Assignment 10

The due date for submitting this assignment has passed.

Due on 2021-03-31, 23:59 IST.

As per our records you have not submitted this assignment.

1) Consider GI, the graph isomorphism problem and GNI, the graph nonisomorphism problem. Which of the following statements is/are known to be true? *4 points*

- $GI \in AM$
- GI is NP complete
- $GNI \in IP$ with verifier's messages restricted to random bits.
- If GNI is $coNP$-complete, then PH collapses

No, the answer is incorrect.
Score: 0

Accepted Answers:
$GI \in AM$
$GNI \in IP$ with verifier's messages restricted to random bits.
If GNI is $coNP$-complete, then PH collapses

2) A number q is said to be a quadratic residue modulo m if there exists a number p such that $q = p^2 \pmod m$. Let QR be the language of pairs (q, m) such that q is a quadratic residue modulo m. Let QNR be the language of pairs (q, m) such that q is not a quadratic residue modulo m. All the numbers are given in binary. Which of the following options is true? *4 points*

- $QR \in IP$
- $QNR \in IP$
- When $m = 2$, QNR consists of pairs $(q, 2)$ for all $q \in \mathbb{N}$
- When $m = p$, an odd prime, then $QR \in P$

No, the answer is incorrect.
Score: 0

Accepted Answers:
$QR \in IP$
$QNR \in IP$
When $m = p$, an odd prime, then $QR \in P$

3) Select all the correct statement(s) *2 points*

- $AM \subseteq MA$
- $NP \subseteq MA$
- $MA \neq AM$
- $AM = BP \cdot NP$

No, the answer is incorrect.
Score: 0

Accepted Answers:
$NP \subseteq MA$
$AM = BP \cdot NP$

4) Which of the following is/are known to be true? *4 points*

- $AM[k] \subseteq IP[k]$ when k is a constant.
- $AM[\log n + 1] \subseteq AM[\log n]$
- $IP[k] \subseteq AM[k + 2]$ when $k = O(\log n)$
- $AM[\log \log n] = AM[2]$

No, the answer is incorrect.
Score: 0

Accepted Answers:
$AM[k] \subseteq IP[k]$ when k is a constant.
$AM[\log n + 1] \subseteq AM[\log n]$
$IP[k] \subseteq AM[k + 2]$ when $k = O(\log n)$

5) Which of the following changes does not preserve the class IP? *2 points*

- Making the prover probabilistic.
- Making the verifier deterministic.
- Changing the soundness parameter from 1/3 to 0
- Changing the completeness parameter from 2/3 to $1 - 1/2^{n^c}$ for some constant $c > 0$.

No, the answer is incorrect.
Score: 0

Accepted Answers:
Making the verifier deterministic.
Changing the soundness parameter from 1/3 to 0

6) Suppose a set S has cardinality p. Then, using the set lower bound protocol, which of the following is true? *4 points*

- Merlin can make Arthur accept that the size of S is atleast p with probability 2/3
- Merlin can make Arthur accept that the size of S is atleast $p/2$ with probability 2/3
- Merlin can make Arthur accept that the size of S is atleast p with probaility 1
- Merlin can make Arthur accept that the size of S is atleast $2p$ with probability 2/3

No, the answer is incorrect.
Score: 0

Accepted Answers:
Merlin can make Arthur accept that the size of S is atleast p with probability 2/3
Merlin can make Arthur accept that the size of S is atleast $p/2$ with probability 2/3
Merlin can make Arthur accept that the size of S is atleast p with probaility 1

7) Let $y_1, \ldots, y_n$ be uniform random bits. For each non empty set $S \subseteq [n]$, define $\chi_S = \oplus_{i \in S} y_i$. Then for two non empty subsets $A, B \subseteq [n]$, which of the following are true? *4 points*

- $Pr[\chi_A = 1 \wedge \chi_B = 0] = 1/4$
- $Pr[\chi_A = 1 \wedge \chi_B = 0] = 1/2$
- $Pr[\chi_A = 0] = 1/4$
- $Pr[\chi_A = 0] = 1/2$

No, the answer is incorrect.
Score: 0

Accepted Answers:
$Pr[\chi_A = 1 \wedge \chi_B = 0] = 1/4$
$Pr[\chi_A = 0] = 1/2$

8) If we denote the class $AM[3]$ by AMA, $AM[4]$ by $AMAM$ and so on, then the class $AMAMAMAMA \cup MAMAMAM$ is contained in which of the below classes? *2 points*

- MA
- AM
- IP
- BPP

No, the answer is incorrect.
Score: 0

Accepted Answers:
AM
IP