Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Departement Informatik
Wintersession 2021

Prof. Ueli Maurer

Exam
Diskrete Mathematik

5. Februar 2021

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 115 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 verwenden Sie einen dokumentenechten Stift (also keinen Bleistift) und nicht die Farben Rot oder Grün.

5.) Bitte legen Sie die Legi für die Ausweiskontrolle auf den Tisch.

6.) Sie dürfen bis 10 Minuten vor Ende der Prüfung vorzeitig abgeben und den Raum still verlassen.

7.) Mobiltelefone und Smartwatches müssen komplett ausgeschaltet sein (kein Standby) und dürfen nicht am Körper getragen werden.

Prüfungs-Nr.

Stud.-Nr.:

Name:

Unterschrift:

Korrektur:

	Punkte		Unterschrift	
Aufgabe	Max	Erreicht	Korr.	Ver.
1	32			
2	18			
3	30			
4	35			
Total	115			

Task 1. Sets, Relations and Functions..32 Points

a) Short Questions. Each correct answer gives one point. No justification is required. *(10 Points)*

1.) List the elements of the set $\{0,1\} \times \{(0,1)\}$.

2.) List the elements of the set $(\varnothing \cup \{\varnothing\}) \cap \{\varnothing, \{\varnothing\}\}$.

3.) How many elements has the set $\mathcal{P}(\{\varnothing, \{\varnothing\}, \varnothing\} \cup \{\{\varnothing\}, \{\{\varnothing\}\}\})$?

4.) For any set A and any relation ρ on A we have

$$\mathsf{id}_A \subseteq \rho \iff \mathsf{id}_A \subseteq \widehat{\rho}.$$

☐ True ☐ False

5.) The composition of two symmetric relations is symmetric. ☐ True ☐ False

6.) The union of two transitive relations is transitive. ☐ True ☐ False

7.) The complement of an irreflexive relation is reflexive. ☐ True ☐ False

8.) Find a set A and a function $f : A \to A$ such that f is injective but not surjective.

9.) The power set of the set of all prime numbers is countable. ☐ True ☐ False

10.) For all $n \in \mathbb{N}$, the set $(\mathbb{Q}[x])^n$ is countable. ☐ True ☐ False

b) Prove or disprove: The poset $(\{2,3,4,5,6,7,8,9\}; |)$ is a lattice. *(2 Points)*

c) ($\star\star$) Let $(A; \preceq)$ be a poset and define the relation $\prec$ on A by

$$a \prec b \overset{\text{def}}{\iff} a \preceq b \ \wedge \ a \neq b$$

for all $(a, b) \in A \times A$. Prove that $\prec$ is transitive. *(5 Points)*

d) We want to define the integers $\mathbb{Z}$ based on the natural numbers $\mathbb{N}$. In order to do this, we let $A \stackrel{\text{def}}{=} \mathbb{N} \times \mathbb{N}$ and think of an element $(a, b) \in A$ as a representation of the integer that is the difference of a and b.

1.) ($\star$) Find an equivalence relation $\sim$ on A which captures that two representations correspond to the same integer, i.e., allowing us to define

$$\mathbb{Z} \stackrel{\text{def}}{=} A/\!\sim .$$

Use only addition (and no minus sign $-$) in $\mathbb{N}$. No justification is required. *(1 Point)*

2.) ($\star$) Define the sum of two representations of integers as a function $\mathsf{sum} : A^2 \to A$, only using addition (and no minus sign $-$) in $\mathbb{N}$. No justification is required. *(1 Point)*

3.) ($\star\,\star$) A function $f : B^2 \to B$ is called *θ-consistent* for an equivalence relation θ on B if

$$(b_1 \;\theta\; b_1' \text{ and } b_2 \;\theta\; b_2') \implies f(b_1, b_2) \;\theta\; f(b_1', b_2')$$

is true for all $b_1, b_2, b_1', b_2' \in B$.

Prove that sum is $\sim$-consistent (for the choices of $\sim$ and sum of the previous subtasks). Make sure that no minus sign $-$ occurs in your proof. *(6 Points)*

e) ($\star\star\star$) Prove or disprove: The set

$$S = \{a \in \mathbb{N}^\infty \mid \forall i \in \mathbb{N}\ \exists j \in \mathbb{N}\ (i < j \land a_j = 2^{a_i})\}$$

is countable. *(7 Points)*

Hint: Recall that $\mathbb{N}^\infty$ is the set of all semi-infinite sequences over $\mathbb{N}$. Moreover, for any $a \in \mathbb{N}^\infty$ and any $i \in \mathbb{N}$, a_i is the natural number at the i-th position of a.

