

Homework 1

Lecturer: Aggelos Kiayias

Scribes: Serdar Pehlivanoglu & Hong-Sheng Zhou

Consider the following samplers that given A (so that A is not a power of 2, n -bit number with most significant bit of $A = 1$) they perform the following steps to select a number in range $[0, A)$:

Sampler 1:

1. $n := \lceil \log_2 A \rceil$.
2. choose: $x_0, x_1, \dots, x_{n-1} \leftarrow_R \{0, 1\}$.
3. $y := \sum_{\ell=0}^{n-1} 2^\ell x_\ell$.
4. output $y \bmod A$.

Sampler 2:

1. choose: $x_0, x_1, \dots, x_{A-1} \leftarrow_R \{0, 1\}$.
2. $y := \sum_{\ell=0}^{A-1} x_\ell$.
3. output y .

Sampler 3:

1. $n := \lceil \log_2 A \rceil$.
2. repeat
3. choose: $x_0, x_1, \dots, x_{n-1} \leftarrow_R \{0, 1\}$.
4. $y := \sum_{\ell=0}^{n-1} 2^\ell x_\ell$.
5. if $y < A$ output y and halt.
6. else repeat.

Measure the quality of each sampler by computing the statistical distance of the output distribution of sampler to the uniform distribution over set $\{0, 1, 2, \dots, A - 1\}$. The statistical distance should be expressed as a function in n and possibly A . Moreover, you should identify range of values for A for which the sampler behaves more favorably. You should also consider the quality of the sampler in the asymptotic sense : how does it scale as n becomes larger? Finally you should take into account the number of coins used by each sampler; if coins are a scarce resource, which one is the best sampler? how do the samplers compare in this case?