

CMPSCI 711: “Really Advanced Algorithms”

Lecture 17 & 18 – Entropy, Randomness, and Information

Andrew McGregor

Last Compiled: April 9, 2009

Definitions

Entropy and Binomial Coefficients

Extracting Random Bits

Pairwise Independent Functions

Outline

Definitions

Entropy and Binomial Coefficients

Extracting Random Bits

Pairwise Independent Functions

Entropy

Definition

Given a discrete random variable X , the entropy of X is

$$H(X) = - \sum_x \mathbb{P}[X = x] \log \mathbb{P}[X = x]$$

Given two discrete random variables X, Y , the conditional entropy of X given Y is $H(X|Y) = \sum_y \mathbb{P}[Y = y] H(X|Y = y)$.

Entropy

Definition

Given a discrete random variable X , the entropy of X is

$$H(X) = - \sum_x \mathbb{P}[X = x] \log \mathbb{P}[X = x]$$

Given two discrete random variables X, Y , the conditional entropy of X given Y is $H(X|Y) = \sum_y \mathbb{P}[Y = y] H(X|Y = y)$.

Lemma

For function g , $H(g(X)|X) = 0$. $H(X|g(X)) = 0$ iff g invertible.

Entropy

Definition

Given a discrete random variable X , the entropy of X is

$$H(X) = - \sum_x \mathbb{P}[X = x] \log \mathbb{P}[X = x]$$

Given two discrete random variables X, Y , the conditional entropy of X given Y is $H(X|Y) = \sum_y \mathbb{P}[Y = y] H(X|Y = y)$.

Lemma

For function g , $H(g(X)|X) = 0$. $H(X|g(X)) = 0$ iff g invertible.

Lemma

If X_1, \dots, X_n are discrete random variables:

$$H(X_1, \dots, X_n) = \sum_{i \in [n]} H(X_i | X_1, \dots, X_{i-1})$$

If X_1, \dots, X_n are independent, then $H(X_1, \dots, X_n) = \sum_{i \in [n]} H(X_i)$

Mutual Information

Definition

Given discrete random variables X, Y , the mutual information is

$$I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

Given discrete random variables X, Y, Z , the conditional mutual information is

$$I(X; Y|Z) = \sum_z \mathbb{P}[Z = z] I(X; Y|Z = z)$$

Mutual Information

Definition

Given discrete random variables X, Y , the mutual information is

$$I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X)$$

Given discrete random variables X, Y, Z , the conditional mutual information is

$$I(X; Y|Z) = \sum_z \mathbb{P}[Z = z] I(X; Y|Z = z)$$

Lemma

If X_1, \dots, X_n, Y are discrete random variables:

$$I(X_1, \dots, X_n; Y) = \sum_{i \in [n]} I(X_i; Y | X_1, \dots, X_{i-1})$$

If X and Y are independent $I(X; Y) = 0$.

Outline

Definitions

Entropy and Binomial Coefficients

Extracting Random Bits

Pairwise Independent Functions

Entropy and Binomial Coefficients

Lemma

$$\frac{2^{nH(r/n)}}{n+1} \leq \binom{n}{r} \leq 2^{nH(r/n)}$$

where $H(x) = -x \log x - (1-x) \log(1-x)$.

Entropy and Binomial Coefficients

Lemma

$$\frac{2^{nH(r/n)}}{n+1} \leq \binom{n}{r} \leq 2^{nH(r/n)}$$

where $H(x) = -x \log x - (1-x) \log(1-x)$.

Proof.

- ▶ Let $q = r/n$.



Entropy and Binomial Coefficients

Lemma

$$\frac{2^{nH(r/n)}}{n+1} \leq \binom{n}{r} \leq 2^{nH(r/n)}$$

where $H(x) = -x \log x - (1-x) \log(1-x)$.

Proof.

- ▶ Let $q = r/n$.
- ▶ RHS:

$$1 = \sum_{k=0}^n \binom{n}{k} q^k (1-q)^{n-k} \geq \binom{n}{qn} q^{qn} (1-q)^{n-qn} = \binom{n}{qn} 2^{-nH(q)}$$



Entropy and Binomial Coefficients

Lemma

$$\frac{2^{nH(r/n)}}{n+1} \leq \binom{n}{r} \leq 2^{nH(r/n)}$$

where $H(x) = -x \log x - (1-x) \log(1-x)$.

