CS3230 Tutorial 5

AY 25/26 Sem 1 — github/omgeta

Q1). Take $A = [1], B = [1]$ so $AB = [1]$ and $C = [0]$ so $C \neq AB$. Thus, we have $AB\vec{r} = r$ and $C\vec{r} = 0$, which means that when we pick $r = 1$ with probability $\frac{1}{2}$, we get $AB \neq C$ (correct) and when we pick $r = 0$ with probability $\frac{1}{2}$ we get $AB = C$ (false positive).

Q2). Case 1 ($S_A = S_B$): trivially $S_A \mod p = S_B \mod p$

Case 2 ($S_A \neq S_B$): Let $D = S_A - S_B$, then $S_A \mod p = S_B \mod p \implies p \mid D$
Since $S_A, S_B \leq 2^n$, then $D \leq 2^n$
Also since by prime factorisation theorem, D can be written uniquely as $D = p_1 p_2 \cdots p_k$ and all prime numbers are ≥ 2, then $D \geq 2 \cdot 2 \ldots \cdot 2 = 2^k$
Now, $2^k \leq D \leq 2^n \implies 2^k \leq 2^n \implies k \leq n \iff D$ has atmost n prime factors

$Pr[\text{failure}] = Pr[p \mid D] = \frac{\#\text{ distinct prime factors in } D}{\#\text{ of prime numbers } p} \leq \frac{k}{|S|} \leq \frac{n}{n^2} = \frac{1}{n}$
$\therefore Pr[\text{success}] \geq 1 - \frac{1}{n}$

Q3). Suppose not, that we send $m < n$ bits and test for equality.
If S_A was n bits we would have 2^n different messages, but with m bits we only have $2^m < 2^n$ different messages.
By Pigeonhole Principle, two different S_A now correspond to the same encoded message then Bob cannot distinguish between the 2 original messages.

Q4). For each edge e, denote indicator random variable $X_e = \begin{cases} 1 & \text{if } e \text{ crosses the cut} \\ 0 & \text{if } e \text{ does not cross the cut} \end{cases}$

$\therefore$ Total edges crossing the cut $= \sum_{e \in E} X_e$
By fixing the cut, $Pr[X_e = 1] = \frac{1}{2}$ so $E[X_e] = 1 \cdot P[X_e = 1] + 0 \cdot P[X_e = 0] = \frac{1}{2}$

Therefore, $E[\text{total edges crossing cut}] = E[\sum_{e \in E} X_e] = \sum_{e \in E} E[X_e] = \sum_{e \in E} \frac{1}{2} = \frac{|E|}{2}$

Q5). We don't guarantee V_1, V_2 are non empty sets. To fix this, we fix our original cut across the first edge e^*.

Therefore, $E[\sum_{e \in E} X_e] = \sum_{e \in E} E[X_e] = E[X_{e^*}] + \sum_{e \in E \setminus \{e^*\}} E[X_e] = 1 + \frac{|E| - 1}{2} = \frac{|E| + 1}{2} > \frac{|E|}{2}$