Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Departement Informatik
Wintersession 2023

Prof. Ueli Maurer

Exam
Diskrete Mathematik

27. Januar 2023

Hinweise:

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

2.) Falls nicht explizit ausgeschlossen dürfen Resultate (z.B. Lemmas oder Theoreme) aus dem Skript mit entsprechendem Verweis (z.B. *"Lemma Skript"*; die Nummer ist nicht notwending falls klar ist welches Resultat gemeint ist) ohne Beweis verwendet werden. Resultate aus der Übung dürfen **nicht** ohne Beweis verwendet werden.

3.) Die Aufgaben sind in drei Schwierigkeitsstufen von ($\star$) bis ($\star\star\star$) eingeteilt.

4.) 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.**

5.) Die Antwortfelder unter den Aufgaben sind jeweils grosszügig bemessen. Es ist oft nicht die Erwartung, dass eine Antwort das ganze Feld füllt.

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

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

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

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

Prüfungs-Nr.

Stud.-Nr.:

Korrektur:

	Punkte		Unterschrift	
Aufgabe	Max	Erreicht	Korr.	Ver.
1	31			
2	11			
3	25			
4	27			
Total	94			

Task 1. Sets, Relations, Functions, and Proof Patterns .... 31 Points

a) Short Questions. Each correct answer gives one point. No justification is required. *(8 Points)*

1.) How many elements does the set $\{\{0,1\},\{0\}\times\{1\}\}\times\{0\}$ have?

2.) List each element of the set $\{\varnothing,(0,1)\}\times\{\{0\}\cup\{1\},\{1,0\}\}$ exactly once.

3.) Find sets A, B, and C such that $A\cap C\neq\varnothing$ and $A\setminus B\subseteq A\setminus C$.

4.) Find a set A such that $A\cap\mathcal{P}(A)\neq\varnothing$.

5.) Consider the relation $\rho=\{(a,b),(a,c),(b,a)\}$ on $\{a,b,c\}$. List each element of the relation ρ^3.

6.) Which of the properties *reflexive*, *symmetric*, *antisymmetric*, *transitive* are satisfied by the relation $\mid\,\cup\equiv_2$ on $\mathbb{N}\setminus\{0\}$? List all satisfied properties.

7.) Consider the partial order $\preceq$ on $\mathbb{N}^2$ defined by $(a,b)\preceq(c,d)\iff a\leq c\,\wedge\,b\leq d$. What is the least upper bound of the set $\{(3,8),(1,4),(2,9)\}$?

8.) Find a surjective function $f:\mathbb{N}\to\mathbb{Z}$.

b) ($\star\,\star$) Consider the set $S=\{1,2,\ldots,9\}$. Prove that any subset $A\subseteq S$ with $|A|=6$ contains at least two **distinct** elements $x,y\in A$ such that $x+y=10$. *(4 Points)*

c) ($\star$) Consider the relation $\preceq$ on $\mathbb{N}^2$ defined by

$$(a, b) \preceq (c, d) \quad \iff \quad (a, b) = (c, d) \ \vee \ (a < c \ \wedge \ a + d \leq b + c).$$

Prove that $\preceq$ is a partial order. *(6 Points)*

d) ($\star\,\star$) Let X and Y be two non-empty sets. Moreover, let $f : X \to Y$ and $g : Y \to X$ be functions such that $f \circ g \circ f$ is injective **and** surjective.

Prove that **both** f and g are injective **and** surjective. State **clearly** which assumptions and properties you use in each step. *(8 Points)*

f is injective:

f is surjective:

g is injective:

g is surjective:

e) ($\star\star$) Consider the set

$$S = \{A \subseteq \mathbb{N} \mid A \text{ or } \mathbb{N} \setminus A \text{ is finite}\}.$$

Prove or disprove that the set S is countable. *(5 Points)*

Task 2. Number Theory . . . . **11 Points**

a) Short Questions. Each correct answer gives one point. No justification is required. *(4 Points)*

1.) Compute $R_{2023}(2022^{2023})$.

2.) Compute $R_{17}(2^{2023})$.

3.) Compute $\gcd(455, 182)$.

4.) Let $a, b \in \mathbb{N} \setminus \{0\}$ such that $\gcd(a, b) = 1$. What are the possible values of $\gcd(3a, 7b)$?

b) ($\star$) Alice proposes a variant of RSA encryption where e is chosen such that $\gcd(e, \varphi(n)) > 1$. That is, the public key is (n, e) for $n = pq$ (where p and q are distinct primes), e is chosen such that $\gcd(e, \varphi(n)) > 1$ and the ciphertext of a message $m \in \mathbb{Z}_n^*$ is $c = R_n(m^e)$.

What is the problem with this variant? You do **not** need to prove your claim(s). *(2 Points)*

c) ($\star\,\star$) Prove, **without using the concept of prime numbers**, that for all $a, b, c \in \mathbb{N} \setminus \{0\}$ we have

$$\gcd(a, bc) \mid \gcd(a, b) \cdot \gcd(a, c).$$

(5 Points)

Hint: For any $x, y \in \mathbb{N} \setminus \{0\}$ there exist $u, v \in \mathbb{Z}$ such that $ux + vy = \gcd(x, y)$.