Proof.

- ▶ Let $q = r/n$.
- ▶ RHS:

$$1 = \sum_{k=0}^n \binom{n}{k} q^k (1-q)^{n-k} \geq \binom{n}{qn} q^{qn} (1-q)^{n-qn} = \binom{n}{qn} 2^{-nH(q)}$$

- ▶ Claim: $\binom{n}{qn} q^{qn} (1-q)^{n-qn} \geq \binom{n}{k} q^k (1-q)^{n-k}$ for $0 \leq k \leq n$



Entropy and Binomial Coefficients

Lemma

$$\frac{2^{nH(r/n)}}{n+1} \leq \binom{n}{r} \leq 2^{nH(r/n)}$$

where $H(x) = -x \log x - (1-x) \log(1-x)$.

Proof.

- ▶ Let $q = r/n$.
- ▶ RHS:

$$1 = \sum_{k=0}^n \binom{n}{k} q^k (1-q)^{n-k} \geq \binom{n}{qn} q^{qn} (1-q)^{n-qn} = \binom{n}{qn} 2^{-nH(q)}$$

- ▶ Claim: $\binom{n}{qn} q^{qn} (1-q)^{n-qn} \geq \binom{n}{k} q^k (1-q)^{n-k}$ for $0 \leq k \leq n$
- ▶ LHS: $1 \leq (n+1) \binom{n}{qn} q^{qn} (1-q)^{n-qn} = (n+1) \binom{n}{qn} 2^{-nH(q)}$



Proof of Claim

Claim

$$\binom{n}{qn} q^{qn} (1-q)^{n-qn} \geq \binom{n}{k} q^k (1-q)^{n-k} \text{ for } 0 \leq k \leq n$$

Proof of Claim

Claim

$$\binom{n}{qn} q^{qn} (1-q)^{n-qn} \geq \binom{n}{k} q^k (1-q)^{n-k} \text{ for } 0 \leq k \leq n$$

Proof.

- ▶ Consider difference of terms:

$$\begin{aligned} & \binom{n}{k} q^k (1-q)^{n-k} - \binom{n}{k+1} q^{k+1} (1-q)^{n-k-1} \\ = & \binom{n}{k} q^k (1-q)^{n-k} \left(1 - \frac{n-k}{k+1} \frac{q}{1-q} \right) \end{aligned}$$



Proof of Claim

Claim

$$\binom{n}{qn} q^{qn} (1-q)^{n-qn} \geq \binom{n}{k} q^k (1-q)^{n-k} \text{ for } 0 \leq k \leq n$$

Proof.

- ▶ Consider difference of terms:

$$\begin{aligned} & \binom{n}{k} q^k (1-q)^{n-k} - \binom{n}{k+1} q^{k+1} (1-q)^{n-k-1} \\ &= \binom{n}{k} q^k (1-q)^{n-k} \left(1 - \frac{n-k}{k+1} \frac{q}{1-q} \right) \end{aligned}$$

- ▶ This is non-negative when: $k \geq qn - 1 + q$



Proof of Claim

Claim

$$\binom{n}{qn} q^{qn} (1-q)^{n-qn} \geq \binom{n}{k} q^k (1-q)^{n-k} \text{ for } 0 \leq k \leq n$$

Proof.

- ▶ Consider difference of terms:

$$\begin{aligned} & \binom{n}{k} q^k (1-q)^{n-k} - \binom{n}{k+1} q^{k+1} (1-q)^{n-k-1} \\ &= \binom{n}{k} q^k (1-q)^{n-k} \left(1 - \frac{n-k}{k+1} \frac{q}{1-q} \right) \end{aligned}$$

- ▶ This is non-negative when: $k \geq qn - 1 + q$
- ▶ Terms increasing up to $k = qn$ and decreasing afterwards.