Hint: The sequence $2^0, 2^1, 2^2, 2^3, \ldots$ is an element of S.

Task 2. Number Theory .... **18 Points**

a) Short Questions. Each correct answer gives one point. No justification is required. *(5 Points)*

1.) Compute $R_{31}(313131033^{31313131313318})$.

2.) Compute $R_{12345}(12344^{(1234512345^{1234512345})})$.

3.) Compute $\gcd(284, 384)$.

4.) Find $x \in \mathbb{Z}_{13}$ such that $4x \equiv_{13} 1$.

5.) There exists $x \in \mathbb{Z}_{137875}$ such that $256x \equiv_{137875} 1$. ☐ True ☐ False

b) ($\star$) We have generated the RSA public key $(n, e) = (15, 3)$.

1.) Encrypt the message $m = 4$ under the public key (n, e). *(1 Point)*

2.) Find the secret key d that corresponds to the public key (n, e). *(2 Points)*

3.) The ciphertext $y = 7$ was encrypted with the public key (n, e). Decrypt it. *(1 Point)*

c) ($\star$) Alice and Bob execute the Diffie-Hellman protocol using the subgroup of $\langle \mathbb{Z}_{15}^*; \odot \rangle$ that is generated by $g = 2$. Alice sends the message $y_A = 8$. They agree on the secret key $k_{AB} = 2$. *(3 Points)*

What message did Bob send?

Calculation. You will get full points if the answer above is correct. Otherwise, you may get partial points for the calculation in this box.

d) ($\star\,\star$) Let $m, n \in \mathbb{N} \setminus \{0, 1\}$ and consider the function $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ with

$$f(x) = (R_m(x), R_n(x)) \quad \text{for all } x \in \mathbb{Z}_{mn}.$$

Prove that if f is injective then $\gcd(m, n) = 1$. *(6 Points)*

Task 3. Algebra .... **30 Points**

a) Short Questions. Each correct answer gives one point. No justification is required. *(5 Points)*

1.) Every group of order 17 has 16 generators. ☐ True ☐ False

2.) How many zerodivisors has $\mathbb{Z}_{91}$? *(Hint:* $91 = 7 \cdot 13$*)*

3.) Find a field with 27 elements.

4.) Compute $(2x+2) \cdot (2x+1)$ in $\mathbb{Z}_3[x]_{x^2+1}$.

5.) List all irreducible monic polynomials of degree 2 in $\mathbb{Z}_2[x]$.

b) ($\star$) Consider the algebra $\langle \mathbb{Z}; \star \rangle$ where $\star$ is defined by $a \star b \stackrel{\text{def}}{=} a^3 + b^3$ for any $a, b \in \mathbb{Z}$. Decide whether $\langle \mathbb{Z}; \star \rangle$ is a monoid, a group or neither. Prove your answer. *(3 Points)*

c) ($\star$) Let $\langle R; +, -, 0, \cdot, 1\rangle$ be a ring and let $a, b \in R$. Use only the ring axioms and the fact that $0x = x0 = 0$ for all $x \in R$ to prove that

$$(-a)b = a(-b).$$

(6 Points)

d) ($\star$ $\star$) Prove or disprove: If for a finite field F two polynomials $p(x) \in F[x]$ and $q(x) \in F[x]$ correspond to the same function (i.e., $p(a) = q(a)$ for all $a \in F$), then they are the same polynomial.

(4 Points)

e) ($\star\star$) Find an isomorphism between the groups $\langle \mathbb{Z}_3; \oplus \rangle \times \langle \mathbb{Z}_{35}; \oplus \rangle$ and $\langle \mathbb{Z}_{21}; \oplus \rangle \times \langle \mathbb{Z}_5; \oplus \rangle$. No justification is required. *(6 Points)*

f) $(\star\,\star)$ Consider the ring $\mathbb{Z}_2[x]_{x^2+x+1}[y]$. Divide $(x+1)y^4 + y^3 + (x+1)y^2 + x$ by $y^2 + y + (x+1)$ with remainders.

