See also: http://en.wikibooks.org/High_School_Mathematics_Extensions/Discrete_Probability

Introduction

Discrete Probability (crash course, cont.)

Recap

U: finite set (e.g. $U = \{0,1\}^n$)

Prob. distr. P over U is a function $P: U \longrightarrow [0,1]$ s.t. $\sum_{x \in U} P(x) = 1$

$A \subseteq U$ is called an **event** and $\Pr[A] = \sum_{x \in A} P(x) \in [0,1]$

A **random variable** is a function $X: U \longrightarrow V$.

X takes values in V and defines a distribution on V

Independence

<u>Def</u>: events A and B are **independent** if $\Pr[\,A \text{ and } B\,] = \Pr[A] \cdot \Pr[B]$

random variables X,Y taking values in V are **independent** if

$\forall a,b \in V$: $\Pr[\,X=a \text{ and } Y=b] = \Pr[X=a] \cdot \Pr[Y=b]$

<u>Example</u>: $U = \{0,1\}^2 = \{00, 01, 10, 11\}$ and $r \xleftarrow{R} U$

Define r.v. X and Y as: $X = \mathrm{lsb}(r)$, $Y = \mathrm{msb}(r)$

$$\Pr[\,X=0 \text{ and } Y=0\,] = \Pr[\,r=00\,] = \tfrac{1}{4} = \Pr[X=0] \cdot \Pr[Y=0]$$

Review: XOR

XOR of two strings in $\{0,1\}^n$ is their bit-wise addition mod 2

$$
\begin{array}{r}
0\ 1\ 1\ 0\ 1\ 1\ 1 \\
\oplus \quad 1\ 0\ 1\ 1\ 0\ 1\ 0 \\
\hline
\end{array}
$$

An important property of XOR

<u>**Thm**</u>: Y a rand. var. over $\{0,1\}^n$, X an indep. uniform var. on $\{0,1\}^n$

Then $Z := Y \oplus X$ is uniform var. on $\{0,1\}^n$

Proof: (for n=1)

Pr[Z=0] =

The birthday paradox

Let $r_1, \ldots, r_n \in U$ be indep. identically distributed random vars.

<u>Thm</u>: when $n = 1.2 \times |U|^{1/2}$ then $\Pr[\, \exists i \neq j: \; r_i = r_j \,] \geq ½$

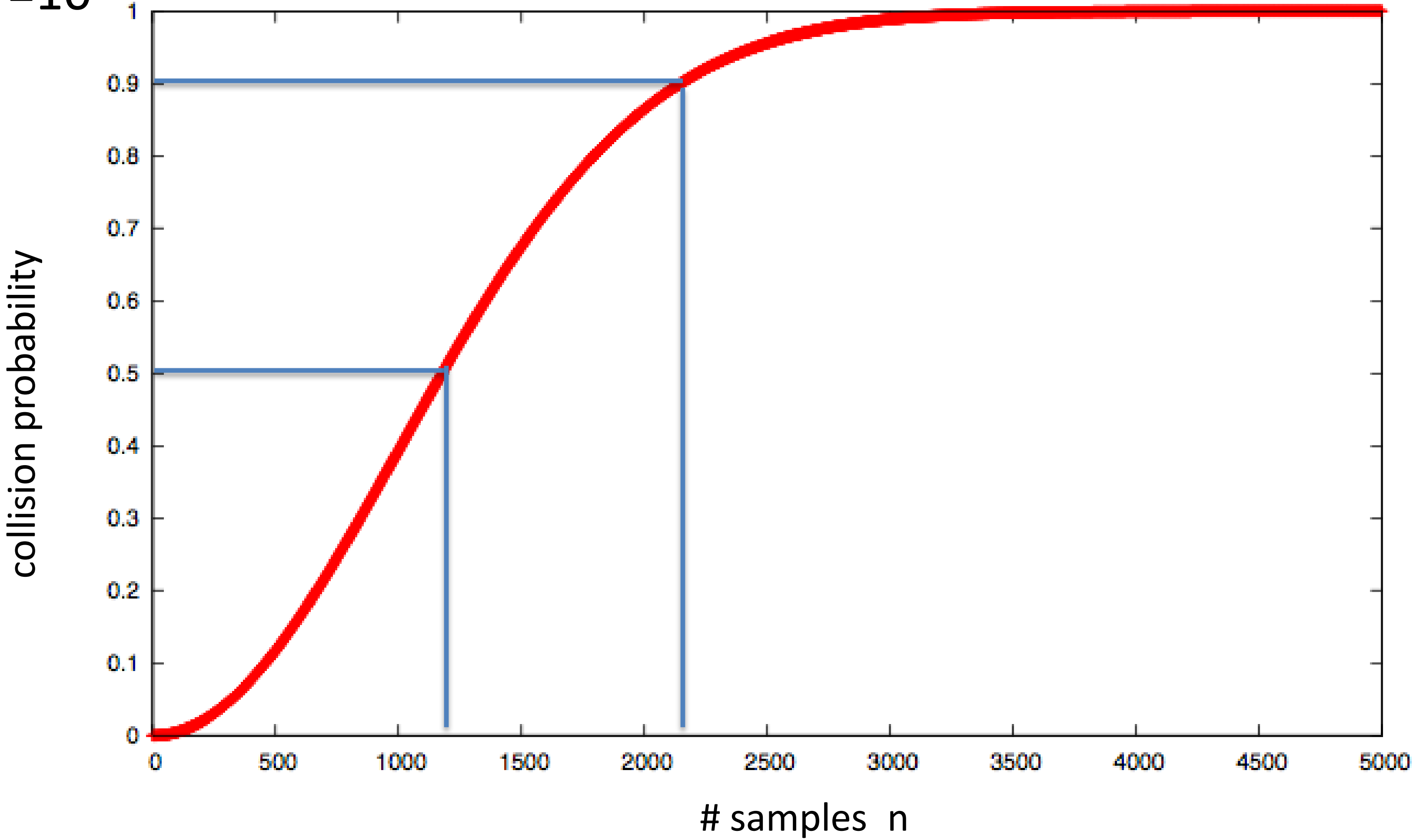
notation: $|U|$ is the size of U

<u>Example</u>: Let $U = \{0,1\}^{128}$

After sampling about 2^{64} random messages from U,

some two sampled messages will likely be the same

$|U|=10^6$



collision probability
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
500
1000
1500
2000
2500
3000
3500
4000
4500
5000
samples n

End of Segment