Outline

Definitions

Entropy and Binomial Coefficients

Extracting Random Bits

Pairwise Independent Functions

Extracting Random Bits

Definition

An extraction function Ext takes the value of a random variable X and outputs a sequence of bits y such that, if $\mathbb{P}[|y| = k] \neq 0$,

$$\mathbb{P}[\text{Ext}(X) = y \mid |y| = k] = 2^{-k}$$

Extracting Random Bits

Definition

An extraction function Ext takes the value of a random variable X and outputs a sequence of bits y such that, if $\mathbb{P}[|y| = k] \neq 0$,

$$\mathbb{P}[\text{Ext}(X) = y \mid |y| = k] = 2^{-k}$$

Theorem

Consider a coin with bias $p > 1/2$. For any constant $\delta > 0$ and n sufficiently large:

- ▶ *There exists an extraction function that takes n independent coin flips and outputs an average of at least $(1 - \delta)nH(p)$ unbiased and independent random bits.*
- ▶ *The average number of unbiased and independent bits output by any extraction function on an input sequence of n independent flips is at most $nH(p)$.*

Extracting bits from uniform distributions (1/2)

Lemma

Suppose X is uniformly distributed in $\{0, \dots, m - 1\}$. Then there is an extraction function for X that outputs on average at least $\lfloor \log m \rfloor - 1$ unbiased and independent bits.

Extracting bits from uniform distributions (1/2)

Lemma

Suppose X is uniformly distributed in $\{0, \dots, m - 1\}$. Then there is an extraction function for X that outputs on average at least $\lfloor \log m \rfloor - 1$ unbiased and independent bits.

Proof.

- ▶ Let $\alpha = \lfloor \log m \rfloor$ and define the extraction function recursively



Extracting bits from uniform distributions (1/2)

Lemma

Suppose X is uniformly distributed in $\{0, \dots, m - 1\}$. Then there is an extraction function for X that outputs on average at least $\lfloor \log m \rfloor - 1$ unbiased and independent bits.

Proof.

- ▶ Let $\alpha = \lfloor \log m \rfloor$ and define the extraction function recursively
- ▶ If $X \leq 2^\alpha - 1$ output the α -bit representation of X .



Extracting bits from uniform distributions (1/2)

Lemma

Suppose X is uniformly distributed in $\{0, \dots, m - 1\}$. Then there is an extraction function for X that outputs on average at least $\lfloor \log m \rfloor - 1$ unbiased and independent bits.

Proof.

- ▶ Let $\alpha = \lfloor \log m \rfloor$ and define the extraction function recursively
- ▶ If $X \leq 2^\alpha - 1$ output the α -bit representation of X .
- ▶ If $X \geq 2^\alpha$, use the extraction function on $X - 2^\alpha$ since this is uniform on $\{0, \dots, m - 2^\alpha - 1\}$



Extracting bits from uniform distributions (1/2)

Lemma

Suppose X is uniformly distributed in $\{0, \dots, m - 1\}$. Then there is an extraction function for X that outputs on average at least $\lfloor \log m \rfloor - 1$ unbiased and independent bits.

Proof.

- ▶ Let $\alpha = \lfloor \log m \rfloor$ and define the extraction function recursively
- ▶ If $X \leq 2^\alpha - 1$ output the α -bit representation of X .
- ▶ If $X \geq 2^\alpha$, use the extraction function on $X - 2^\alpha$ since this is uniform on $\{0, \dots, m - 2^\alpha - 1\}$
- ▶ For each k , we get uniform distribution over k -bit sequences.



Extracting bits from uniform distributions (1/2)

Lemma

Suppose X is uniformly distributed in $\{0, \dots, m - 1\}$. Then there is an extraction function for X that outputs on average at least $\lfloor \log m \rfloor - 1$ unbiased and independent bits.

Proof.

- ▶ Let $\alpha = \lfloor \log m \rfloor$ and define the extraction function recursively
- ▶ If $X \leq 2^\alpha - 1$ output the α -bit representation of X .
- ▶ If $X \geq 2^\alpha$, use the extraction function on $X - 2^\alpha$ since this is uniform on $\{0, \dots, m - 2^\alpha - 1\}$
- ▶ For each k , we get uniform distribution over k -bit sequences.
- ▶ Remains to show that we expect to output $\lfloor \log m \rfloor - 1$ unbiased and independent bits.



Extracting bits from uniform distributions (2/2)

- ▶ Let Y be the number of bits output.

