実践セキュリティ特論 II　Blockchain 理論　第二回課題

28G23027 川原尚己

1. 二値入力においてアルゴリズムが妥当であるとは，全ノードが同一の値vを入力として与えられた場合は決定値もvとなり，そうでない場合は0と1のいずれかが決定値として出力されることである．Algorithm1 はこの条件を満たす．
2. 十分大きなラウンド数が経過した時点では，各ノードが持つv_iは

$$\Pr[v_i = 0] = \Pr[v_i = 1] = \frac{1}{2}$$

である．Algorithm1 が停止するのは全てのv_iが同一値$v \in \{0,1\}$を持つときである．この事象が発生する確率は

$$\Pr[\text{Algorithm1 が停止}] = \Pr[v_1 = 0 \ \wedge \ldots \wedge v_n = 0] + \Pr[v_1 = 1 \wedge \ldots \wedge v_n = 1]$$

$$= \frac{1}{2^n} + \frac{1}{2^n}$$

$$= \frac{1}{2^{n-1}}$$

となり，非零の値を持つため Algorithm1 は有限のラウンドで停止する．また，停止に必要なラウンド数の期待値は，

$$O(1/\Pr[\text{Algorithm1 が停止}]) = O\left(\frac{1}{\frac{1}{2^{n-1}}}\right) = O(2^n)$$

となるから，$f(n) = 2^n$である．

3. 回答に必要な情報が不足していたため回答できませんでした．