

1. (a) Flip coin in pairs, if the outcome is  $\langle \mathbf{head}, \mathbf{tail} \rangle$ , output  $\mathbf{head}$ , if the outcome is  $\langle \mathbf{tail}, \mathbf{head} \rangle$ , output  $\mathbf{tail}$ . Keep doing this until one of the above events occurs. The probability of the two final outcomes are the same and equal to  $p(1-p)$ , which means it is a well-defined unbiased coin. It is easy to verify that each pair of flips is a Bernoulli trial that terminates the process with probability  $2p(1-p)$ , thus the number of pairs of coin flips follows the classic geometric distribution, which implies it takes expectedly  $\frac{1}{2p(1-p)}$  pairs of flips to succeed, i.e. the expected number of coin flips is  $\frac{1}{p(1-p)}$ .
- (b) Given  $n$  coin flips, we denote by  $t$  the number of tails among them. For any specific  $n$  and  $t$ , the probability of each combination of  $t$  tails among  $n$  coins output  $\mathbf{tail}$  is the same and equals to  $p^{(1-t)}(1-p)^t$ . Therefore given  $n$  coin flips, among which there are exactly  $t$  tails, we can distill  $\lfloor \log_2 \binom{n}{t} \rfloor$  unbiased bits out of them, by mapping each combination of  $t$  tails to an assignment of  $\lfloor \log_2 \binom{n}{t} \rfloor$  bits.

The optimality of this scheme is supported by the fact that the expected number of distilled bits approaches the entropy of the sequence of coin flips.

2. Choose an integer  $t$  from  $[4n]$  uniformly at random. Check whether  $p(t) = q(t)$ . Note that  $p(x) - q(x)$  is a polynomial with degree at most  $n$ , which means  $p(x)$  and  $q(x)$  can only agree on at most  $n$  points if  $p \neq q$ . Therefore we are correct with probability at least  $3/4$ .

For deterministic algorithm, with less than  $2n$  calls (supposed that a call is the evaluation of one blackbox on a single input value), the adversary can always fool us by interpolating  $(p-q)$  arbitrarily.

3. Given the inputs of a set  $A$  of  $n$  elements and an integer  $k$ , the algorithm randomly pick an element  $x$  from  $A$  as the pivot. Let  $A^- = \{y \in A \mid y < x\}$  and  $A^+ = \{y \in A \mid y > x\}$ . If  $|A^-| = k$  return  $x$ , else if  $|A^-| > k$  recurse with the input  $A^-$  and  $k$ , and if  $|A^-| < k$  recurse with the input  $A^+$  and  $k - |A^-| - 1$ .

We denote by  $T(n)$  the expected number of comparisons. Obviously  $T(1) < 4$ . Suppose inductively that  $T(i) < 4i$  for all  $i < n$ .

$$\begin{aligned}
T(n) &\leq n + \frac{1}{n} \left( \sum_{i=1}^{k-2} T(n-i-1) + \sum_{i=k+1}^{n-1} T(i) \right) \\
&\leq n + \frac{4}{n} \left( \sum_{i=n-k+1}^{n-1} i + \sum_{i=k+1}^{n-1} i \right) \\
&\leq n + \frac{8}{n} \sum_{i=n/2+1}^{n-1} i \\
&\leq 4n.
\end{aligned}$$

4. Given a random graph  $G$ , and a structure  $H$  on specified vertices, let  $X_H$  be a random variable indicating whether  $H$  is in  $G$  (e.g.  $X_{uv}$  is the edge indicator of  $uv$ ). The expected number of triangles is

$$\mu = E \left( \sum_{\Delta} X_{\Delta} \right) = \sum_{u,v,w \in V, u < v < w} E(X_{uv} X_{vw} X_{uw}) = \frac{1}{8} \binom{n}{3}.$$

**Markov Inequality:**  $\Pr \left[ \sum_{\Delta} X_{\Delta} > 2\mu \right] < 1/2$ .

**Chebyshev Inequality:**

$$\text{var} \left( \sum_{\Delta} X_{\Delta} \right) = \sum_{\Delta_1, \Delta_2} \text{cov}(X_{\Delta_1}, X_{\Delta_2}).$$

For the  $\Delta_1$  and  $\Delta_2$  do not share edge, the corresponding random variables are independent and thus  $cov(X_{\Delta_1}, X_{\Delta_2}) = 0$ .