Extracting bits from uniform distributions (2/2)

- ▶ Let Y be the number of bits output.
- ▶ By induction on m :

$$\begin{aligned}\mathbb{E}[Y] &= \frac{2^\alpha}{m}\alpha + \frac{m - 2^\alpha}{m}\mathbb{E}[\text{bits from } \{0, \dots, m - 2^\alpha - 1\}] \\ &\geq \frac{2^\alpha}{m}\alpha + \frac{m - 2^\alpha}{m}(\lfloor \log(m - 2^\alpha) \rfloor - 1)\end{aligned}$$

Extracting bits from uniform distributions (2/2)

- ▶ Let Y be the number of bits output.
- ▶ By induction on m :

$$\begin{aligned}\mathbb{E}[Y] &= \frac{2^\alpha}{m}\alpha + \frac{m - 2^\alpha}{m}\mathbb{E}[\text{bits from } \{0, \dots, m - 2^\alpha - 1\}] \\ &\geq \frac{2^\alpha}{m}\alpha + \frac{m - 2^\alpha}{m}(\lfloor \log(m - 2^\alpha) \rfloor - 1)\end{aligned}$$

- ▶ Some algebra gives this is at least $\alpha - 1$ completing induction.

Extracting Bits from Biased Coin: Upper Bound (1/2)

Theorem

Consider coin with bias $p > 1/2$. For any constant $\delta > 0$ and n sufficiently large, there exists a function that takes n independent coin flips and outputs an average of at least $(1 - \delta)nH(p)$ independent and unbiased bits.

Extracting Bits from Biased Coin: Upper Bound (1/2)

Theorem

Consider coin with bias $p > 1/2$. For any constant $\delta > 0$ and n sufficiently large, there exists a function that takes n independent coin flips and outputs an average of at least $(1 - \delta)nH(p)$ independent and unbiased bits.

Proof.

- ▶ Let Z be number of heads seen.



Extracting Bits from Biased Coin: Upper Bound (1/2)

Theorem

Consider coin with bias $p > 1/2$. For any constant $\delta > 0$ and n sufficiently large, there exists a function that takes n independent coin flips and outputs an average of at least $(1 - \delta)nH(p)$ independent and unbiased bits.

Proof.

- ▶ Let Z be number of heads seen.
- ▶ Conditioned on $Z = k$, each of sequence $\binom{n}{k}$ sequences is equally likely. Can expect to extract $\lfloor \log \binom{n}{k} \rfloor - 1$ bits.



Extracting Bits from Biased Coin: Upper Bound (1/2)

Theorem

Consider coin with bias $p > 1/2$. For any constant $\delta > 0$ and n sufficiently large, there exists a function that takes n independent coin flips and outputs an average of at least $(1 - \delta)nH(p)$ independent and unbiased bits.

Proof.

- ▶ Let Z be number of heads seen.
- ▶ Conditioned on $Z = k$, each of sequence $\binom{n}{k}$ sequences is equally likely. Can expect to extract $\lfloor \log \binom{n}{k} \rfloor - 1$ bits.
- ▶ Let B be total number of bits extracted:

$$\mathbb{E}[B] = \sum_{k=0}^n \mathbb{P}[Z = k] \mathbb{E}[B|Z = k] \geq \sum_{k=0}^n \mathbb{P}[Z = k] (\lfloor \log \binom{n}{k} \rfloor - 1)$$



Extracting Bits from Biased Coin: Upper Bound (2/2)

- ▶ Consider only k such that $n/2 \leq n(p - \epsilon) \leq k \leq n(p + \epsilon)$:

$$\mathbb{E}[B] \geq \sum_{k=\lfloor n(p-\epsilon) \rfloor}^{\lceil n(p+\epsilon) \rceil} \mathbb{P}[Z = k] \left(\left\lfloor \log \binom{n}{k} \right\rfloor - 1 \right)$$

Extracting Bits from Biased Coin: Upper Bound (2/2)

- ▶ Consider only k such that $n/2 \leq n(p - \epsilon) \leq k \leq n(p + \epsilon)$:

$$\mathbb{E}[B] \geq \sum_{k=\lfloor n(p-\epsilon) \rfloor}^{\lceil n(p+\epsilon) \rceil} \mathbb{P}[Z = k] \left(\left\lfloor \log \binom{n}{k} \right\rfloor - 1 \right)$$

- ▶ Relating binomial coefficients to entropy:

$$\left\lfloor \log \binom{n}{k} \right\rfloor - 1 \geq \left(\log \frac{2^{nH(p+\epsilon)}}{n+1} \right) - 2$$

