Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Departement Informatik
Wintersession 2019

Prof. Ueli Maurer

Exam
Diskrete Mathematik

21. Januar 2019

Hinweise:

1.) **Erlaubte Hilfsmittel:** Selbstverfasste, handgeschriebene Notizen auf 6 A4-Seiten. Es ist erlaubt ein Wörterbuch zu benutzen. Es sind keine weiteren Hilfsmittel erlaubt (auch kein Taschenrechner).

2.) Die Prüfung besteht aus 5 Aufgaben mit total 90 Punkten. Die Aufgaben sind in drei Schwierigkeitsstufen von ($\star$) bis ($\star\star\star$) eingeteilt.

3.) Die Aufgaben sind direkt auf dem Prüfungsblatt zu lösen. Bei Platzmangel befinden sich am Ende der Prüfung vier Zusatzblätter. Weitere Zusatzblätter können während der Prüfung bei uns bezogen werden. **Nur von uns verteilte Zusatzblätter sind erlaubt.**

4.) Bitte einen dokumentenechten Stift verwenden (also kein Bleistift) und nicht die Farben Rot oder Grün verwenden.

5.) Die Legi bitte für die Ausweiskontrolle auf den Tisch legen.

6.) Bis 10 Minuten vor Ende der Prüfung darf man vorzeitig abgeben und den Raum still verlassen.

7.) Mobiltelefone und Smartwatches müssen komplett ausgeschaltet sein (kein Stand-By).

Prüfungs-Nr.

Stud.-Nr.:

Name:

Unterschrift:

Korrektur:

	Punkte		Unterschrift	
Aufgabe	Max	Erreicht	Korr.	Ver.
1	23			
2	16			
3	23			
4	24			
5	4			
Total	90			

Task 1. Sets, Relations and Functions .... **23 Points**

a) ($\star$) Short questions. Each correct answer gives one point. *(3 Points)*

1.) What is the number of elements in the set $\{1,2\} \times \{1,(2,3)\}$?

2.) What is the number of elements in the set $\mathcal{P}(\varnothing) \setminus \varnothing$?

3.) List all elements in the set $\mathcal{P}(\{\{\varnothing\},\varnothing\})$.

b) ($\star$) Prove that for any sets A, B, C, we have $(A \setminus B) \setminus C = A \setminus (B \cup C)$. *(2 Points)*

c) ($\star$) Prove or disprove: if ρ and σ are partial order relations on a set A, then $\rho \cup \sigma$ is a partial order relation on A. *(2 Points)*

d) Let ρ be a relation on a set A (both A and ρ are non-empty). Is it possible that (justify your answers):

1.) ($\star$) $\widehat{\rho} = (A \times A) \setminus \rho$ ☐ Yes ☐ No *(2 Points)*

2.) ($\star$) ρ is both symmetric and antisymmetric ☐ Yes ☐ No *(2 Points)*

e) Let ρ and σ be two equivalence relations on a set A. Prove that if $\rho \circ \sigma = \sigma \circ \rho$ then $\rho \circ \sigma$ is an equivalence relation. That is, prove that it is reflexive, symmetric and transitive.

($\star$) **reflexive:** *(1 Point)*

($\star\star$) **symmetric:** *(3 Points)*

($\star\star\star$) **transitive:** *(4 Points)*

f) ($\star\star$) We call a function $f : \mathbb{N} \to \mathbb{N}$ a zigzag function if for all $n > 0$, we have: if $f(n-1) < f(n)$ then $f(n) > f(n+1)$, and if $f(n-1) > f(n)$ then $f(n) < f(n+1)$ (that is, the function alternates between bigger and smaller values). Is the set of all zigzag functions countable? Prove your answer.

(4 Points)

Task 2. Number Theory .... **16 Points**

a) ($\star$) Compute $|Z_{56}^*|$. *(1 Point)*

b) ($\star$) Show that 10 divides $(43^{43} - 17^{17})$. *(2 Points)*

c) ($\star\,\star$) The RSA public key of Alice is $(n, e) = (77, 7)$. Compute her secret key d. *(3 Points)*

d) ($\star\,\star$) Find **all** solutions x to the following system of modular congruences, satisfying $0 \leq x < 180$. Justify why you listed all solutions. *(5 Points)*

$$\begin{aligned} x &\equiv_{15} 2 \\ x &\equiv_{12} 8 \end{aligned}$$

e) $(\star\star\star)$ Prove that if G is a subgroup of $\langle \mathbb{Z}; + \rangle$, then $G = \{n \cdot d \mid n \in \mathbb{Z}\}$ for some $d \in \mathbb{Z}$. *(5 Points)*

Task 3. Algebra .... **23 Points**

a) ($\star$) Short questions. Each correct answer gives half a point. *(5 Points)*

1.) Does there exist a non-abelian group of order 47? ☐ Yes ☐ No

2.) Is $\langle \mathbb{Z}_{12}; + \rangle$ isomorphic to $\langle \mathbb{Z}_2; + \rangle \times \langle \mathbb{Z}_6; + \rangle$? ☐ Yes ☐ No

3.) Is $\langle \mathbb{Z}_{12}; + \rangle$ isomorphic to $\langle \mathbb{Z}_3; + \rangle \times \langle \mathbb{Z}_4; + \rangle$? ☐ Yes ☐ No

4.) Find a group isomorphic to $\mathbb{Z}_{18}$ other than $\mathbb{Z}_{18}$.

