COMS 633:
Advanced Topics in Computational Randomness

Lecture Notes - Fall 2017

Professor: Dr. Jack Lutz
Notes by: Alex Scheel

Updated: 08-31-2017

1 Introduction

1.1 Overview

These notes were prepared by Alex Scheel; they are not official class notes. Unless otherwise noted, the primary source is lectures by Dr. Jack Lutz.

1.2 Prerequisite Knowledge, Terminology, and Notation

- An extended real number is an element of the set $[-\infty, \infty] = \mathbb{R} \cup \{-\infty, \infty\}$.
- An upper bound of a set $E \subseteq \mathbb{R}$ is an extended real number, u such that $(\forall x \in E)$, $x \leq u$.
- A maximum of a set $E \subseteq \mathbb{R}$ is an element $x \in E$ that is an upper bound of E.
- It is easy to see that a set has at most one maximum, but maybe none.
  - $\mathbb{N}$ has none,
  - $(0, 1) \subset \mathbb{R}$ has none,
  - $[0, 1]$ has one; 1.
- A supremum (or least upper bound) of a set $E \subseteq \mathbb{R}$ is an upper bound u of E with the property that, $(\forall v \in E)$, that is an upper bound of E, $u \leq v$. A set has at most one supremum. A max, if it exists, is a sup.
- **Supremum principle**: Every set $E \subseteq \mathbb{R}$ has a supremum.
- We write *sup* E for the supremum of E.
- The terms lower bound, minimum, and infimum are analogously defined.
- The notation $\forall^\infty$ means "for all but finitely many"; that is, excluding only a finite number of elements.
- The notation $\exists^\infty$ means "there exist infinitely many".

Let $f : \mathbb{N} \to \mathbb{R}$.

- f converges to a real $\alpha \in \mathbb{R}$ if, $(\forall \epsilon > 0)$, and $(\forall^\infty n \in \mathbb{N})$, then $|f(n) - \alpha| < \epsilon$.
- f converges (or diverges) to ∞ if, $(\forall m \in \mathbb{N})$, and $(\forall^\infty n \in \mathbb{N})$, then $f(n) > m$.
- f converges (or diverges) to $-\infty$ if, $(\forall m \in \mathbb{N})$, and $(\forall^\infty n \in \mathbb{N})$, then $f(n) < -m$.
- There is at most one $u \in [-\infty, \infty]$ such that f converges to u.

- Notation: $\lim_{n\to\infty} f(n) = u$.
- f is nondecreasing if, $(\forall n \in \mathbb{N})$, $f(n) \leq f(n+1)$.
- f is strictly increasing if, $(\forall n \in \mathbb{N})$, $f(n) < f(n+1)$.
- f is nonincreasing if, $(\forall n \in \mathbb{N})$, $f(n) \geq f(n+1)$.
- f is strictly decreasing if, $(\forall n \in \mathbb{N})$, $f(n) > f(n+1)$.
- f is monotone if f is nonincreasing or nondecreasing.
- Every monotone function has a limit in $[-\infty, \infty]$.

Definition 1.1. Let $f : \mathbb{N} \to \mathbb{R}$.

1. The limit superior of f as $n \to \infty$ is:

$$\limsup_{n\to\infty} f(n) = \lim_{n\to\infty} \sup_{m\geq n} f(m)$$

2. The limit inferior of f as $n \to \infty$ is:

$$\liminf_{n\to\infty} f(n) = \lim_{n\to\infty} \inf_{m\geq n} f(m)$$

Observations:

1. liminf, limsup always exist.
2. liminf $\leq$ limsup.
3. limit exists $\iff$ $\liminf = \limsup$. Then, $\lim = \liminf = \limsup$.
4. $\liminf_{n\to\infty} f(n) = \infty \iff \lim_{n\to\infty} f(n) = \infty$
5. $\limsup_{n\to\infty} f(n) = \infty \iff$ f is not bounded above, ∞ is the only upper bound of range f.

