Information Theory and Networks

Lecture 10: Sampling with Fair Coins

Matthew Roughan
<matthew.roughan@adelaide.edu.au>
http://www.maths.adelaide.edu.au/matthew.roughan/Lecture_notes/InformationTheory/

School of Mathematical Sciences,
University of Adelaide

September 18, 2013

Part I

Sampling with Fair Coins

> USA Today has come out with a new survey: Apparently three out of four people make up 75 percent of the population.
> *David Letterman*

USA Today has come out with a new survey: Apparently three out of four people make up 75 percent of the population.
David Letterman

Problem

Imagine you have a fair coin, but you want to sample from an arbitrary distribution, how would you do it?

Problem
Imagine you have a fair coin, but you want to sample from an arbitrary distribution, how would you do it?

From [CT91, p.110-116]

Example 1

Example: use a sequence of fair coin tosses to generate a random variable X with PMF

$$X = \begin{cases} a, & \text{with probability } 1/2, \\ b, & \text{with probability } 1/4, \\ c, & \text{with probability } 1/4, \end{cases}$$

Example 1
Example: use a sequence of fair coin tosses to generate a random variable X with PMF
X = { a, with probability 1/2, b, with probability 1/4, c, with probability 1/4,

Example 1

Example 1

General Problem

- We want to generate a random varible $X \in \Omega = \{1, 2, \cdots, m\}$
  - X has PMF $\{p_1, p_2, \ldots, p_m\}$
- We have a series of (independent) fair coin tosses $Z_1, Z_2, \ldots$
  - let T denote the number of coin tosses (which is potentially a RV)
  - we'd like methods that minmise $E[T]$

General Problem
- We want to generate a random varible $X \in \Omega = \{1, 2, \cdots, m\}$
  - X has PMF $\{p_1, p_2, \ldots, p_m\}$
- We have a series of (independent) fair coin tosses $Z_1, Z_2, \ldots$
  - let T denote the number of coin tosses (which is potentially a RV)
  - we'd like methods that minmise $E[T]$

Example 1

Problem

How could we go about designing such a tree for a dyadic distribution (one whose probabilities are powers of two)?

Is it related to entropy?

Problem
How could we go about designing such a tree for a dyadic distribution (one whose probabilities are powers of two)?
Is it related to entropy?

Example 2

Example 2

Problem

What about non-dyadic probabilities?

Problem
What about non-dyadic probabilities?

Obviously, we could do powers of three with ternary codes, and so on, do lets assume that the probabilities don't all fit some simple power-law.

Theorem

The expected number of fair bits $E[T]$ required by the optimal algorithm to generate a random variable X satisfies

$$H(X) \leq E[T] < H(X) + 2$$

Proof: see [CT91, pp.115-116]

Example 3

Example 3

Example 3

Example 3

Problem

What if you don't even know if your coin is fair?

Problem
What if you don't even know if your coin is fair?

We could have also looked into Stochastic Computing here – i.e., techniques for doing computation using operations stochastic processes.

Source Coding and 20 Questions

Yet another way to think about coding

- 20 questions:
  - Want to guess a 'fact' — say an experiment's outcome
  - Only allowed Yes/No questions
  - Want to find the most efficient set of questions
- Obviously, Huffman code is optimal way of generating questions if we know the PMF

Further reading I

Thomas M. Cover and Joy A. Thomas, *Elements of information theory*, John Wiley and Sons, 1991.