(6 Points)

Task 4. Logic .... 35 Points

a) Short Questions. Each correct answer gives one point. No justification is required. *(3 Points)*

1.) The expression $(\forall x\, P(x)) \vee (\exists x\, \neg P(x))$ is a mathematical statement. ☐ True ☐ False

2.) The following derivation rule is sound: $\{F, \neg F\} \vdash G$. ☐ True ☐ False

3.) Any calculus with the following derivation rule is complete: $\varnothing \vdash F$. ☐ True ☐ False

b) $(\star)$ Consider the formula $\exists x\, \big((\forall y\, Q(x,y)) \to P(z)\big) \wedge Q(y,x)$. Give an equivalent formula in prenex form. No justification is required. *(2 Points)*

c) $(\star)$ Let $\mathcal{S} = \{2,3,5,7,9\}$ and $\mathcal{P} = \mathbb{N} \setminus \{0,1\}$. Moreover, define for all $s \in \mathcal{S}$ and all $p \in \mathcal{P}$

$$\tau(s) = 1 \overset{\text{def}}{\iff} s \text{ is not prime}, \quad \text{and} \quad \phi(s,p) = 1 \overset{\text{def}}{\iff} p^2 \mid s.$$

Is the proof system $(\mathcal{S}, \mathcal{P}, \tau, \phi)$ sound? Is it complete? Justify both of your answers. *(4 Points)*

d) ($\star$) Mark each step that is wrong in the following derivation in the resolution calculus. *(2 Points)*

$$
\begin{tikzcd}[column sep=small]
\{\neg D, E\} \arrow[dr, dash] & & \{A, \neg E\} \arrow[dl, dash] & & \{\neg B, D\} \arrow[ddll, dash] & & \{B\} \arrow[dr, dash] & & \{\neg A, B, \neg B\} \arrow[dl, dash] \\
& \{A, \neg D\} \arrow[dr, dash] & & & & & & \{\neg A, B\} \arrow[ddlll, dash] & \\
& & \{A, \neg B\} \arrow[drr, dash] & & & & & & \\
& & & & \emptyset & & & &
\end{tikzcd}
$$

e) ($\star$) Prove or disprove: If F and G are formulas such that $\neg F$ and $F \vee G$ are satisfiable, then G is satisfiable. *(3 Points)*

f) ($\star$) Prove that $(\neg C \land (A \to B)) \lor C \equiv A \to (B \lor C)$ by using only the following rules:

1.) $F \to G \equiv \neg F \lor G$	10.) $\neg\neg F \equiv F$
2.) $F \land F \equiv F$	11.) $\neg(F \land G) \equiv \neg F \lor \neg G$
3.) $F \lor F \equiv F$	12.) $\neg(F \lor G) \equiv \neg F \land \neg G$
4.) $F \land G \equiv G \land F$	13.) $F \lor \top \equiv \top$
5.) $F \lor G \equiv G \lor F$	14.) $F \land \top \equiv F$
6.) $(F \land G) \land H \equiv F \land (G \land H)$	15.) $F \lor \bot \equiv F$
7.) $(F \lor G) \lor H \equiv F \lor (G \lor H)$	16.) $F \land \bot \equiv \bot$
8.) $F \land (G \lor H) \equiv (F \land G) \lor (F \land H)$	17.) $F \lor \neg F \equiv \top$
9.) $F \lor (G \land H) \equiv (F \lor G) \land (F \lor H)$	18.) $F \land \neg F \equiv \bot$

In each step, *syntactically* apply exactly one rule and **state the number** of the rule you applied. Within one step, do *not* apply a rule multiple times.

Example step: $\neg A \lor ((C \land B) \lor \neg B) \overset{7.)}{\equiv} (\neg A \lor (C \land B)) \lor \neg B$. *(8 Points)*

g) ($\star\star$) Consider the calculus consisting of the following four derivation rules:

$$\begin{aligned}
\{F \to G, F\} &\vdash_{R_1} G \\
\varnothing &\vdash_{R_2} F \to (G \to F) \\
\varnothing &\vdash_{R_3} (\neg F \to \neg G) \to (G \to F) \\
\varnothing &\vdash_{R_4} (F \to (G \to H)) \to ((F \to G) \to (F \to H))
\end{aligned}$$

Formally derive $A \to A$ from $\varnothing$ in the calculus. *(6 Points)*

h) ($\star$ $\star$) Prove without using any lemmas or theorems from the lecture notes that for any formulas F and G we have $\forall x\,(F \vee G) \models F \vee (\exists x\, G)$. Argue over the definition of $\models$ and the semantics of predicate logic. *(7 Points)*

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)”).