Radomized Algorithms Solution to Hw3.

15.- (*) (This was an important problem) The way the algorithm works flips coins $c_n, c_{n-1}, \ldots, c_{s_1}$, recall in the flip of c_i: $\mathbf{Pr}[c_i = H] = 1/i$. After flip $c_{s_1}, \ldots c_{s_3}$ and so on. Every coin will be flipped and s_i will be selected as many times as it flip to H (they have to be consecutive ones). That numbers are the m's in the list item (a).

(a) If we pick each s_i using the method of the coins, it is equivalent to flipping each coin c_j for $j = n, n-1, \ldots$ until it lands T, and then go to generate next one. The value $m_j = \#$ times c_j lands H before it lands T. The probability c_j lands exactly m_j times H's before the first T is $(1/j)^{m_j}(1-1/j)$. Notice that $j = 1$ is missed because we always have $m_j = 1$, therefore, the probability it generates all sequence $\{s_i\}$ is $\prod_{j=2}^{n}(\frac{1}{j})^{m_j}(1-\frac{1}{j})$.

(b) Write $r \in \{1, \ldots, n\}$ in factored form as $\prod_p p^{\beta_p} \Rightarrow \mathbf{Pr}[m_p = \beta_p \text{for all primes } p \leq n] = \prod(1/p)^{\beta_p}(1-1/p) = \alpha_n/r$, so the algorithm outputs r with prob. $= \frac{r}{n}\frac{\alpha_n}{r} = \frac{\alpha_n}{n}$.

(c) The probability that the algorithm does not fail is $\sum_{r=1}^{n} \mathbf{Pr}[\text{algo. outputs } r] = n\alpha_n/n = \alpha_n$. So the expected number of trials is $\alpha_n^{-1} \sim \ln n$.

(d) Let $X =$ number of primality tests performed by one trial of the algorithm. We can write this as $X = \sum_{i=1}^{n} X_i$ where X_i is an indicator rv of the event that j is tested for primality, which happens iff $m_j \geq 1$, so by analysis of part (a) $\Rightarrow \mathbf{E}[X] = \sum_{i=1}^{n} \mathbf{E}[X_i] = H_n$.

(e) If we are making T trials, let Z be a rv counting the total number of primality tests performed. Then $\mathbf{E}[Z] = \sum_{j=1}^{T} \mathbf{E}[Z_j]$, where Z_t denotes the number of tests done at tth trial. Note T is a rv!!!!, so we are summing on a rv. Then $\mathbf{E}[Z_t] = H_n$ (from (d)), moreover from (e) we get that $\mathbf{E}[T] = \alpha_n^{-1}$. Notice, that if we argue that since Z is the sum of T rv each with same expectation $\mathbf{E}[Z_1]$, then $\mathbf{E}[Z] = \mathbf{E}[T]\,\mathbf{E}[Z_1] = H_n/\alpha_n$, which turns to be the correct answer but the wrong argument, as the Z_t are NOT independent of T.
Write $Z = \sum_{t=1}^{\infty}\sum_{j=1}^{n} Y_{t,j}$, where $Y_{t,j}$ is an ind. rv taking value 1 iff j is tested for primality on the tth trial (0 otherwise). Let A_t the event we do t or more trials, then
$\mathbf{E}[Y_{t,j}] = \mathbf{Pr}[j \text{ is tested in trial } t] = \mathbf{Pr}[j \text{ is tested in trial } t | A_t] = (1-\alpha_n)^{t-1}1/j$
$\mathbf{E}[Z] = \sum_{t=1}^{\infty}\sum_{j=1}^{n}\mathbf{E}[Y_{t,j}] = \sum_{t=1}^{\infty}\sum_{j=1}^{n}(1-\alpha_n)^{t-1}1/j = \sum_{t=1}^{\infty}(1-\alpha_n)^{t-1}\sum_{j=1}^{n}1/j = H_n/\alpha_n$. The result follows as $H_n = \Theta(\lg n)$ and $\alpha_n^{-1} = \Theta(\lg n)$.

19.- (a) All possible ith pairs of bits (b_{i_1}, b_{i_2}) are $(0,0),(0,1),(1,0),(1,1)$. Recall $b_{i_1} \oplus b_{i_2} = 1$ iff $b_{i_1} \neq b_{i_2}$, thus $\mathbf{Pr}[Y_i = 0] = \mathbf{Pr}[y_2 = 1] = 1/2$

(b) Let $b_1, \ldots, b_n$ be n random bits. Let $Y_1 = b_1 \oplus b_2, Y_2 = b_2 \oplus b_3, Y_3 = b_1 \oplus b_1$. From (a) we get $\mathbf{Pr}[Y_1 = 1] = \mathbf{Pr}[Y_2 = 1] = \mathbf{Pr}[Y_3 = 1] = 1/2$. Moreover, $\mathbf{Pr}[Y_1 = 1 \cap Y_2 = 1 \cap Y_3 = 1] = 0$, since when $Y_1 = Y_2 = 1$, we have $b_1 = b_3$ so Y_3 can't be 1.

