ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Institute of Theoretical Computer Science
Thomas Holenstein, Ueli Maurer, Angelika Steger, Emo Welzl, Peter Widmayer

Algorithms, Probability, and Computing — Final Exam — HS13

Candidate

First name: .....

Last name: .....

Student ID (Legi) Nr.: .....

I attest with my signature that I was able to take the exam under regular conditions and that I have read and understood the general remarks below.

Signature: .....

General remarks and instructions

1. You can solve the four tasks in any order. Begin by reading all tasks carefully. They are not ordered by difficulty or in any other meaningful way.
2. Check your exam documents for completeness (2 cover pages and 3 pages with 4 tasks).
3. Immediately inform an assistant in case you are not able to take the exam under regular conditions or if anything disturbs you. Later complaints are not accepted.
4. Pencils are not allowed. Pencil-written solutions will not be reviewed. Do not use red pens: this color is reserved for corrections.
5. No auxiliary material allowed. All electronic devices must be turned off and are not allowed to be on your desk. We will write the current time on the blackboard every 15 minutes.
6. Attempts to cheat/defraud lead to immediate exclusion from the exam and can have judicial consequences.
7. Provide only one solution to each task. Cancel invalid solutions clearly.
8. **All solutions must be understandable and well-founded. Write down the important thoughts in clear sentences and keywords. No points will be awarded for unfounded or incomprehensible solutions. You can write your solution in English or German.**
9. You may use anything that has been introduced and proved in the lecture without re-proving it. However, if you need something *different* than what we have in the notes, you must write a new proof or at least list all necessary changes.
10. Write your student-ID (**Legi-number**) on **all** sheets (and your name only on this cover sheet).

Good luck!

	achieved points (maximum)	reviewer's signature
1	(25)	
2	(25)	
3	(25)	
4	(25)	
Σ	(100)	

Task 1: Assorted Tasks (25 points)

(a) Prove that every triangulation on n vertices has at least 2^{n-1} Pfaffian orientations.

(b) Let L be a set of n horizontal and vertical lines in the plane. Consider a point $q \in \mathbb{R}^2$ and a uniformly random permutation $\ell_1, \ldots, \ell_n$ of L. Let X be the number of times the arrangement cell containing q changes when we insert the lines one by one in the order $\ell_1, \ldots, \ell_n$. Prove that $\mathbf{E}[X] \in O(\log n)$.

(c) Compute the expected number of nodes in a random binary search tree with n nodes that have a left child but no right child.

(d) Consider a ClSP F on n variables and $m = |F|$ clauses. Suppose that the dependency graph of F contains no edges. Consider a finite prefix $\mathcal{C}_t = \langle C_1, \ldots, C_t \rangle$ of a journal corresponding to an execution of of the Local-Lemma-Solver on F. In the lecture, we associated one or more witness trees T with each $\mathcal{C}_t$. Give a (graph-theoretic) chracterization of the set of such witness trees and prove that your answer is correct.

Task 2: Circuit-SAT Verification (25 points)

Please refer to Figure 1, which describes the algorithms **Local Decoding** and **Circuit-SAT Verifier**. Recall that the correctness of the latter proves the Baby PCP Theorem. In this task, we consider a variation where the circuit can have AND-gates in addition to NAND-gates. Formally, we consider the following modification to the Baby PCP Theorem (changes underlined).

Theorem 1 (Modified Baby PCP Theorem). *There exists $q \in \mathbb{N}$, $\rho > 0$, and a polynomial time verifier $V^w(C)$ with the following properties. The verifier reads the description of its input C, a circuit with input-gates, AND-gates and NAND-gates (n gates in total), tosses some random coins, queries w at most q times, then accepts or rejects.*

- *If $C(y) = 1$ for some y, then there exists a $w : \{0,1\}^{n^2} \to \{0,1\}$ such that $V^w(C)$ accepts with probability 1.*
- *If $C(y) = 0$ for all y then for every $w : \{0,1\}^{n^2} \to \{0,1\}$ the probability that $V^w(C)$ rejects is at least ρ.*

Solve the following subtasks.

(a) Modify the code of **Circuit-SAT Verifier** to obtain a verifier $V^w(C)$ as described in Theorem 1. For this subtask, it is sufficient to describe the changes in the pseudocode: you do not have to prove correctness.