For the cases that  $\Delta_1 = \Delta_2$ ,  $cov(X_{\Delta_1}, X_{\Delta_2}) = E(X_{\Delta}^2) - E^2(X_{\Delta}) = 7/64$ .

For the  $\Delta_1$  and  $\Delta_2$  that share exact one edge  $uv$ ,

$$cov(X_{\Delta_1}, X_{\Delta_2}) = E(X_{uv}X_{vw}X_{uw}X_{vt}X_{ut}) - E(X_{uv}X_{vw}X_{uw})E(X_{uv}X_{vt}X_{ut}) = 1/64.$$

There are  $\binom{n}{3}$  many  $\Delta$  and  $12\binom{n}{4}$  many pairs of  $\Delta_1$  and  $\Delta_2$  that share exact one edge, thus

$$var\left(\sum_{\Delta} X_{\Delta}\right) = \frac{7}{64}\binom{n}{3} + \frac{12}{64}\binom{n}{4} = \frac{3n-2}{64}\binom{n}{3}.$$

By Chebyshev inequality,

$$\Pr\left[\sum_{\Delta} X_{\Delta} > 2\mu\right] \leq \frac{var\left(\sum_{\Delta} X_{\Delta}\right)}{(2\mu)^2} = \frac{3n-2}{4\binom{n}{3}}.$$

**Chernoff Bound:** Observe that  $\sum_{\Delta} X_{\Delta} > 2\mu$  implies that

$$\sum_{u \neq v} X_{uv} > \sqrt{2}E\left(\sum_{u \neq v} X_{uv}\right)$$

or  $\exists u \neq v, \sum_{w \notin \{u,v\}} X_{uw}X_{vw} > \sqrt{2}E\left(\sum_{w \notin \{u,v\}} X_{uw}X_{vw}\right).$

Both types of events can be bounded from above by Chernoff bound, and by union bound we have a  $n^2 \exp(-\Theta(n))$  upper bound on the probability that  $\sum_{\Delta} X_{\Delta} > 2\mu$ .

**Janson Inequality:** cf. “The infamous upper tail” by Janson *et al.*

5. Choose  $\sigma(i)$  for each  $i$  uniformly and independently at random. Use the deterministic routing algorithm for  $s$  steps to route messages from  $[n]$  to  $\sigma([n])$ , and apply the reversed deterministic routing algorithm for another  $s$  steps to rout messages from  $\sigma([n])$  to  $\mu([n])$ , note that we can do so because we have the global knowledge of the graph and the communication is bidirectional on each edge. For each  $i$ , the probability that it fails to reach  $\sigma(i)$  after the first  $s$  steps is obviously  $\epsilon$ , and the probability that it fails to reach  $\mu(i)$  from  $\sigma(i)$  is also  $\epsilon$ , because the distribution of  $\mu^{-1}\sigma(i)$  is the same as that of  $\sigma(i)$ , i.e.  $\sigma(i)$  is as chosen uniformly and independently at random with respect to each  $\mu(i)$ . Then by union bound the total probability of failure is  $2\epsilon$  for each  $i$ .
6. (a) The Contract algorithm chooses a particular min-cut with probability at least  $\frac{2}{n(n-1)}$ , therefore there cannot be more than  $\frac{n(n-1)}{2}$  min-cuts.
- (b) The algorithm remains the same except the following.
  - Run the Contract algorithm till there are  $2\alpha$  vertices left.
  - Choose a cut in the contracted graph uniformly at random among all cuts.

Follows the similar analysis, for any  $\alpha$ -approximate cut  $C$ ,

$$\Pr[\text{no edge in } C \text{ is contracted}] \geq \prod_{j=n}^{2\alpha+1} \left(\frac{j-2\alpha}{j}\right) = \frac{1}{\binom{n}{2\alpha}}$$

Note that there are at most  $2^{2\alpha}$  cuts in the  $2\alpha$  vertices contracted graph. The probability that an  $\alpha$ -approximate cut is chosen by the algorithm is thus no less than  $\frac{1}{2^{2\alpha}\binom{n}{2\alpha}}$ . Therefore there are at most  $2^{2\alpha}\binom{n}{2\alpha}$  many  $\alpha$ -approximate cuts.