Homework 10

1. In Luby's algorithm, we need to show that if we expect to delete at least a fixed fraction of the remaining edges in each stage, then the expected number of stages is logarithmic in the number of edges. We can formalize this as follows.

   Proposition *Let $m \geq 0$ and $0 < \epsilon < 1$. Let $X_1, X_2, \ldots$ and $S_0, S_1, S_2, \ldots$ be nonnegative integer-valued random variables such that*

   $$\begin{aligned} S_n &= X_1 + \cdots + X_n \leq m \\ \mathcal{E}(X_{n+1} \mid S_n) &\geq \epsilon \cdot (m - S_n) \ . \end{aligned}$$

   Then the expected least n such that $S_n = m$ is $O(\log m)$.

   In our application, m is the number of edges in the original graph, X_n is the number of edges deleted in stage n, S_n is the total number of edges deleted so far after stage n, and $\epsilon = \frac{1}{72}$.

   (a) Show that

   $$\mathcal{E}S_n \geq m(1 - (1 - \epsilon)^n) \ .$$

   (*Hint.* Using the fact $\mathcal{E}(\mathcal{E}(X_{n+1} \mid S_n)) = \mathcal{E}X_{n+1}$ shown in class, give a recurrence for $\mathcal{E}S_n$.)

   (b) Using the definition of expectation, show also that

   $$\mathcal{E}S_n \leq m - 1 + \Pr(S_n = m)$$

   and therefore

   $$\Pr(S_n = m) \geq 1 - m(1 - \epsilon)^n \ .$$

   (c) Conclude that the expected least n such that $S_n = m$ is $O(\log m)$. (*Hint.* Define the function

   $$f(x) = \begin{cases} 1 \ , & \text{if } x < m \\ 0 \ , & \text{otherwise} \end{cases}$$

   and compute the expectation of the random variable

   $$R = f(S_0) + f(S_1) + f(S_2) + \cdots$$

   that counts the number of rounds.)

Homework 10 Solutions

1. (a) As shown in Lecture 36, the expected value of the random variable $\mathcal{E}(X_{n+1} \mid S_n)$ is

$$\mathcal{E}(\mathcal{E}(X_{n+1} \mid S_n)) \;=\; \mathcal{E}X_{n+1} \;.$$

This yields the recurrence

$$\begin{aligned}
\mathcal{E}S_0 &= 0 \\
\mathcal{E}S_{n+1} &= \mathcal{E}(S_n + X_{n+1}) \\
&= \mathcal{E}S_n + \mathcal{E}X_{n+1} \\
&= \mathcal{E}S_n + \mathcal{E}(\mathcal{E}(X_{n+1} \mid S_n)) \\
&\geq \mathcal{E}S_n + \mathcal{E}(\epsilon(m - S_n)) \\
&= \epsilon m + (1-\epsilon)\mathcal{E}S_n
\end{aligned}$$

whose solution gives

$$\mathcal{E}S_n \;\geq\; m(1 - (1-\epsilon)^n) \;.$$

(b)

$$\begin{aligned}
\mathcal{E}S_n &= \sum_{i=0}^{m} i \cdot \Pr(S_n = i) \\
&= m \cdot \Pr(S_n = m) + \sum_{i=0}^{m-1} i \cdot \Pr(S_n = i) \\
&\leq m \cdot \Pr(S_n = m) + \sum_{i=0}^{m-1} (m-1) \cdot \Pr(S_n = i) \\
&= m \cdot \Pr(S_n = m) + (m-1) \cdot (1 - \Pr(S_n = m)) \\
&= m - 1 + \Pr(S_n = m) \;.
\end{aligned}$$

Combining this inequality with (a), we obtain

$$\Pr(S_n = m) \;\geq\; 1 - m(1-\epsilon)^n \;.$$

(c) Using (b),

$$\begin{aligned}
\mathcal{E}f(S_n) &= 1 \cdot \Pr(S_n < m) + 0 \cdot \Pr(S_n = m) \\
&= 1 - \Pr(S_n = m) \\
&\leq m(1-\epsilon)^n \;.
\end{aligned}$$

Also, by definition of f,

$$\mathcal{E}f(S_n) \;\leq\; 1 \;.$$

Then for any ℓ,

$$\begin{aligned}\mathcal{E}R &= \sum_{n=0}^{\infty} \mathcal{E}f(S_n) \\ &\leq \sum_{n=0}^{\ell-1} 1 + \sum_{n=\ell}^{\infty} m(1-\epsilon)^n \\ &= \ell + m(1-\epsilon)^{\ell} \sum_{n=0}^{\infty} (1-\epsilon)^n \\ &= \ell + \frac{m}{\epsilon}(1-\epsilon)^{\ell} .\end{aligned}$$

Taking

$$\ell = \left\lceil \frac{\log m - \log \epsilon}{-\log(1-\epsilon)} \right\rceil$$

gives the desired bound.

2. Let $a_u = |A_u|$. It will suffice to show that for any subset $\mathcal{B}$ of $\mathcal{Z}_p$ of size $k \leq d$,

$$\Pr(\bigwedge_{u \in \mathcal{B}} x_0 + x_1 u + x_2 u^2 + \cdots + x_{d-1} u^{d-1} \in A_u) = \prod_{u \in \mathcal{B}} \frac{a_u}{p} .$$

But

$$\begin{aligned}&\Pr(\bigwedge_{u \in \mathcal{B}} \sum_{i=0}^{d-1} x_i u^i \in A_u) \\ &= \frac{1}{p^d} \, |\{(x_0, \ldots, x_{d-1}) \mid \bigwedge_{u \in \mathcal{B}} \sum_{i=0}^{d-1} x_i u^i \in A_u\}| \\ &= \frac{1}{p^d} \sum_{z_u \in A_u,\ u \in \mathcal{B}} |\{(x_0, \ldots, x_{d-1}) \mid \bigwedge_{u \in \mathcal{B}} \sum_{i=0}^{d-1} x_i u^i = z_u\}| .\end{aligned}$$

Consider the $k \times d$ linear system

$$x_0 + x_1 u + x_2 u^2 + \cdots + x_{d-1} u^{d-1} = z_u , \quad u \in \mathcal{B} .$$

This can be represented in matrix form as

$$Ax = z$$

where A is a $k \times d$ submatrix of a $d \times d$ Vandermonde consisting of all rows

$$(1,\ u,\ u^2,\ \ldots,\ u^{d-1}) , \qquad u \in \mathcal{B} .$$

Since the Vandermonde is nonsingular, A is of full rank k. Its kernel is therefore a subspace of $\mathcal{Z}_p^d$ of dimension $d - k$, thus the affine subspace of