Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Departement Informatik
Wintersession 2020

Prof. Ueli Maurer

Exam
Diskrete Mathematik

31. Januar 2020

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 4 Aufgaben mit total 140 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	38			
2	22			
3	41			
4	39			
Total	140			

Task 1. Sets, Relations and Functions..38 Points

a) Short Questions. No justification is required.

1.) List the elements of the set $P(\varnothing \cup \{\varnothing\})$. *(1 Point)*

2.) List the elements of the set $\{(1,1),1\} \times \{1\}$. *(1 Point)*

3.) We consider the relation $\rho = \{(a,b),(a,c),(c,a)\}$ on the set $\{a,b,c\}$. List the elements of

a) $\widehat{\rho}$: *(1 Point)*

b) ρ^2 : *(1 Point)*

c) ρ^* : *(1 Point)*

4.) If a relation ρ on a non-empty set A is **not** refexive, then it is irreflexive. *(1 Point)*

□ True □ False

5.) Find a relation on $\mathbb{N}$ which is both a partial order and an equivalence relation. *(1 Point)*

6.) The set $\mathbb{N} \times \mathbb{Q}$ is countable. *(1 Point)*

□ True □ False

7.) The set $\{0,1\}^\infty \setminus \{0,1\}^*$ is countable. *(1 Point)*

□ True □ False

b) ($\star$) We consider the poset $(\{1,2,3,4,9,42\}; |\ )$.

1.) Draw the Hasse diagram of the above poset. *(2 Points)*

2.) List all lower bounds of the set $\{3,9,42\}$. *(1 Point)*

c) ($\star$) Prove that $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$. Use the laws for logical operators. *(5 Points)*

d) ($\star\,\star$) Let $(A; \preceq)$ and $(B; \sqsubseteq)$ be two totally ordered posets. Prove that the poset $(A \times B;\ \leq_{\text{lex}})$ is also totally ordered, where $\leq_{\text{lex}}$ is the lexicographic order. (You do **not** have to prove that $\leq_{\text{lex}}$ is a partial order.)

Hint: Recall that $\leq_{\text{lex}}$ is defined by $(a_1, b_1) \leq_{\text{lex}} (a_2, b_2) \overset{\text{def}}{\iff} a_1 \prec a_2\ \lor (a_1 = a_2 \land\ b_1 \sqsubseteq b_2)$. *(5 Points)*

e) ($\star\,\star$) Using the diagonalization argument, prove that $\{0, 1, 2\}^\infty$ is uncountable. *(8 Points)*

f) $(\star\star)$ Let $f : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ be any function. Prove that either the image of f, $Im(f)$, is uncountable or there exists an $A \in \mathcal{P}(\mathbb{N})$ such that $f^{-1}(\{A\})$ is uncountable (or both). *(8 Points)*

Task 2. Number Theory .... **22 Points**

a) Short Questions. No justification is required.

1.) Compute the number of elements in $\mathbb{Z}_{12}^*$. *(1 Point)*

2.) Compute $R_{18}(37^{42})$. *(1 Point)*

3.) Compute $R_{11}(2^{3^{40}})$. *(2 Points)*

b) ($\star$) Is the function $f : \mathbb{Z}_{48} \to \mathbb{Z}_6 \times \mathbb{Z}_8$ defined by $f(x) = (R_6(x), R_8(x))$ a surjection? Prove your answer. *(5 Points)*

☐ Yes ☐ No

c) ($\star\,\star$) Prove that for all $a, b, c \in \mathbb{Z} \setminus \{0\}$, if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$. *(6 Points)*

d) ($\star\,\star$) Prove that for all $n \geq 2$, if n is not divisible by 3, then $n^2 + 2^n$ is not prime. *(7 Points)*

Task 3. Algebra .... 41 Points

a) Short Questions. No justification is required.