Extracting Bits from Biased Coin: Upper Bound (2/2)

- ▶ Consider only k such that $n/2 \leq n(p - \epsilon) \leq k \leq n(p + \epsilon)$:

$$\mathbb{E}[B] \geq \sum_{k=\lfloor n(p-\epsilon) \rfloor}^{\lceil n(p+\epsilon) \rceil} \mathbb{P}[Z = k] \left(\left\lfloor \log \binom{n}{k} \right\rfloor - 1 \right)$$

- ▶ Relating binomial coefficients to entropy:

$$\left\lfloor \log \binom{n}{k} \right\rfloor - 1 \geq \left(\log \frac{2^{nH(p+\epsilon)}}{n+1} \right) - 2$$

- ▶ Appealing to Chernoff bound:

$$\sum_{k=\lfloor n(p-\epsilon) \rfloor}^{\lceil n(p+\epsilon) \rceil} \mathbb{P}[Z = k] \geq (1 - 2e^{-n\epsilon^2/3p})$$

Extracting Bits from Biased Coin: Upper Bound (2/2)

- ▶ Consider only k such that $n/2 \leq n(p - \epsilon) \leq k \leq n(p + \epsilon)$:

$$\mathbb{E}[B] \geq \sum_{k=\lfloor n(p-\epsilon) \rfloor}^{\lceil n(p+\epsilon) \rceil} \mathbb{P}[Z = k] \left(\left\lfloor \log \binom{n}{k} \right\rfloor - 1 \right)$$

- ▶ Relating binomial coefficients to entropy:

$$\left\lfloor \log \binom{n}{k} \right\rfloor - 1 \geq \left(\log \frac{2^{nH(p+\epsilon)}}{n+1} \right) - 2$$

- ▶ Appealing to Chernoff bound:

$$\sum_{k=\lfloor n(p-\epsilon) \rfloor}^{\lceil n(p+\epsilon) \rceil} \mathbb{P}[Z = k] \geq (1 - 2e^{-n\epsilon^2/3p})$$

- ▶ Putting it together:

$$\mathbb{E}[B] = (H(p+\epsilon) - \log(n+1) - 2)(1 - 2e^{-n\epsilon^2/3p}) \geq (1 - \delta)nH(p)$$

where the last inequality is for sufficiently large n .

Extracting Bits from Biased Coin Tosses: Lower Bound

Theorem

Consider a coin with bias $p > 1/2$. The average number of bits output by any extraction function on an input sequence of n independent flips is at most $nH(p)$.

Extracting Bits from Biased Coin Tosses: Lower Bound

Theorem

Consider a coin with bias $p > 1/2$. The average number of bits output by any extraction function on an input sequence of n independent flips is at most $nH(p)$.

Proof.

- ▶ Consider extraction function Ext.



Extracting Bits from Biased Coin Tosses: Lower Bound

Theorem

Consider a coin with bias $p > 1/2$. The average number of bits output by any extraction function on an input sequence of n independent flips is at most $nH(p)$.

Proof.

- ▶ Consider extraction function Ext .
- ▶ If x occurs with probability q , then $|\text{Ext}(x)| \leq \log(1/q)$ since:

$$q2^{|\text{Ext}(x)|} \leq 1$$



Extracting Bits from Biased Coin Tosses: Lower Bound

Theorem

Consider a coin with bias $p > 1/2$. The average number of bits output by any extraction function on an input sequence of n independent flips is at most $nH(p)$.

Proof.

- ▶ Consider extraction function Ext .
- ▶ If x occurs with probability q , then $|\text{Ext}(x)| \leq \log(1/q)$ since:

$$q2^{|\text{Ext}(x)|} \leq 1$$

- ▶ Let B be number of bits extracted by Ext :

$$\mathbb{E}[B] = \sum_x \mathbb{P}[X = x] |\text{Ext}(x)| \leq \sum_x \mathbb{P}[X = x] \log \frac{1}{\mathbb{P}[X = x]}$$



Outline

Definitions

Entropy and Binomial Coefficients

Extracting Random Bits

Pairwise Independent Functions

Pairwise Independent Functions

- ▶ Let n be a prime and $a, b \in_R \{0, 1, \dots, n - 1\}$.

