Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Department of Computer Science
Winter Session 2025

Prof. Ueli Maurer

Exam
Diskrete Mathematik

4. February 2025

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 15 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.:

Task	Points
1	33
2	17
3	33
4	33
Total	116

Task 1. Sets, Relations, Functions, and Proof Patterns .... 33 Points

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

1.) Let $A = \{\{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\{\varnothing\}\}\}$. In the following list, **circle** all sets x such that $x \in A$, and **cross** all sets y such that $y \subseteq A$. *(1 Point)*

$\{\varnothing\}$ $\quad\quad$ $\{\{\varnothing\}, \{\varnothing\}\}$ $\quad\quad$ $\varnothing$ $\quad\quad$ $\{\{\{\varnothing\}\}, \varnothing\}$

2.) Let A, B, C be sets and let $X = (A \cap B) \setminus ((A \cup B) \cap C)$. Write an expression for X using (not necessarily all) set operations $\cup, \cap$, and $\setminus$ in which A, B, C appear *at most once.* *(1 Point)*

3.) Let A, B, C be sets such that $|(A \cup B) \times (C \cup B)| = 3$ and $A \cap B = \varnothing$. Write all the possible values of $|A| + |C|$. *(2 Points)*

4.) Let $A = \{a, b, c, d\}$. Find the smallest relation ρ on A such that $\{(a, b), (d, b)\} \subseteq \rho$ and both $\rho = \hat{\rho}$ and $\rho^2 \subseteq \rho$. *(2 Points)*

5.) Consider the poset $(\{1, 2, 3, 4, 8, 9, 24, 36\}; |)$ and let $S = \{2, 3\}$. Write all upper bounds of S in A. If there are least upper bounds of S in A, identify them, or else, write that none exist. *(2 Points)*

b) ($\star$) Let X be a set and let ρ and σ be equivalence relations on X. **Prove or disprove** that $\rho \cap \sigma$ is an equivalence relation. *(4 Points)*

c) ($\star$) Let A, B be non-empty sets such that there exists an injective function $f : A \to B$. **Prove or disprove** that there exists a surjective function $g : B \to A$. *(6 Points)*

d) ($\star$) Let $(X, \preceq)$ be a poset. Let $\prec$ be the relation on X defined as follows:

$$a \prec b \iff a \preceq b \;\wedge\; a \neq b.$$

Prove or disprove that $\prec$ is transitive.

(6 Points)

e) ($\star\,\star$) Let X be a set and let ρ be a countable relation on X. **Prove or disprove** that the transitive closure ρ^* of ρ is countable. *(9 Points)*

Task 2. Number Theory .... **17 Points**

a) Short Questions. Each correct answer gives 1 point. No justification is required. *(4 Points)*

1.) Compute $R_{13}(2^{4536})$.

2.) Find distinct $k, \ell, m \in \mathbb{N}$ such that $\varphi(k) = \varphi(\ell) = \varphi(m)$, where φ denotes Euler's function.

3.) Compute $\gcd(81, 48 + 3^{25})$.

4.) Compute the multiplicative inverse of 13 modulo 17.

b) ($\star$) Compute the set of solutions $(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11}$ to the congruence system

$$\begin{aligned} 2x + 9y &\equiv_{11} 7 \\ 2x + 7y &\equiv_{11} 5 \\ 4x + 5y &\equiv_{11} 1. \end{aligned}$$

Show your work. *(4 Points)*

c) ($\star$) Consider the polynomial $f(x) = x^4 + x^2 + 1$. **Prove** that: for all primes $p \in \mathbb{Z}$, the evaluation $f(p)$ is **not** prime. *(4 Points)*

d) ($\star\star$) Let φ denote the Euler's function. **Prove or disprove** that for all $n \in \mathbb{N} \setminus \{0\}$ the equation $\varphi(x) = n$ has finetely many solutions $x \in \mathbb{N}$. *(5 Points)*

Task 3. Algebra .... **33 Points**

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

1.) Give the number of subgroups of $\langle \mathbb{Z}_2 \times \mathbb{Z}_6;\ \oplus \rangle$. *(1 Point)*

2.) Find a generator of a largest cyclic subgroup of $\langle \mathbb{Z}_9^* \times \mathbb{Z}_5^*;\ * \rangle$ and compute its order, where $(a, b) * (c, d) = (a \odot_9 c, b \odot_5 d)$ for $(a, b), (c, d) \in \mathbb{Z}_9^* \times \mathbb{Z}_5^*$. *(2 Points)*