1.) The set $\mathcal{P}(\mathbb{N})$ with the operation $\cap$ is a monoid (for some neutral element). *(1 Point)*

☐ True ☐ False

2.) The set $\mathcal{P}(\mathbb{N})$ with the operation $\cap$ is a group (for some neutral element and some inverse operation). *(1 Point)*

☐ True ☐ False

3.) The group $\langle \mathbb{Z}_4; \oplus \rangle \times \langle \mathbb{Z}_6; \oplus \rangle$ is cyclic. *(1 Point)*

☐ True ☐ False

4.) List all elements of the subgroup of $\langle \mathbb{Z}_{15}^*; \odot \rangle$ generated by 4. *(1 Point)*

5.) List all subgroups of $\langle \mathbb{Z}_7^*; \odot \rangle$. *(3 Points)*

6.) List all units of the ring $\mathbb{Z}_7[x]$. *(2 Points)*

7.) Compute $\left| \mathrm{GF}(3)[x]_{x^2+x+2} \right|$. *(1 Point)*

8.) True or false: For all polynomials $a(x), b(x) \in \mathbb{Z}_{12}[x]$, if $\deg(a(x)) = \deg(b(x)) = 2$, then $\deg(a(x)b(x)) = 4$. *(2 Points)*

☐ True, because ☐ False, a counterexample is

9.) Find all roots of $a(x) = 2x^2 + 3x + 2 \in \mathrm{GF}(7)[x]$. *(1 Point)*

b) $(\star\star)$ Let $\langle G; *, \widehat{\ }, e\rangle$ be a group and let H be a subgroup of G. We define the relation $\approx$ on G as follows:

$$a \approx b \overset{\text{def}}{\iff} a * \widehat{b} \in H.$$

Prove that $\approx$ is an equivalence relation. *(8 Points)*

c) $(\star\star)$ Let $\langle R; +, -, 0, \cdot, 1\rangle$ be any ring such that $a \cdot a = a$ for all $a \in R$. Using only the definition of a ring, prove that R is commutative. *(10 Points)*

Hint: Prove first that $a + a = 0$ for all $a \in R$.

d) 1.) ($\star\,\star$) Find a polynomial $m(x)$ of degree 5 such that $F = \mathrm{GF}(2)[x]_{m(x)}$ is a field. Prove your answer. *(7 Points)*

2.) ($\star\,\star$) Find a generator of F^*. Prove your answer. *(3 Points)*

Task 4. Logic .... **39 Points**

a) Short Questions. No justification is required.

1.) Let $F = A \leftrightarrow B$. Give an equivalent formula in DNF. *(1 Point)*

2.) Find a model for the formula $(A \rightarrow B) \vee C$ of propositional logic. *(1 Point)*

3.) The following formula is a tautology: $A \rightarrow (\neg A \rightarrow B)$. *(1 Point)*

☐ True ☐ False

4.) Find a model for the formula $\forall x\ P(f(x), y)$ of predicate logic. *(1 Point)*

5.) The expression $\forall x\,(P(y) \equiv Q(y))$ is a formula. *(1 Point)*

☐ True ☐ False

6.) The statement $\forall x\ (F \wedge G) \models (\forall x\ F) \wedge (\forall x\ G)$ is true for all formulas F and G. *(1 Point)*

☐ True ☐ False

b) ($\star$) Find a formula in the prenex normal form which is equivalent to the folloing formula: $\neg\forall x(P(x) \vee \neg Q(y)) \wedge \exists y(P(x) \vee Q(y))$. *(4 Points)*

c) ($\star\,\star$) Find a formula F of predicate logic with equality which contains the binary function symbol f and a constant symbol e, such that a structure $\mathcal{A}$ is a model for F if and only if $\langle U^{\mathcal{A}}; f^{\mathcal{A}}, e^{\mathcal{A}}\rangle$ is a monoid. *(5 Points)*

d) ($\star$) Let $F = (A \vee B) \wedge (A \to \neg C) \wedge \neg(B \wedge C)$ and $G = \neg C$. Using the resolution calculus, prove that $F \models G$. *(8 Points)*

e) ($\star\star$) Prove or disprove: For all formulas F and G,

$$(\forall x\ F) \vee G \ \models\ \forall x\ (F \vee G).$$

(8 Points)

☐ True ☐ False

f) $(\star\,\star)$ Prove or disprove: For all formulas F and G,

$$(\exists x\ F) \vee G \ \models\ \exists x\ (F \vee G).$$

(8 Points)

□ True □ False

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)”).