2 Finite-State Gambling

Let Σ be an alphabet with $2 \leq |\Sigma| < \infty$. That is, Σ is finite. A probability measure on Σ is a function:

$$\pi : \Sigma \to [0, \infty)$$

satisfying:

$$\sum_{a\in\Sigma} \pi(a) = 1$$

A rational probability measure on Σ is a function:

$$\pi : \Sigma \to \mathbb{Q} \cap [0, \infty)$$

that is a probability measure on Σ. We write:

$$\begin{aligned}
&\Delta(\Sigma) = \{\text{probability measures on } \Sigma\} \\
&\Delta_{\mathbb{Q}} = \{\text{rational probability measures on } \Sigma\} \\
&\Delta^{+}(\Sigma) = \{\pi \in \Delta(\Sigma) | (\forall a \in \Sigma) \pi(a) > 0\} \\
&\Delta^{+}_{\mathbb{Q}}(\Sigma) = \{\pi \in \Delta_{\mathbb{Q}}(\Sigma) | (\forall a \in \Sigma) \pi(a) > 0\}
\end{aligned}$$

Note that $\Delta(\Sigma)$ is a $(|\Sigma| - 1)$-dimensional simplex in $\mathbb{R}^{|\Sigma|}$.

Definition 2.1. A finite-state automaton (FSA) on Σ is a triple:

$$A = (Q, \delta, s)$$

where:

$$\begin{aligned} &Q \text{ is a finite set of states,} \\ &\delta : Q \times \Sigma \to Q \text{ is a transition function,} \\ &s \in Q \text{ is a start state.} \end{aligned}$$

Example 2.2. DIAGRAM

Given an FSA, $A = (Q, \delta, s)$ on Σ, we define the extended-transition function:

$$\hat{\delta} : Q \times \Sigma^* \to Q$$

by the recursion:

$$\begin{aligned} \hat{\delta}(q, \lambda) &= q \\ \hat{\delta}(q, wa) &= \delta(\hat{\delta}(q, w), a) \end{aligned}$$

$\forall q \in Q, w \in \Sigma^*$, and $a \in \Sigma$.

Notational Conventions:

1. We write $\delta(q, w)$ for $\hat{\delta}(q, w)$.
2. We write $\delta(w)$ for $\delta(s, w)$.

Our next objective is to endow FSAs with the ability to gamble.

Definition 2.3. A bet on Σ is a rational probability measure $\beta \in \Delta_{\mathbb{Q}}(\Sigma)$.

Intuition: Assume that:

- You have $d \in \mathbb{Q} \cap [0, \infty)$ dollars
- You are confronting an experiment whose outcome is some element of Σ
- You place the bet $\beta \in \Delta_{\mathbb{Q}}(\Sigma)$

This means that $\forall a \in \Sigma$, you are betting $d \cdot \beta(a)$ dollars that the outcome is a. Since $\sum_{a \in \Sigma} d\beta(a) = d$, you have to bet all your money in this scenario. After the bet, if the martingale's outcome was a, you will have $d(a)$, an amount that we now specify.

Suppose that the outcomes of this experiment occur according to a probability measure $\pi \in \Delta(\Sigma)$. What is your expected amount of money after the bet, given that you had d dollars?

Answer:

$$\sum_{a \in \Sigma} \pi(a) d(a) = \mathbb{E}_\pi[d(a)|d]$$

Therefore "the payoffs are fair" if:

$$d = \sum_{a \in \Sigma} \pi(a) d(a)$$

Recall: A bet on Σ is a probability measure $\beta \in \Delta_{\mathbb{Q}}(\Sigma)$. For now, a payoff rule on Σ is a probability measure $\rho \in \Delta(\Sigma)$.

Intuition: Assume that a gambler has $d \in [0, \infty)$ dollars and places a bet, β on an experiment that will have an outcome that is an element of Σ. Placing this bet means that, $(\forall a \in \Sigma)$, the gambler is betting $d\beta(a)$ dollars that the outcome is a. Note that $d = \sum_{a \in \Sigma} d\beta(a)$, so the gambler is required to bet all its money.

If the payoff rule is $\rho \in \Delta(\Sigma)$, and the actual outcome is $a \in \Sigma$, then the gambler will have:

$$d(a) := \frac{\beta(a)}{\rho(a)} \tag{2.1}$$

dollars after the bet.

Now assum that the outcome of the experiment occurs according to a probabilty measure, $\pi \in \Delta(\Sigma)$, which we call the actual probability measure of the experiment. The expected value of the gambler's amount of money after the bet (given that it has d dollars before the bet) is:

$$\mathbb{E}_{a\sim\pi}[d(a)] := \sum_{a\in\Sigma} d(a)\pi(a), \tag{2.2}$$

where $a \sim \pi$ means "a is drawn according to π". By (2.1) and (2.2),

$$\mathbb{E}_{a\sim\pi}[d(a)] = d\sum_{a\in\Sigma} \frac{\beta(a)\pi(a)}{\rho(a)} \tag{2.3}$$

Observation: If $\rho = \pi$, i.e., the payoff rule is the actual probability measure on Σ, then the payoffs are fair in the sense that $\mathbb{E}_{a\sim\pi}[d(a)] = d$.

