CS124 **How to get 1 fair flip efficiently?** Lecture 1

Biased coin, get unbiased

symmetry
heads p independent
tails $1-p$

flip until HT or TH → NOPE, no symmetry

flip 2 coins, if HT I win, TH you win
$p(1-p)$ $(1-p)p$

otherwise

efficiency

# of times to flip $2 \cdot \frac{1}{2pq} = \frac{1}{pq}$

$q = 1-p$

X = expected # of flips

$X = 2pq(2) + (1-2pq)(2+X)$ recursive based on independence of trials.

$(2pq)X = 2$ $\quad X = \frac{1}{pq}$

pick $p = 2/3$, make algorithm more efficient?

HH → 4/9
HT → 2/9
TH → 2/9
TT

group together

2x efficiency of flipping

but depends on specific p value

generalize?

HT
TH

HHTT
TTHH

first failure, new flips

HHHHTTTT
TTTTHHHH

prev failure

... by induction

only fail if 2^k all H or all T

still consider HT TH independently

next question: how to get many coin flips?...
efficiently..

extract more # of flips from a string of flips

levels	
0	HH TT HT HH HT HH HT
1	H T H H
2	H

vs # of all? are we getting all randomness out?
indep. flips

cannot shift by one → not indep!

additional symmetry

switch

HH HT TT ...... HH TT HT ...
[H T [H T

same → symmetry unused

generate another sequence to take this symmetry into account

0	HH	TT	HT	HH	HT	HH
1	H	T		H		
A	H	H	T	H	T	H

← H same
T different

$$\begin{array}{ccccccc} & & & 0 & & & \\ & & \swarrow & & \searrow & & \\ & 1 & & & & A & \\ \swarrow & & \searrow & & \swarrow & & \searrow \\ 2 & & 2B & & A1 & & B \end{array}$$

all unbiased indep coin flips pulled out of a string of biased

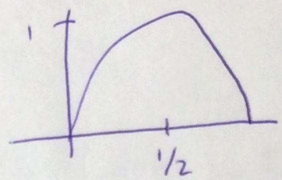
can reconstruct sequence from flips

entropy = measure randomness

Biased coin p

$H(p)$ = entropy → average # of bits available per coin flip

$H(1/2) = 1$
↑
1 bit per flip



$H(p) = 0.72$
↑
0.72 bits per flip

$$H(p) = -p\log_2 p - (1-p)\log_2(1-p)$$ for coin flipping process

Proof for A construction

$A(p)$ = avg # bits pulled out per flip, when bias is p, asymptotically in seq length

expected top layer; per flip from HH or TT

$$= \frac{2pq}{2} + \frac{p^2+q^2}{2} A\left(\frac{p^2}{p^2+q^2}\right) + \frac{1}{2} A(p^2+q^2)$$

av. # of bits when get a flip from HH or TT

one char for every 2 in original

can show $A(p) = H(p)$

thus $A(p)$ pulls out as many bits as $H(p)$