3.) Compute $R_{x^2+x+1}(x^4 + x^2)$ in $\mathbb{Z}_5[x]$. *(2 Points)*

4.) Find the smallest integer $n > 8$ such that $\mathbb{Z}_n^*$ is isomorphic to $\mathbb{Z}_8^*$. *(2 Points)*

5.) Compute $\gcd(x^3 + x^2 + x + 1,\ 2x^3 + x + 3)$ in $\mathbb{Z}_5[x]$. *(2 Points)*

b) ($\star$) Let $\langle G;\ \star, \widehat{\ }, e \rangle$ be a group and $Z(G) := \{h \mid h \in G,\ g \star h \star \widehat{g} = h \text{ for all } g \in G\}$ the so-called *center* of G. **Prove** that $Z(G) = G$ if and only if G is commutative. *(5 Points)*

c) ($\star$) Let $\langle R;\ +, *, -, ^{-1}, 0, 1\rangle$ be a commutative ring. **Prove** that the following are equivalent:

- R is an integral domain.
- For all $p(x)$ and $q(x)$ in $R[x]$ it holds that $\deg\big(p(x) \cdot q(x)\big) = \deg(p(x)) + \deg(q(x))$.

(4 Points)

d) ($\star$) Let F be a finite field. **Prove** that there exist infinitely many irreducible polynomials in $F[x]$.

(6 Points)

e) $(\star\,\star)$ Let $\langle G;\ \star, \widehat{\ }, e\rangle$ be an abelian group, $k \in \mathbb{N}$ and $H := \{x \mid x \in G,\ \mathrm{ord}(x) = k\} \cup \{e\}$. **Prove** that H is a subgroup of G if and only if $H = \{e\}$ or k is prime. *(9 Points)*

Task 4. Logic .... **33 Points**

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

1.) Circle all *symbols* that occur free in the formula *(2 Points)*

$$\Big(\forall x\, P(f(x), y)\Big) \wedge \exists y\, Q(x, g(y)).$$

2.) Circle all the formulas in CNF and cross all formulas in DNF in the list below. *(2 Points)*

$A \wedge B \wedge \neg C \qquad A \wedge \neg(B \vee C) \qquad A \vee (\neg B \wedge C) \qquad A \vee \neg B \vee \neg C$

3.) Let $F = \forall x\, P(x)$. Circle *all* formulas G in the following list such that $F \models G$. *(2 Points)*

$\forall x\, Q(x) \qquad P(y) \qquad Q(y) \to P(z) \qquad \exists y\, Q(y) \qquad (Q(z) \to Q(y)) \vee (Q(y) \to Q(z))$

4.) Find a formula in prenex normal form equivalent to *(3 Points)*

$$\exists\, x \Bigg(P(y) \wedge \neg \Big(\forall y\, (Q(x, y) \wedge \exists z\, R(z, y)) \Big) \Bigg).$$

b) ($\star$) **Disprove** that the resolution calculus is complete, that is disprove that for all sets of clauses $\mathcal{K}$ and for all clauses K it holds that

$$\mathcal{K} \models K \implies \mathcal{K} \vdash_{\mathsf{Res}} K.$$

(3 Points)

c) ($\star$) We extend the resolution calculus with two new rules ext and tnd. The rules work as follows, for all clauses K and all literals L:

$$\begin{aligned} K &\vdash_{\mathsf{ext}} K \cup \{L\}, \\ &\vdash_{\mathsf{tnd}} \{L, \overline{L}\}, \end{aligned} \tag{1}$$

where

$$\overline{L} = \begin{cases} \neg A & \text{if } L = A \text{ for some atomic formula } A, \\ A & \text{if } L = \neg A \text{ for some atomic formula } A. \end{cases}$$

Prove that the rules ext and tnd are correct. *(3 Points)*

$(\star\star\star)$ **Prove** that the extended calculus $\mathsf{ResExt} = \{\mathsf{ext}, \mathsf{res}, \mathsf{tnd}\}$ is complete, that is, for all clause sets $\mathcal{K}$ and all clauses K it holds that:

$$\mathcal{K} \models K \Longrightarrow \mathcal{K} \vdash_{\mathsf{ResExt}} K.$$

Hint: What is the clause set corresponding to the negation of K? *(11 Points)*

d) ($\star\,\star$) Consider the formulas

- $F = \forall x\, \exists y Q(x, y)$,
- $G = \forall x\, Q(x, f(x))$.

Prove or disprove that if F is satisfiable then G is satisfiable. *(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)").