Task 3. Algebra .... **25 Points**

a) Short Questions. Each correct answer gives the indicated number of points. No justification is required.

1.) How many generators does the group $\langle \mathbb{Z}_{29}; \oplus_{29} \rangle$ have? *(1 Point)*

2.) Let $\langle G; \cdot \rangle$ be a group and let $x \in G$ be an element with order 36. What is the order of (x^6, x^{16}) in the direct product group $G \times G$? *(2 Points)*

3.) Find a noncyclic group G such that all proper subgroups H of G (i.e., all subgroups $H \neq G$) are cyclic. *(2 Points)*

4.) Consider the polynomial $p(x) = x^4 + 2x + 1$ in the ring $\mathbb{Z}_3[x]$. Find all monic divisors of $p(x)$ with degree 1. *(1 Point)*

5.) Compute $R_{x^2+1}(x^6)$ in $\mathbb{Z}_3[x]$. *(2 Points)*

b) ($\star$) Prove that the groups $\langle \mathbb{Z}_{12}^*; \odot_{12} \rangle$ and $\langle \mathbb{Z}_4; \oplus_4 \rangle$ are **not** isomorphic. *(3 Points)*

c) ($\star$) Let $\langle G; +, \hat{}, e_G \rangle$, $\langle H; \odot, \tilde{}, e_H \rangle$, and $\langle J; \otimes, ^{-1}, e_J \rangle$ be groups. Moreover, let $\varphi : G \to H$ and $\phi : H \to J$ be group homomorphisms.

Prove that $\phi \circ \varphi$ is a group homomorphism. *(3 Points)*

d) ($\star$) Let $\langle G; \cdot, ^{-1}, e\rangle$ be an **abelian** group. Consider the set

$$H = \{x \in G \mid \operatorname{ord}(x) \neq \infty\}.$$

Prove that H is a subgroup of G. *(5 Points)*

Hint: You can use without proof that for any $a \in G$ and any $i, j \in \mathbb{Z}$ we have $a^{ij} = (a^i)^j = (a^j)^i$.

e) ($\star\star\star$) Let $p(x) \in \mathbb{Z}_2[x]$ be an irreducible polynomial of degree 5. Consider the field $F = \mathbb{Z}_2[x]_{p(x)}$. How many solutions $(a, b) \in F \times F$ does the equation

$$a^2 + b^2 + ab = 0$$

have? *(6 Points)*

Hint: $(a-b)(a^2+b^2+ab) = a^3 - b^3$.

Task 4. Logic .... **27 Points**

a) Short Questions. Each correct answer gives the indicated number of points. No justification is required.

1.) Find a formula H which has both x and y as free variables, such that $\forall x H \equiv \forall y H$. *(1 Point)*

2.) Consider the formulas $F = P(x) \wedge \neg Q(x)$ and $G = \exists x \, \neg(\neg P(x) \rightarrow Q(x))$. Give an interpretation suitable for both formulas that is a model for F but **not** for G. *(2 Points)*

3.) Find a formula equivalent to $(\forall x P(x)) \rightarrow (\exists x \, Q(x) \vee P(y))$ that is in prenex form. *(2 Points)*

b) ($\star$) Use the **resolution calculus** to prove that the formula

$$(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$$

is a tautology. You are allowed to apply multiple steps at once when transforming the formula (as long as it is easy to follow). **Show your work!** *(5 Points)*

c) ($\star$) Let $\Pi_1 = (\mathcal{S}_1, \mathcal{P}_1, \tau_1, \phi_1)$ and $\Pi_2 = (\mathcal{S}_2, \mathcal{P}_2, \tau_2, \phi_2)$ be two proof systems. We combine Π_1 and Π_2 into a third proof system

$$\Pi_3 = (\mathcal{S}_1 \times \mathcal{S}_2, \mathcal{P}_1 \times \mathcal{P}_2, \tau_3, \phi_3),$$

where

$$\tau_3(s_1, s_2) = 1 \quad \overset{\text{def}}{\iff} \quad \tau_1(s_1) \neq \tau_2(s_2),$$

and

$$\phi_3((s_1, s_2), (p_1, p_2)) = 1 \quad \overset{\text{def}}{\iff} \quad \phi_1(s_1, p_1) \neq \phi_2(s_2, p_2).$$

Prove or disprove: *If Π_3 is complete, then Π_1 or Π_2 is complete.* *(5 Points)*

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

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

Formally derive $\neg A \to (A \to B)$ from $\emptyset$ in the calculus. *(5 Points)*

Hint: You may want to instantiate R_4 with $F = \neg A$ and $H = A \to B$.

e) ($\star\,\star$) We extend predicate logic by a new operator $\diamondsuit$ as follows:

Syntax: If F and G are formulas, then $(F \diamondsuit G)$ is a formula.

Semantics: $\mathcal{A}((F \diamondsuit G)) = 1$ if and only if $\mathcal{A}(F) = 0$ or $\mathcal{A}(G) = 1$.

Prove the following statement: *For any formulas F and G we have*

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

Do **not** use any theorems or lemmas from the lecture notes. Use the definition of $\models$ and the semantics of predicate logic. Note that x may appear free in F, G, or both. *(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)").