, 2, 3, 4, 5, 6}
  - Birthday: Ω = {1, 2, …, 365}

- Pr(Each outcome) = $\frac{1}{|\Omega|}$
- Pr(E) = $\frac{|E|}{|\Omega|}$
  - Where $|E|$ = number of outcomes in E and
    $|\Omega|$ = number of outcomes in Ω

Birthday Problem

- What is the probability that none of *n* people share the same birthday?
- |Ω| = ?
- |E| = ?
- Pr(no matching birthdays)

  $= (365)(364)\ldots(365 - n + 1)/(365)^n$
- Cases
  - *n*= 23: Pr(no matching birthdays) < ½ (least such *n*)
  - *n*= 75: Pr(no matching birthdays) < 1/3,000
  - *n*= 100: Pr(no matching birthdays) < 1/3,000,000

Verifying Polynomial Identities

SCONE Lab.

- **Problem**
  - Verify if $F(x) \equiv G(x)$
  - Where F(x) is given in a product of monomials form and
    G(x) is given in a canonical form
- **Example**
  - $F(x) = (x+1)(x-2)(x+3)(x-4)(x+5)(x-6)$
  - $G(x) = x^6 - 7x^3 + 25$
- **Deterministic method**
  - Convert F(x) to a canonical form and check if all coefficients are the same
- **Complexity**
  - If $F(x) = \prod_{i=1}^{d}(x - a_i)$ then it takes $\Theta(d^2)$ where *d* is the degree of the polynomial

Randomized Algorithm - Background

- If F(x) = G(x)
  - ➔ For all integers *r*, F(*r*) = G(*r*)
- Suppose F(x) ≠ G(x)
  - Compute F(r) and G(r) for a randomly selected integer r
  - Case 1: F(*r*) ≠ G(*r*) ➔ F(x) ≠ G(x)
  - Case 2: F(*r*) = G(*r*) ➔ F(x) = G(x) **Wrong Decision!!**
- What is the probability of making a wrong decision?
- Consider F(x) – G(x)
  - There are at most *d* roots that yield F(x) - G(x) = 0

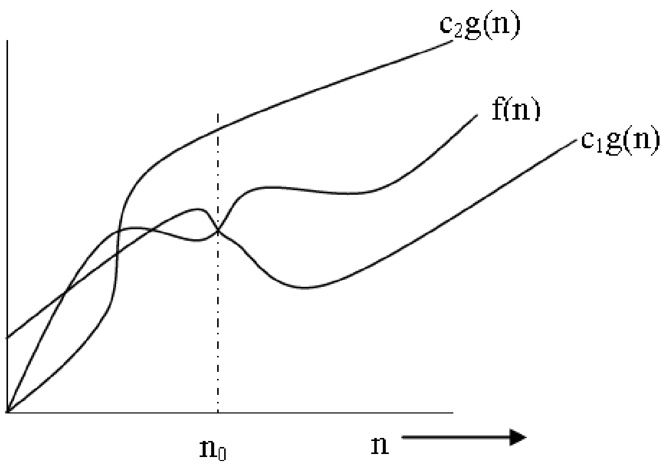
Randomized Algorithm

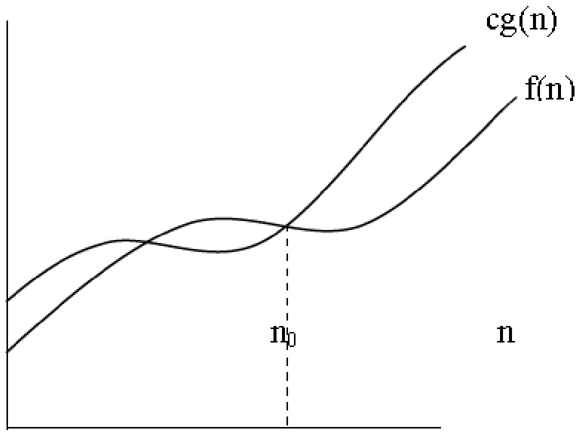
- Simple randomized algorithm
  - Select a number *r*, uniformly at random from $\Omega = \{1, 2, \ldots, 100d\}$
  - If F(r) = G(r), then conclude that F(x) = G(x)

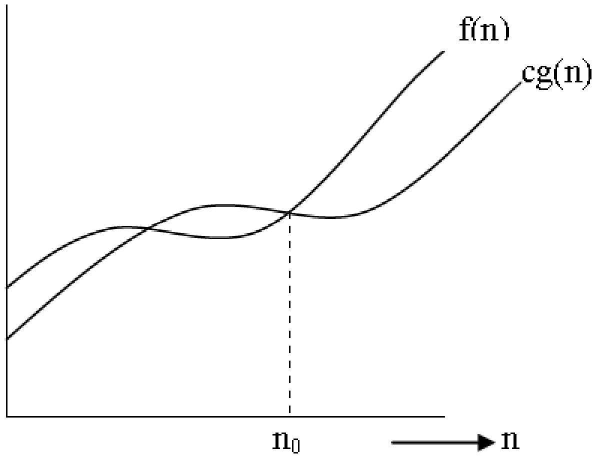
- Analysis of the simple randomized algorithm
  - Probability of making wrong decision
    - Pr(Wrong Decision) = Pr(r is one of roots) ≤ $\frac{d}{100d} = \frac{1}{100}$

- How do you improve the simple algorithm?
  - Increase the sample space to {1, 2, ..., 1000d}
  - Any other methods?

Approximate Bounds







Asymptotically Tight Bound
$\Theta(g(n)$

Asymptotic Upper Bound
$O(g(n))$

Asymptotic Lower Bound
$\Omega(g(n))$

Upper Bound
$o(g(n))$

Lower Bound
$\omega(g(n))$

Ref:
1. https://www2.cs.arizona.edu/classes/cs345/summer14/files/bigO.pdf
2. CLRS " Int. to Algorithms" 3rd Ed. MIT Press, Chapter 3.