Prof. Juraj Hromkovič
Juraj.Hromkovic@inf.ethz.ch
Richard Královič
Richard.Kralovic@inf.ethz.ch

Design of Randomized Algorithms

Sample solutions

Exercise 1

Due to Definition 2.2.23, we need to show

$$Prob[X_1 = a \wedge X_2 = b] = Prob[X_1 = a] \cdot Prob[X_2 = b].$$

Let $W = PRIM(n^2)$ be the set of primes from range 1 to n^2. We deal with the probability space (S, P), where $S = \{(k, l) | k, l \in W\}$ is the set of all tuples of primes from range 1 to n^2. Since the first and second primes are chosen independently, the following condition is true for the probability distribution P:

$$P(k, l) = \left(\sum_{l' \in W} P(k, l') \right) \cdot \left(\sum_{k' \in W} P(k', l) \right)$$

Let $W_1 \subseteq W$ be the set of "good" primes for comparing (x, y), and let $W_0 \subseteq W$ be the set of "bad" primes. It holds that:

$$Prob[X_1 = a \wedge X_2 = b] = \sum_{k \in W_a, l \in W_b} P(k, l)$$

What can be rewritten as:

$$\begin{aligned}
\sum_{k \in W_a, l \in W_b} P(k, l) &= \sum_{k \in W_a, l \in W_b} \left(\sum_{l' \in W} P(k, l') \right) \cdot \left(\sum_{k' \in W} P(k', l) \right) \\
&= \sum_{k \in W_a} \left(\sum_{l' \in W} P(k, l') \right) \sum_{l \in W_b} \left(\sum_{k' \in W} P(k', l) \right) \\
&= \left(\sum_{k \in W_a, l' \in W} P(k, l') \right) \cdot \left(\sum_{k' \in W, l \in W_b} P(k', l) \right) \\
&= Prob[X_1 = a] \cdot Prob[X_2 = b]
\end{aligned}$$

Random variable Y can be defined by the inclusion/exclusion principle as follows:

$$Y = X_1 + X_2 - X_1 X_2$$

The proof of correctness is straightforward: Consider arbitrary elementary event $e = (k, l)$. If $X_1(e) = X_2(e) = 0$, then $Y(e) = 0$, as it is required by the definition of Y. In any other case $Y(e) = 1$, again satisfying the definition of Y.

Exercise 2

The method of increasing the size of the set of witness candidates (i.e. choosing primes from range $1 \dots n^d$) requires $2d\lceil \log_2 n \rceil$ bits to be communicated and yields the probability of error at most $\frac{d \ln n}{n^{d-1}}$. When choosing primes from range $1 \dots n^2$ and executing k independent runs, it is necessary to communicate $4k\lceil \log_2 n \rceil$ bits and the probability of error is at most $\left(\frac{2 \ln n}{n}\right)^k$.

Hence, in both cases it is enough to communicate $4\lceil \log_2 n \rceil$ to have the probability of error converging to 0 with increasing n. (It is enough to take $d = 2$ and $k = 1$).

If we are allowed to communicate $c(n)$ bits, the first method yields probability of error $\frac{d \ln n}{n^{d-1}}$ for $d = \lfloor \frac{c(n)}{2\lceil \log_2 n \rceil} \rfloor$. The second method yields probability of error $\left(\frac{2 \ln n}{n}\right)^k$ for $k = \lfloor \frac{c(n)}{4\lceil \log_2 n \rceil} \rfloor$. Let $d(n) = \frac{c(n)}{2\lceil \log_2 n \rceil}$. The probability of error of the first method is $\frac{\lfloor d(n) \rfloor \ln n}{n^{\lfloor d(n) \rfloor - 1}}$ and the probability of error of the second method is $\left(\frac{2 \ln n}{n}\right)^{\lfloor d(n)/2 \rfloor}$. Obviously, the error of the first method is decreasing faster with increasing $c(n)$.

Exercise 3

Due to the proof of Lemma 3.2.2, we know that the expected number of collisions in slot l equals to $E[X^l] = \frac{n(n-1)}{2m^2}$ for each l. Hence, the total expected number of collisions is

$$E\left[\sum_{i=1}^{m} X^i\right] = \sum_{i=1}^{m} E\left[X^i\right] = m\frac{n(n-1)}{2m^2} < \frac{n^2}{2m}.$$

Exercise 4

According to the well-known algebraic theorem, for each prime p and natural number a there exists a field with p^a elements. Hence, the proof of Lemma 3.3.13 is correct also for a field with $m = p^a$ elements.