Pairwise Independent Functions

- ▶ Let n be a prime and $a, b \in_R \{0, 1, \dots, n-1\}$.
- ▶ Consider $Z = (R_0, \dots, R_{n-1})$ where $R_i = ai + b \pmod{n}$.

Pairwise Independent Functions

- ▶ Let n be a prime and $a, b \in_R \{0, 1, \dots, n-1\}$.
- ▶ Consider $Z = (R_0, \dots, R_{n-1})$ where $R_i = ai + b \pmod{n}$.
- ▶ Entropy of each R_i :

Pairwise Independent Functions

- ▶ Let n be a prime and $a, b \in_R \{0, 1, \dots, n-1\}$.
- ▶ Consider $Z = (R_0, \dots, R_{n-1})$ where $R_i = ai + b \pmod{n}$.
- ▶ Entropy of each R_i : $H(R_i) = \log n$

Pairwise Independent Functions

- ▶ Let n be a prime and $a, b \in_R \{0, 1, \dots, n-1\}$.
- ▶ Consider $Z = (R_0, \dots, R_{n-1})$ where $R_i = ai + b \pmod{n}$.
- ▶ Entropy of each R_i : $H(R_i) = \log n$
- ▶ Entropy of Z :

Pairwise Independent Functions

- ▶ Let n be a prime and $a, b \in_R \{0, 1, \dots, n-1\}$.
- ▶ Consider $Z = (R_0, \dots, R_{n-1})$ where $R_i = ai + b \pmod n$.
- ▶ Entropy of each R_i : $H(R_i) = \log n$
- ▶ Entropy of Z : $H(Z) = 2 \log n$

Pairwise Independent Functions

- ▶ Let n be a prime and $a, b \in_R \{0, 1, \dots, n-1\}$.
- ▶ Consider $Z = (R_0, \dots, R_{n-1})$ where $R_i = ai + b \pmod{n}$.
- ▶ Entropy of each R_i : $H(R_i) = \log n$
- ▶ Entropy of Z : $H(Z) = 2 \log n$

Lemma

For discrete random variable X and function g : $H(g(X)) \leq H(X)$ with equality iff g is invertible.

Pairwise Independent Functions

- ▶ Let n be a prime and $a, b \in_R \{0, 1, \dots, n-1\}$.
- ▶ Consider $Z = (R_0, \dots, R_{n-1})$ where $R_i = ai + b \pmod{n}$.
- ▶ Entropy of each R_i : $H(R_i) = \log n$
- ▶ Entropy of Z : $H(Z) = 2 \log n$

Lemma

For discrete random variable X and function g : $H(g(X)) \leq H(X)$ with equality iff g is invertible.

Proof.

- ▶ $H(X, g(X)) = H(X) + H(g(X)|X) = H(X)$



Pairwise Independent Functions

- ▶ Let n be a prime and $a, b \in_R \{0, 1, \dots, n-1\}$.
- ▶ Consider $Z = (R_0, \dots, R_{n-1})$ where $R_i = ai + b \pmod{n}$.
- ▶ Entropy of each R_i : $H(R_i) = \log n$
- ▶ Entropy of Z : $H(Z) = 2 \log n$

Lemma

For discrete random variable X and function g : $H(g(X)) \leq H(X)$ with equality iff g is invertible.

Proof.

- ▶ $H(X, g(X)) = H(X) + H(g(X)|X) = H(X)$
- ▶ $H(X, g(X)) = H(g(X)) + H(X|g(X)) \geq H(g(X))$.



Pairwise Independent Functions

- ▶ Let n be a prime and $a, b \in_R \{0, 1, \dots, n-1\}$.
- ▶ Consider $Z = (R_0, \dots, R_{n-1})$ where $R_i = ai + b \pmod{n}$.
- ▶ Entropy of each R_i : $H(R_i) = \log n$
- ▶ Entropy of Z : $H(Z) = 2 \log n$

Lemma

For discrete random variable X and function g : $H(g(X)) \leq H(X)$ with equality iff g is invertible.

Proof.

- ▶ $H(X, g(X)) = H(X) + H(g(X)|X) = H(X)$
- ▶ $H(X, g(X)) = H(g(X)) + H(X|g(X)) \geq H(g(X))$.



- ▶ $Z = f(a, b)$ where f is invertible. Hence,

$$H(Z) = H(a, b) = H(a) + H(b) = 2 \log n$$