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

January 28, 2013

Algorithms, Probability, and Computing Fall 2012 Final Exam

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 5 exercises in any order. We recommend that you read all tasks. 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 containing 5 exercises).
3. Immediately inform an assistant in case you are not able to take the exam under regular conditions. Later complaints are not accepted.
4. Pencils are not allowed. Pencil-written solutions will not be reviewed.
5. No auxiliary material allowed.
6. Attempts to cheat/defraud lead to immediate exclusion from the exam and can have judicial consequences.
7. Provide only one solution to each exercise. 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 (except in the multiple-choice parts). You can write your solution in English or German.**
9. You do not need to reprove things thats were already proved in the lecture. But if you want to prove something *different* then you must point out all details that need to be done differently in your proof.
10. Make sure to write your student-ID (**Legi-number**) on **all** the sheets (but **your name only on this cover sheet**).

Good luck!

	achieved points (maximum)	reviewer's signature
1	(30)	
2	(30)	
3	(30)	
4	(30)	
5	(30)	
Σ	(150)	

Exercise 1 - Multiple Choice (30 Pts)

Consider the following 6 claims and mark the corresponding boxes. Grading: 2 points for a correct marking without a correct justification, 5 points for a correct marking with a correct short justification, and -2 points for a wrongly marked box (you will receive non-negative total points in any case).

(a) Consider a set L of n lines in the plane. It is possible to preprocess L with $O(n)$ *storage* to answer the following query in time $O(\log n + k)$: For a query point q report all lines l where q lies above l; k is the number of such lines.

[ ] True [ ] False

Justification: ....

....

(b) There exists a graph G s.t. if we orient every edge uniformly at random (mutually independent), the resulting orientation $\overrightarrow{G}$ is Pfaffian with probability exactly $\frac{1}{7}$.

[ ] True [ ] False

Justification: ....

....

(c) Remember that for a binary random variable X the *bias* $b(X)$ is defined as $1 - 2\,\mathbf{E}[X]$.
Let X and Y be two (possibly dependent) binary random variables. Then $b(X \oplus Y) \leq b(X)b(Y)$.

[ ] False [ ] True

Justification: ....

....

(d) For *any* satisfiable ClSP F, the Local-Lemma-Solver from the lecture terminates with probability 1.

[ ] False [ ] True

Justification: ....

....

(e) Analogous to the lecture, we call a function $f : \{0,1\}^n \to \{0,1\}^n$ *linear* if $f(x) \oplus f(y) = f(x \oplus y)$ for all $x, y \in \{0,1\}^n$ (where $\oplus$ means componentwise XOR).
There are $2^{(n^2)}$ *linear* functions from $\{0,1\}^n$ to $\{0,1\}^n$.

[ ] True [ ] False

Justification: ....

....

(f) Let X_0 and X_1 be two random variables with some (finite) range $\mathcal{X}$. If $\Delta^D(X_0, X_1) \leq \varepsilon$ for all distinguishers D, then $\delta(X_0, X_1) \leq \varepsilon$.[1]

[ ] False [ ] True

Justification: ....

....

[1] Recall that $\Delta^{\cdot}(\cdot,\cdot)$ denotes the distinguishing advantage and $\delta(\cdot,\cdot)$ the statistical distance.

Exercise 2 - Cryptography (30 Pts)

(a) Phrase the computational Diffie-Hellman problem as a game and prove that it is random self-reducible.

(b) Consider a function $f : \{0,1\}^n \to \{0,1\}^n$ and define

$$g : \{0,1\}^{4n} \to \{0,1\}^{3n}, (w, x, y, z) \mapsto (f(x \oplus y), z, f(x) \oplus w)).$$

Recall that $\mathcal{I}^f$ denotes the inversion problem for f. Show that

$$\mathcal{I}^f \quad \preceq^{(\phi,=)} \quad \mathcal{I}^g$$

and

$$(\mathcal{I}^f)^2\wedge \quad \preceq^{(\phi',=)} \quad \mathcal{I}^g$$

for some efficiency-preserving ϕ, ϕ'.[2] Which of the two reductions is more useful when one is interested in proving that g is harder to invert than f, and why?

Exercise 3 - Randomized Checking of Quadratic Forms (30 Pts)

Let $\mathrm{GF}(2)^{n\times n}$ denote the set of $n \times n$ matrices over $\mathrm{GF}(2)$.

Consider the term $x^T Ax$ for $x \in \mathrm{GF}(2)^n$, $A \in \mathrm{GF}(2)^{n\times n}$.

(a) Let $n = 2$. Give a matrix A such that for $x \in_{\text{u.a.r.}} \mathrm{GF}(2)^2$,

$$\Pr\left[x^T Ax = 1\right] = \frac{1}{4}$$

(b) For general n, let $A \in_{\text{u.a.r.}} \mathrm{GF}(2)^{n\times n}$. Show that for a given $x \neq 0$,

$$\Pr\left[x^T Ax = 0\right] = \frac{1}{2}$$

(c) What is $\Pr\left[x^T Ax = 0\right]$, if x and A are chosen independently uniformly at random?

[2] The exact efficiency notion is not relevant for the solution, but to exclude inefficient solutions, your solution should work for the standard poly-time notion: If W is implementable by a poly-time algorithm, then $\phi(W)$ and $\phi(W')$ must be as well.

Exercise 4 - Limited Verifier Capabilities (30 Pts)

Let L be a language and $V(x, w)$ a polynomial time verifier with the following properties. The verifier expects a proof w of size polynomial in $|x|$ for the statement $x \in L$. It first reads x, tosses $\mathcal{O}(\log |x|)$ random coins and reads at most q bits of the proof. If at least two of the read bits are 1, then it accepts. Otherwise it either accepts or rejects. If $x \in L$, then there exists a proof w such that the verifier accepts with probability 1. If $x \notin L$, then for all w, the verifier rejects with probability at least some constant $\rho > 0$.

The goal of this exercise is to show that in this case $L \in \mathrm{P}$, i.e. there is a polynomial time algorithm deciding the language.

(a) Prove that $L \in \mathrm{P}$ under the assumption that V reads *at most one* bit (i.e. V always reads either zero or exactly one bit).

(b) Prove that $L \in \mathrm{P}$ under the assumption that V *never* reads *exactly one* bit (i.e. V always reads either zero or at least two bits).

(c) Prove that $L \in \mathrm{P}$ without the assumptions of (a) and (b).

HINT: Start with the solution for (b) and modify it to accomodate the case when V reads exactly one bit.

Exercise 5 - A Simple Random Process (30 Pts)

Let $n \in \mathbf{N}$ and let $k_0 := n$.

We consider the following random process: First we choose a number $k_1 \in_{\text{u.a.r.}} [k_0]$, then a number $k_2 \in_{\text{u.a.r.}} [k_1]$, ... In general, we choose $k_{i+1} \in_{\text{u.a.r.}} [k_i]$ until we have reached $k_N = 1$. If we start with $n = 1$ then we terminate immediately and hence $N = 0$.

Let $t_n := \mathbf{E}[N]$ (in terms of n), i.e. the expected number of numbers chosen altogether when starting with n.

(a) Determine t_1, t_2 and t_3.

(b) For $n \geq 2$, write t_n as a function of $t_1, \ldots, t_{n-1}$.

(c) For $n \geq 3$, write t_n as a function of t_{n-1}.

(d) Determine t_n.