

Random Algorithm HW 9.12

March 27, 2006

a

First it is clear that the extracted bits are independent since x_{2i-1}, x_{2i} are independent on different i .

So we only need to show the i th bit has equal probability to be 1 or 0. This is actually also quite obvious since the probability for the original bias coin to generate a (heads,tails) is the same as to generate a (tails, heads) since they are independent trials.

b

There are $\lfloor \frac{n}{2} \rfloor$ pairs. One pair will only generate a bit if it is a (heads,tails) or (tails,head). The expected number of bits one single pair will generate is $p(1-p) + (1-p)p = 2p(1-p)$ by the linearity of expectation. The expected total number of bits will be $\lfloor \frac{n}{2} \rfloor 2p(1-p)$

c

Y is a sequence of independent trials with head probability $\frac{p^2}{p^2+(1-p)^2}$. So from the result of (a), running A on Y would produce bits that are independent and unbiased. Furthermore, since the original trials are independent and the sequence X and Y will generate bits on are mutually exclusive. So the bits generated from Y are independent from the bits generated from X.

d

Z is a sequence of independent trials with head probability $p^2 + (1-p)^2$. So the bits extracted from Z using A is independent and unbiased. It is also independent from X and Y, since giving X and Y will not affect Z.

e

From the result of (b),(c) and (d), the total number of bits generated is the sum of those generated from X, Y, Z

So, $A(p) = Prob(X \text{ will generate a bit}) * A(X) + Prob(Y \text{ will generate a bit}) * A(Y) + Prob(Z \text{ will generate a bit}) * A(Z)$
 $A(Z) = p(1-p) + \frac{1}{2} * (p^2 + q^2) A(\frac{p^2}{p^2+q^2}) + \frac{1}{2} * A(p^2 + q^2)$

f

Substitute the function A with the entropy function H. The recursive function holds.