

Game theory: proofs, testing and equilibria

Homework – MPRI/M2R – February 2, 2006

This homework has to be made alone by each student of the class. The corresponding evaluation will contribute as 40% of the final evaluation. The language can be either french or english. All answers need to be argued, and all constructed algorithms to be analyzed.

In this homework, $\varepsilon > 0$ is any small enough constant.

Probabilistic Checkable Proofs

Let us define the following problem. Arithmetic operations are over the booleans $\{0, 1\}$, where the addition is the logical exclusive-or, and the multiplication is the logical and.

QP-SAT is the set of m -tuples of boolean quadratic polynomials (P_1, P_2, \dots, P_m) over n variables x_1, x_2, \dots, x_n , such that $P_1(a) = P_2(a) = \dots = P_m(a) = 0$ for some $a \in \{0, 1\}^n$.

Question 1 Show that **QP-SAT** is NP-complete, by showing that **QP-SAT** is in NP and that **3-SAT** can be reduced to **QP-SAT**. Test your reduction on the **3-SAT** instance $(x_1 \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3}) \wedge (\overline{x_1} \vee \overline{x_2} \vee x_3)$.

For any $a \in \{0, 1\}^n$, we define the binary word $\pi_a = (v \odot a)_{v \in \{0, 1\}^n}$ of length 2^n , where \odot denotes the inner product over booleans, and the binary word $a \circ a = (a_i a_j)_{1 \leq i, j \leq n}$ of length n^2 . Finally, we let $\Pi_a = (\pi_a, \pi_{a \circ a})$.

*Observe that in the lecture we have defined $a \circ a$ in a slightly different way by $a \circ a = (a_i a_j)_{1 \leq i < j \leq n}$, whose length is $2^{n(n-1)/2}$. Here we just require more informations which will be useful for **Question 5**. Therefore, take care while adapting the proofs that were given during the lecture.*

Question 2 Construct an $(O(n^2), O(1))$ -PCP-verifier for **QP-SAT** when the proof is assumed to be of the form Π_a . Run your verifier on the input $(P_1, P_2, P_3) = (x_1 x_2 + x_2 x_3 + 1, x_1 x_3 + x_1, x_1 + x_2 + x_3)$ and proofs corresponding to assignments $a = (0, 1, 1)$ and $a = (1, 1, 0)$.

Question 3 Construct a tester that, given a word $w \in \{0, 1\}^{2^n}$,

1. accepts w (with probability 1) if $w = \pi_a$, for some $a \in \{0, 1\}^n$,
2. rejects w with high probability, if it is at (normalized) Hamming distance more than ε to every words π_a , where $a \in \{0, 1\}^n$,

and that uses $O(m)$ random bits and looks at a constant number (depending only on ε) of bits of w .

Question 4 Construct the self-corrector corresponding to the above tester: given w at distance at most ε to some π_a , give a randomized algorithm that computes any bit of π_a using $O(n)$ random bits and looks at a constant number of bits of w .

Question 5 Let $a \in \{0, 1\}^n$ and $b \in \{0, 1\}^{n^2}$.

a) Prove that for every $w, w' \in \{0, 1\}^n$, $(a \odot w)(a \odot w') = (a \circ a) \odot (w \circ w')$.

b) Prove that when $b \neq a \circ a$, $\Pr_{w, w' \in \{0, 1\}^n} [(a \odot w)(a \odot w') \neq b \odot (w \circ w')] \geq 1/4$.

Question 6 Construct a tester that, given two words $w^1 \in \{0, 1\}^{2^n}$ and $w^2 \in \{0, 1\}^{2^{n^2}}$ that are known to be respectively at distance ε to π_a and π_b , for some unknown $a \in \{0, 1\}^n$ and $b \in \{0, 1\}^{n^2}$

1. accepts (w^1, w^2) (with probability 1) if $(w^1, w^2) = \Pi_a$, for some $a \in \{0, 1\}^n$,
2. rejects (w^1, w^2) with high probability, if w^2 is at (normalized) Hamming distance more than ε to $\pi_{a \circ a}$,

and that uses $O(n^2)$ random bits and looks at a constant number (depending only on ε) of bits of w .