5.) List all subgroups of $\langle \mathbb{Z}_6; + \rangle$.

6.) Find all units in the ring $\mathbb{Z}[x]$.

7.) Find all zero divisors in the ring $\mathbb{Z}_{12}$.

8.) Determine all roots of $2x^2 + 3x + 1 \in \mathbb{Z}_5[x]$.

9.) Find $m(x) \in \mathbb{Z}_5[x]$ such that $\mathbb{Z}_5[x]_{m(x)}$ is a field.

10.) List the elements of $\mathbb{Z}_2[x]_{x^2+x+1}$.

b) ($\star\,\star$) Let $\langle G; * \rangle$ be a group and let $H := \{a \in G \mid \forall b \in G \; a * b = b * a\}$. Prove that H is a subgroup of G. *(5 Points)*

c) ($\star\,\star$) Is it possible that $F[x]$ is a field if F is a field with at least two elements? Prove your answer. *(3 Points)*

☐ Yes ☐ No

d) ($\star\,\star$) Consider the ring $R := \mathbb{Z}_7[x]_{x^2+x+1}$.

1.) Find the multiplicative inverse of $2x + 1 \in R^*$. *(3 Points)*

2.) List the elements of $R \setminus R^*$. Justify your answer. *(3 Points)*

e) ($\star\,\star$) Let $\langle R; +, -, 0, \cdot, 1\rangle$ be any ring such that $a^2 = a$ for all $a \in R$. Prove that $a + a = 0$ for all $a \in R$. *(4 Points)*

Task 4. Logic .... **24 Points**

a) ($\star$) Let $F := ((A \to B) \to C) \vee (C \leftrightarrow \neg A)$. Find an equivalent formula in CNF (no justification is necessary). *(2 Points)*

b) ($\star$) Let $G := ((A \vee B) \to (B \wedge C)) \;\vee\; ((A \vee B) \wedge (A \vee \neg C)) \;\vee\; (A \wedge B)$. Using the resolution calculus, prove that G is **valid**. *(5 Points)*

c) ($\star$) Extend the syntax and semantics of propositional logic by the symbol $\downarrow$, denoting the not-or (NOR) operation ($A \downarrow B$ is true if and only if both A and B are false). *(1 Point)*

For every formula, there exists an equivalent formula that contains only the operation $\downarrow$. To prove this, for given formulas F and G, find formulas that contain only the operation $\downarrow$, and that are equivalent to $\neg F$, to $F \vee G$ and to $F \wedge G$. *(3 Points)*

$\neg F \equiv$

$F \vee G \equiv$

$F \wedge G \equiv$

d) ($\star$) Let the sequence $F_0, F_1, \ldots$ of formulas be defined as follows: $F_0 := A$ and $F_{i+1} := (F_i \to A)$ for $i \geq 0$. Determine the truth table of F_{2019}. *(2 Points)*

e) ($\star$) Find a formula F in predicate logic **with equality**, such that:

1.) In every model for F, the universe has at least 2 elements. *(1 Point)*

2.) F contains a binary function symbol f and a constant function symbol e, and for every model $\mathcal{A}$ for F, it holds that $\langle U^{\mathcal{A}}; f^{\mathcal{A}}, e^{\mathcal{A}}\rangle$ is a monoid. *(2 Points)*

f) ($\star\,\star$) Find a formula F in predicate logic **without equality**, such that in every model for F, the universe has at least 2 elements. *(1 Point)*

g) ($\star$) For the formula $F := P(x,x) \ \wedge\ \exists x\ ((\forall x\ P(x,y)) \to Q(x))$, give an equivalent formula in the prenex normal form. *(2 Points)*

h) ($\star\,\star$) Let $F := \forall x\ \Big(P(x, f(x))\ \vee\ \exists y\ \neg P(x,y)\Big)$. Is F a tautology? Prove your claim. *(5 Points)*

☐ Tautology ☐ Not a tautology

Task 5. Proof Patterns .... 4 Points

a) ($\star\star$) Let $a_1, \ldots, a_n$ be any integers. Prove that there exists a sequence $a_i, a_{i+1}, \ldots, a_j$ for some $1 \le i \le j \le n$, such that the sum $a_i + a_{i+1} + \cdots + a_j$ is divisible by n. *(4 Points)*

Hint: Use the pigeonhole principle.

Additional page: Use this sheet in case the space on the exercise sheets is not sufficient. Always indicate the number of the exercise you solve (for example, “Task 3 b)”).

Additional page: Use this sheet in case the space on the exercise sheets is not sufficient. Always indicate the number of the exercise you solve (for example, “Task 3 b)”).

Additional page: Use this sheet in case the space on the exercise sheets is not sufficient. Always indicate the number of the exercise you solve (for example, “Task 3 b)”).

Additional page: Use this sheet in case the space on the exercise sheets is not sufficient. Always indicate the number of the exercise you solve (for example, “Task 3 b)”).