(c) Any two bits, which do not share a bit are independent so $\mathbf{E}[Y_i Y_j] = \mathbf{E}[Y_i]\mathbf{E}[Y_j]$. Consider the case they share a bit: $Y_i = b_1 \oplus b_2$ and $Y_j = b_2 \oplus b_3$ (share b_2) Then the possible outcomes for b_1, b_2, b_3 are 0,1 but the possible cases are 8, so $\mathbf{Pr}[Y_i = 1 \cap Y_j = 1] = 2/8 = 1/4$ so that $\mathbf{E}[Y_i Y_j] = 1\mathbf{Pr}[Y_i = 1 \cap Y_j = 1] = 1/4 = \mathbf{E}[Y_i]\mathbf{E}[Y_j]$.

(d) Using exercise **??**) if $\mathbf{E}[Y_i Y_j] = \mathbf{E}[Y_i]\mathbf{E}[Y_j]$ for every of pairs i, j then $\mathbf{Var}[Y] = \sum_{i=1}^{m} \mathbf{Var}[X_i]$, then by (c)
$\mathbf{Var}[Y] = \sum_{i=1}^{m} \mathbf{Var}[X_i] = \sum_{i=1}^{m} \mathbf{E}\left[Y_i^2\right] - (\mathbf{E}[Y_i])^2 = m(\frac{1}{2} - (\frac{1}{2})^2) = \frac{\binom{n}{2}}{4}$.

(e) $\mathbf{Pr}[|Y - \mathbf{E}[Y]| \geq n] \leq \frac{\mathbf{Var}[Y]}{n^2} \frac{n(n-1)/8}{n^2} = \frac{1}{8} - \Omega(n^{-1}$.

20.- (*) (More sampling)

(a) Let $Y_t = \left(\sum_{i=1}^{t} X_i/t\right)$, then

$$\begin{aligned}\mathbf{E}[Y_t] =& \mathbf{E}\left[(\sum_{i=1}^{t} X_i)/t\right] = \mathbf{E}\left[\sum_{i=1}^{t} X_i\right]/t \\ =& (\sum_{i=1}^{t} \mathbf{E}[X_i])/t = \frac{t\mathbf{E}[X]}{t} = \mathbf{E}[X].\end{aligned}$$

By independence,

$$\mathbf{Var}[Y_t] = \mathbf{Var}\left[(\sum_{i=1}^{t} X_i)/t\right] = (\sum_{i=1}^{t} \mathbf{Var}[X_i])/t^2 = \mathbf{Var}[X]/t.$$

Using Chebyshev's on Y_t we have:

$$\begin{aligned}\mathbf{Pr}\left[|\frac{1}{t}\sum_{i=1}^{t} X_i - \mathbf{E}[X]| < \epsilon\mathbf{E}[X]\right] =& 1 - \mathbf{Pr}\left[|\frac{1}{t}\sum_{i=1}^{t} X_i - \mathbf{E}[X]| \geq \epsilon\mathbf{E}[X]\right] \\ =& 1 - \mathbf{Pr}[|Y_t - \mathbf{E}[Y_t]| \geq \epsilon\mathbf{E}[Y_t]] \geq 1 - \frac{\mathbf{Var}[Y_t]}{\epsilon^2\mathbf{E}[Y_t]^2} \\ =& 1 - \frac{\mathbf{Var}[X]/t}{\epsilon^2\mathbf{E}[X]^2} = 1 - \frac{1}{t}\frac{r^2}{\epsilon^2}\end{aligned}$$

Taking $t \geq r^2/\epsilon^2\delta$ we get

$$\mathbf{Pr}\left[|\frac{1}{t}\sum_{i=1}^{t} X_i - \mathbf{E}[X]| < \epsilon\mathbf{E}[X]\right] \geq 1 - \frac{1r^2}{t\epsilon^2} \geq 1 - -\frac{1}{r^2/\epsilon^2\delta}\frac{r^2}{\epsilon^2} = 1 - \delta,$$

which shows that $O(r^2/\epsilon^2\delta)$ samples suffice.

(b) Using the previous bound, if $t \geq 4r^2/\epsilon^2$ we get

$$\mathbf{Pr}\left[|\frac{1}{t}\sum_{i=1}^{t} X_i - \mathbf{E}[X]| < \epsilon \mathbf{E}[X]\right] \geq 1 - \frac{1}{t}\frac{r^2}{\epsilon^2} \geq 1 - \frac{r^2}{t\epsilon^2}\frac{1}{4r^2/\epsilon^2} = 1 - \frac{1}{4} = \frac{3}{4}.$$

So $4r^2/\epsilon^2$ samples are sufficient for this weak estimate.