Hint: modifying the circuit does not help. You cannot simply replace each AND-gate by two NAND-gates, since this increases the size of the circuit (and the input size of w is prescribed).

(b) Prove: if C is unsatisfiable and $w(M) = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{n} y_i y_j M_{i,j}$ for some $y \in \{0,1\}^n$, then your verifier $V^w(C)$ rejects with probability at least $1/2$.

Task 3: Coloring Points in the Plane (25 points)

Consider a set of n (uncolored) points and a set of n disks in the plane. In this task, we will color the points red and blue. We say that a disk D is *monochromatic* if all the points inside D have the same color. A 2-coloring of the points is *proper* if no disk is monochromatic.

(a) Suppose that every disk contains more than $\log n + 1$ points. Prove that there exists a proper 2-coloring.

In the remainder, suppose that every disk contains at least 6 points and intersects at most 9 other disks.

(b) Prove that there exists a proper 2-coloring.

(c) Suppose that some points already have a color that you are not allowed to change. Specifically, exactly one point in each disk is precolored.

Give an expected $O(n^2)$-time algorithm to extend such a partial coloring to a proper coloring of all points. Prove that your algorithm is correct and that it achieves the desired running time.

Task 4: Cryptographic Reductions (25 points)

Let p_1, p_2 be two primes and $m = p_1 p_2$.

(a) Formalize the search problem of finding a square root of $y = x^2$ for an x chosen u.a.r. in $\mathbb{Z}_m^*$ as a game S_m.

(b) Prove that S_m is clonable.

(c) Prove that S_m is random self-reducible.

(d) Let $q \in \mathbb{N}$. Describe a function ϕ that maps efficient winners to efficient winners[1] such that

$$S_m \preceq^{(\phi,\psi_q)} S_m$$

for

$$\psi_q(\alpha) = 1 - (1-\alpha)^q.$$

You do not have to prove that your function has the required properties.

[1] For this task you may assume that if two systems S_1 and S_2 are efficient, then so are $S_1 S_2$ and S_1^n for any $n \in \mathbb{N}$.

Local Decoding $\mathrm{LD}^w(x)$:

Input: An element $x \in \{0,1\}^m$.
Oracle: A function $w : \{0,1\}^m \to \{0,1\}$.

$y \leftarrow \{0,1\}^m$.
return $w(y) \oplus w(x \oplus y)$.

Circuit-SAT Verifier $V^w_{\text{Circuit-SAT}}(C)$:

Input: Circuit C with:

- Input-Gates $1, \ldots, k$,
- NAND-GATES $k+1, \ldots, n$, given by $y_i = y_{\ell(i)} \overline{\wedge} y_{r(i)}$,
- Output gate n.

Oracle: A function $w : \{0,1\}^{n^2} \to \{0,1\}$.

$R_1 \leftarrow \{0,1\}^{n^2}$
$R_2 \leftarrow \{0,1\}^{n^2}$
if $w(R_1) \oplus w(R_2) \neq w(R_1 \oplus R_2)$ **then** (Linearity Test)
    return *reject*

$a \leftarrow \{0,1\}^n$
$b \leftarrow \{0,1\}^n$
if $\left(\mathrm{LD}^w(\mathrm{diag}(a)) \wedge \mathrm{LD}^w(\mathrm{diag}(b))\right) \neq \mathrm{LD}^w(a \cdot b^T)$ **then** (Check Form)
    return *reject*

$G \subseteq_R \{k+1, \ldots, n\}$
$M := \bigoplus_{i \in G} (E_{i,i} \oplus E_{\ell(i),r(i)})$
if ($|G|$ even and $\mathrm{LD}^w(M) \neq 0$) **or** ($|G|$ odd and $\mathrm{LD}^w(M) \neq 1$) **then** (Check Gates)
    return *reject*

if $\mathrm{LD}^w(E_{n,n}) \neq 1$ **then**
    return *reject* (Check Output)
return *accept*

Figure 1: The verifier used in the proof of the Baby PCP Theorem. For a vector $v \in \{0,1\}^n$, $\mathrm{diag}(v)$ is the $n \times n$-matrix which has v on the diagonal and zeros elsewhere. The $n \times n$-matrix $E_{i,j}$ has a one in position (i,j) and zeros elsewhere.