Definition 2.4. A finite state gambler (FSG) on Σ is a 5-tuple, $G = (Q, \delta, s, \beta, c)$, where:

- (Q, δ, s) is a FSA,
- $\beta : Q \to \Delta_{\mathbb{Q}}(\Sigma)$ is the betting function,
- $c \in \mathbb{Q} \cap [0, \infty)$ is the initial capital.

Example 2.5. DIAGRAM

Intuition:

Before defining the semantics of FSGs formally, let us use example 2.5 to gain some insight. Assume that G is given an input string $w \in \{0,1\}^*$, whose bits are chosen by independent tosses of a fair coin, and asusme that the payoff rule coincides with this. Let $d_G(w)$ denote the amount of money that G has after betting on w. Then:

$$\begin{aligned}
&d_G(\lambda) = c = 1\\
&d_G(1) = \frac{4}{3} = 2\frac{2}{3}d_G(\lambda)\\
&d_G(11) = 2\frac{1}{3}d_G(1) = \frac{8}{9}\\
&d_G(110) = 2\frac{2}{3}d_G(11) = \frac{32}{27}\\
&\ldots
\end{aligned}$$

Definition 2.6. If $G = (Q, \delta, s, \beta, c)$ is an FSG and $\pi \in \Delta^+(\Sigma)$, then the π-martingale of G is the function:

$$d_G^\pi : \Sigma^* \to [0, \infty)$$

defined by the recursion:

$$\begin{aligned}
&d_G^\pi(\lambda) = c\\
&d_G^\pi(wa) = d_G^\pi(w)\frac{\beta(\delta(w))(a)}{\pi(a)}
\end{aligned}$$

Definition 2.7. (Ville - 1939). Let $\pi \in \Delta(\Sigma)$. A π-martingale on Σ is a function:

$$d : \Sigma^* \to [0, \infty)$$

that satisfies, $(\forall w \in \Sigma^*)$:

$$d(w) = \sum_{a \in \Sigma} d(wa)\pi(a) \tag{2.4}$$

Obervation: For every FSG G on Σ and every probability measure $\pi \in \Delta^+(\Sigma)$, d_G^π is a π-martingale.

Intuition: We work in the sequence space Σ^∞ of all (infinite) sequences $S = a_0 a_1 a_2 ...$ of symbols in Σ. For each $S \in \Sigma^\infty$ and $m, n \in \mathbb{N}$, we use the notation $S[m..n]$ for the string consisting of the mth through nth symbols in S.

1. $S[0]$ is the left most symbol in S.
2. If $m > n$, then $S[m..n] = \lambda$.

We call a string $w \in \Sigma^*$ a prefix of $S \in \Sigma^\infty$ if $S[0..|w| - 1] = w$. Recall that, for $\pi \in \Delta(\Sigma)$, a π-martingale on Σ is a function $d : \Sigma^* \to [0, \infty)$ such that:

$$d(w) = \sum_{a \in \Sigma} d(wa)\pi(a)$$

Definition 2.8. Let $\pi \in \Delta(\Sigma)$ and let d be a π-martingale on Σ.

1. d succeeds on a sequence $S \in \Sigma^\infty$ if:
$$\limsup_{n \to \infty} d(S[0..n-1]) = \infty$$
2. d succeeds strongly on a sequence $S \in \Sigma^\infty$ if:
$$\liminf_{n \to \infty} d(S[0..n-1]) = \infty$$
3. The success set of d is:
$$S^\infty[d] = \{S \in \Sigma^\infty | d \text{ succeeds on } S\}$$
4. The success set of d is:
$$S^\infty_{str}[d] = \{S \in \Sigma^\infty | d \text{ succeeds strongly on } S\}$$

Definition 2.9. The cylinder generated by a string $w \in \Sigma^*$ is the set:

$$w\Sigma^\infty = \{S \in \Sigma^\infty | w \sqsubseteq S\}$$

Intuition: If we choose the symbols in a sequence $S \in \Sigma^\infty$ independently according to π, what is the probability that some given w is a prefix of S?

$$\prod_{i=0}^{|w|-1} \pi(w[i])$$

Call this $\pi(w)$. Now $\pi : \Sigma^* \to [0, 1]$.