Question 7 Construct the self-corrector corresponding to the above tester.

Question 8 The input size of an instance of **QP-SAT** is denoted by N . Construct an $(O(N^2), O(1))$ -PCP-verifier for **QP-SAT**, without any assumption on the proof.

Property Testing for Sorting

In this part we are considering n -array of integers $T = (T[1], T[2], \dots, T[n])$. We access to T by querying the value of $T[i]$ for some $i \in \{1, 2, \dots, n\}$. We assume that all arithmetic operations and random samplings in $\{1, 2, \dots, n\}$ are performed in one unit cost of time.

We suppose that all elements in T are distincts. We would like to check that T is sorted by increasing order, that is $T(1) < T(2) < \dots < T(n)$. We name this property \mathcal{P} .

We consider the following test.

Increasing Test(T, ε)

Repeat $O(1/\varepsilon)$ times

 Choose $i \in \{1, 2, \dots, n\}$ randomly

 Perform a binary search of $T[i]$ in T :

 Set $a = 1$ and $b = n$

 While $b > a + 1$

 If $T[i] < T[\lfloor (a+b)/2 \rfloor]$ then $b = \lfloor (a+b)/2 \rfloor$ else $a = \lfloor (a+b)/2 \rfloor$

 if $(T[a] \neq T[i] \text{ and } T[b] \neq T[i])$ or $(T[a] > T[b])$ then 'not found'

 If 'not found' then reject (and stop)

Accept

An integer $i \in \{1, 2, \dots, n\}$ is *good* if the binary search for $T[i]$ is successful.

Question 9 What is the query complexity to T and the time complexity of **Increasing Test**(T, ε).

Question 10 If at least ε fraction of i 's is not good, what is the probability that the test rejects.

Question 11 Let $1 \leq i < j \leq n$ be both good. Prove that $T[i] < T[j]$.

Question 12 Conclude that **Increasing Test**(T, ε) is an ε -tester of \mathcal{P} for the edit distance.

Question 13 In case when the elements of T are not distinct, modify **Increasing Test**(T, ε) so that it is still an ε -tester for \mathcal{P} , where strict inequalities $<$ have been replaced by weak inequalities \leq . Test your algorithm on the array $T = (1, 2, 3, 5, 7, 2, 2, 2, 9)$ and $\varepsilon = 1/4$.

Property Testing of Languages without Pattern

For a binary string $S \in \{0, 1\}^s$, where $s \geq 1$, we denote by L_S the language of binary strings that does not contain S as a (not necessarily continuous) substring. For instance $0101110111 \notin L_{000}$.

We will prove by induction on s that L_S is testable for the Hamming distance.

Question 14 Prove that L_S is testable when $s = 1$.

We now assume that $s \geq 2$. We define our inductive test where $w[i : -]$ denote the suffix of w from its i -th letter.

Language Test(w, S, ε)

If $|S| = 1$ then apply tester of **Question 14**

Sample $k = O(1/\varepsilon)$ integers i_1, i_2, \dots, i_k from $\{1, 2, \dots, n\}$

Test if there is some i_j such that $w_{i_j} = S_1$

If no then accept

Let a be the smallest i_j such that $w_{i_j} = S_1$

Run **Language Test**($w[a : -], S[2 : -], \varepsilon/2$)

Question 15 We assume for simplicity in this question that $S_1 = 1$. Prove that if a bit '1' is found in **Language Test**(w, S, ε) (before the induction), then with high probability the sequence $w_1 w_2 \dots w_a$ contains no more than $\varepsilon n/2$ bits '1', where n is the length of w .

Question 16 Prove that **Language Test**(w, S, ε) is an ε -tester of L_S for the Hamming distance.