Randomized Algorithms

Andreas Klappenecker

Randomized Algorithms

A randomized algorithm is an algorithm that makes random choices during its execution.

A randomized algorithm uses values generated by a random number generator to decide the next step at several branches of its execution.

Therefore, the steps taken by a randomized algorithm might differ from execution to execution, even if the input remains the same.

Why Randomization?

Randomization can lead to simple algorithms that are easy to implement.

Randomization can lead to efficient implementations.

Running Time

The designer of a randomized algorithm must determine what kind of running time one can expect.

The running time is now a random variable, and one needs tools from probability theory to estimate it.

Motivation (1)

Suppose that a company has several servers containing its database. The database is stored in several locations (e.g. east coast and west coast).

At the end of the business day, the company wants to verify that the copies of the databases are still consistent. Transmission of the data is not feasible. How can we whether the content is the same?

Motivation (2)

Suppose we have implemented an extremely fast algorithm to multiply very large matrices (e.g. of dimension 100,000x100,000).

How can we verify whether the computation was correct?

Motivation (3)

In the RSA key exchange, we need to form the product of two very large primes (each having 1000 digits or more).

How can we efficiently check whether a number is prime?

Basics from Probability Theory

Sample Spaces

The possible outcomes of an experiment are called the sample space Ω.

Examples:

- coin tossing: sample space $\Omega=\{\text{head}, \text{tail}\}$.
- rolling a die: sample space $\Omega=\{1,2,3,4,5,6\}$.

σ-Algebra

A probability measure is not necessarily defined on all subsets of the sample space, but only on those that are considered events. We will have a uniform way of reasoning about event by requiring that they form a σ-algebra.

A σ-algebra F is a collection of subsets of a sample space Ω such that

- the empty set is contained in F,
- if E in F, then its complement $E^c = \Omega \backslash E$ is in F,
- a countable union of sets in F is contained in F.

σ-Algebra Example

Let $\Omega = \{1,2,3,4,5,6\}$ the sample space of a die.

Suppose we are interested in the events:

- $D = \{1,2\}$, the value is less than 3.
- $E = \{3,4,5,6\}$, the value is 3 or more.

Then the smallest σ-algebra F containing D and E is given by

$F=\{ \varnothing, D, E, \Omega \}$.

The empty set $\varnothing$ is called the impossible event.

The set Ω is called the certain event.

σ-Algebra

The σ-algebra allows one to talk about

- the impossible event
- complementary event
- the union of events
- the certain event

When rolling a dice, the event that the outcome is an even face value is {2,4,6}. The event that the outcome is a value larger than 4 is {5,6}.

Operations on Events

Let D and E be events. Then

- $D \cup E$ is an event
- $D \cap E$ is an event
- $D \setminus E$ is an event

Indeed, let $E_1=D$, $E_2=E$, and $E_3=E_4=\ldots=\varnothing$. Then

$$\bigcup E_i = D \cup E.$$

The other two properties are also easy to show.

Probability Measure

Let F be a σ-algebra over a sample space Ω. A probability measure on F is a function Pr: F -> [0,1] such that

- the certain event satisfies Pr[Ω]=1,
- if the events E_1, E_2, ... in F are mutually disjoint, then

$$\Pr[\bigcup_{k=1}^{\infty} E_k] = \sum_{k=1}^{\infty} \Pr[E_k]$$

Properties of Probability Measures

Let E be an event. Then

$$1 = \Pr[\Omega] = \Pr[E] + \Pr[E^c],$$

as E and E^c are disjoint.

Therefore, the complementary event E^c has probability

$$\Pr[E^c] = 1 - \Pr[E].$$

In particular, the impossible event has probability

$$\Pr[\varnothing]=1-\Pr[\Omega]=0$$

Properties of Probability Measures

Let D and E be events such that $D \subseteq E$.

Then $Pr[D] <= Pr[E]$.

Why?

Properties of Probability Measures

Let D and E be events. Then

$$\Pr[D \cup E] = \Pr[D] + \Pr[E] - \Pr[D \cap E].$$

Indeed, we have

(a) $\Pr[D] = \Pr[D - (D \cap E)] + \Pr[D \cap E]$,

(b) $\Pr[E] = \Pr[E - (D \cap E)] + \Pr[D \cap E]$.

Since

$\Pr[D \cup E] = \Pr[D - (D \cap E)] + \Pr[E - (D \cap E)] + \Pr[D \cap E]$,

the claim follows from (a) and (b).

Uniform Probability Distribution

Let Ω be a finite sample space.

Let $F = P(\Omega)$ be the σ-algebra consisting of all subsets of Ω.

Then the probability measure $Pr: F \to [0,1]$ defined by

$$Pr[\{s\}] = 1/|\Omega|$$

for all s in Ω is called the uniform probability distribution on Ω.

Continuous Probability Distribution

The continuous uniform probability distribution over an interval [a,b] associates to each subinterval [c,d] of [a,b] the probability

$$\Pr[\,[c,d]\,] = (d-c)/(b-a).$$

Notice that the probability of any event {x} with x in [a,b] is 0, since $\Pr[\,\{x\}\,] = \Pr[\,[x,x]\,] = 0$.

Continuous Probability Distribution

For the sample space Ω = [a,b], one cannot choose the σ-algebra F=P(Ω), since there does not exist any function on P(Ω) = P([a,b]) that satisfies our axioms of a probability measure (unless one assumes unusual axioms for set theory).

Deep Water!

Instead, define F to be the smallest σ-algebra on Ω =[a,b] that contains the intervals [c,d] for all c,d in the range a <= c <= d <= b. Then there exists a function Pr: F -> [0,1] such that Pr[[c,d]] = (d-c)/(b-a). It is called the Borel measure on F.

Union Bound

Let I $\subseteq$ {1,2,3,...}. Let E_i with i in I be a set of events.

These events do not need to be disjoint.

Then the union bound states that

$$\Pr[\bigcup_{i \in I} E_i] \leq \sum_{i \in I} \Pr[E_i]$$

This simple bound is enormously useful, as it is easy to compute.

Conditional Probabilities

Let D and E be events such that Pr[E] >0.

The conditional probability Pr[D|E] is defined as

$$\Pr[D|E] = \frac{\Pr[D \cap E]}{\Pr[E]}$$

One can interpret Pr[D|E] as the probability that the event D occurs, assuming that the event E occurs.

Useful Multiplication Formula

Quite often, it is easy to determine conditional probabilities:

$$\Pr[D \cap E] = \Pr[D|E] \Pr[E]$$

Independent Events

Two events D and E are called independent if and only if

$$\Pr[D \cap E] = \Pr[D] \Pr[E]$$

If D and E are independent, then

$$\Pr[D|E] = \Pr[D]$$

Bayes Formula

Sometimes, we know Pr[D|E], but would like to know Pr[E|D].

Notice that

$$\Pr[D|E]\ \Pr[E] = \Pr[D \cap E] = \Pr[E|D]\Pr[D]$$

Therefore,

$$\Pr[E|D] = \Pr[D|E]\ \Pr[E]/\Pr[D].$$