Definition 2.10. A set $Z \subseteq \Sigma^\infty$ has π-measure 0, and we write $\mu[\pi](Z) = 0$ if, $(\forall \epsilon > 0)$, there is a function $g : \mathbb{N} \to \Sigma^*$ with the following two properties:

(i) $Z \subseteq \bigcup_{n=0}^{\infty} g(n)\Sigma^\infty$

(ii) $\sum_{n=0}^{\infty} \pi(g(n)) < \epsilon$

Definition 2.11. An ideal on Σ^∞ is a non-empty collection, $\mathscr{I}$, of subsets of Σ^∞ such that the following two conditions hold for all sets $X, Y \subseteq \Sigma^\infty$:

1. $X \subseteq Y \in \mathscr{I} \Rightarrow X \in \mathscr{I}$
2. $X, Y \in \mathscr{I} \Rightarrow X \cup Y \in \mathscr{I}$

An ideal $\mathscr{I}$ is proper if $\Sigma^\infty \neq \mathscr{I}$. An ideal $\mathscr{I}$ is non-atomic if, $\forall s \in \Sigma^\infty$, $\{s\} \in \mathscr{I}$.

Intuition: An ideal is a notion of smallness for subsets of Σ^∞. Condition 1 says that subsets of small sets are small. Condition 2 says that the union of two small sets is small (whence small sets are very small). An ideal is proper if not every set is small, and it is non-atomic if every singleton set is small.

Example 2.12.
1. $\{\emptyset\}$ is the smallest ideal. That is, it is an ideal and it is a subset of every ideal. Claim: $\emptyset$ is in every ideal by (1).
2. $\mathscr{P}(\Sigma^\infty)$ is the largest ideal, which has to contain every ideal, and it is not proper.
3. For every set, $X \subseteq \Sigma^\infty$, $\mathscr{P}(X)$ is an ideal on Σ^∞.
4. $FIN = \{z \subseteq \Sigma^\infty | z \text{ is finite } \}$ is a proper, nonatomic ideal on Σ^∞.
5. $CTBL = \{z \subseteq \Sigma^\infty | z \text{ is countable } \}$ is a proper, nonatomic ideal on Σ^∞.

Definition 2.13. A σ-ideal on Σ^∞ is an ideal $\mathscr{I}$ on Σ^∞ that is closed under countbale unions, i.e.,

$$Z_0, Z_1, Z_2, ... \in \mathscr{I} \Rightarrow \bigcup_{n=0}^{\infty} Z_n \in \mathscr{I}$$

Recall: Let $\pi \in \Delta(\Sigma)$. A set $Z \subseteq \Sigma^\infty$ has π-measure 0 and we write $\mu[\pi](Z) = 0$, if, for every $\epsilon > 0$, there is a function $g : \mathbb{N} \to \Sigma^*$ with the following two properties:

1. $Z \subseteq \bigcup_{n=0}^{\infty} g(n)\Sigma^\infty$
2. $\sum_{n=0}^{\infty} \pi(g(n)) < \epsilon$

Theorem 2.14. *Let $\pi \in \Delta(\Sigma)$. The collection of π-measure 0 subsets of Σ^∞ is a proper σ-ideal on Σ^∞. It is nonatomic if and only if $\pi \in \Delta^+(\Sigma^\infty)$.*

Proof. (scratch) □

Problem 2.1. Let $\Sigma = \{0, 1, ..., b-1\}$ where $b \geq 2$, and let π be the uniform probability measure on Σ, i.e., $\pi(a) = \frac{1}{b}$, $\forall a \in \Sigma$. For each of the following two sets, X, desgin a FSG, G, such that $X \subseteq S^\infty[d_G^\pi]$.

(a) $X = \{S \in \Sigma^\infty | (\forall^\infty n \in \mathbb{N}) S[n] > 0\}$

(b) $X = \{S \in \Sigma^\infty | (\forall^\infty n \in \mathbb{N}) S[3n] = S[3n+1]\}$

Problem 2.2. Let Σ and π be as in problem 2.1. Prove that, for all π-martingales, d, there is a π-martingale, $\hat{d}$ such that:

$$S^\infty[d] \subseteq S^\infty_{str}[\hat{d}]$$