Discrete Mathematics

Giuseppe Accaputo
Computational Science and Engineering, B.Sc.
ETH Zürich

1 Proof

1.1 Proof by contradiction

We want to prove $P \to Q$. Assume that $\not Q$ and start the proof with P trying to proof $\not Q$ until you arrive at something that contradicts P.

2 Sets

2.1 Subsets

Subset

$$A \subseteq B :\Longleftrightarrow \forall x \in A : x \in B$$

Not Subset

$$A \not\subseteq B :\Longleftrightarrow x \in A \wedge x \notin B$$

Empty Set The empty set is a subset of any given Set X:

$$\varnothing \subseteq X$$

Set Equality

$$A = B :\Longleftrightarrow A \subseteq B \wedge B \subseteq A$$

Complement

$$x \notin \overline{A} \Longleftrightarrow x \in A$$

Union of all sets

$$\bigcup \mathcal{A} := \{x | \exists A \in \mathcal{A} : x \in A\}$$

Intersection of all sets

$$\bigcap \mathcal{A} := \{x | \forall A \in \mathcal{A} : x \in A\}$$

3 Relations

Definition Let ρ be a *relation* from a set A to a set B, then $\rho \subseteq A \times B$

Notation

$$(a, b) \in \rho \Longleftrightarrow a \; \rho \; b$$

Representations of relations A relation ρ from A to B denoted as $A \; \rho \; B$ can be represented as a $|A| \times |B|$ matrix M^ρ.

Let $A = B = \{a, b, c\}$ and $\rho = \{(a, a), (a, c), (b, b), (c, c)\}$. The matrix representation is

$$M^\rho = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{ccc} a & b & c \end{array} \\ \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$

Composition of a relation ρ with itself

$$\rho^n = (M^\rho)^n = \underbrace{M^\rho \cdot \ldots \cdot M^\rho}_{n\text{-times}}$$

Note: If an entry in the matrix is $\rangle 1$, then the number is simply replaced by 1.

Reflexive closure of ρ on a set A

$$\rho \cup \{(a, a) | a \in A\}$$

Symmetric closure of ρ on a set A

$$\rho \cup \{(a, b) | (b, a) \in \rho\}$$

Transitive closure of ρ on a set A

$$\rho^* = \bigcup_{n=1}^{\infty} p^n, \qquad \rho \subseteq \rho^*$$

3.1 Equivalence Relations

Definition An *equivalence relation* is a relation that is reflexive, symmetric, and transitive.

Equivalence class The equivalence class $[a]_\theta$ of $a \in A$ contains all elements that are equivalent to a:

$$[a]_\theta := \{b \in A | b \; \theta \; a\}$$

Partition of a set A

$S_i \subseteq A\}$ is a *partition* of A

$$S_i \cap S_j = \emptyset \quad \text{for } i \neq j \qquad \text{and} \bigcup_{i \in I} S_i = A$$

Quotient set of A by θ

$$A/\theta := \{[a]_\theta | a \in A\}$$

(i) A/θ is a partition of A

(ii) A/θ is the set of equivalence classes of an equivalence relation θ on A

3.2 Partial Orders

Definition A *partial order* is a relation that is reflexive, antisymmetric, and transitive. A set A together with a partial order $\preceq$ on A is called a *partially ordered set (poset)* and is denoted as $(A; \preceq)$

Totally ordered If any two elements of a poset $(A, \preceq)$ are comparable, then A is called *totally ordered* by $\preceq$

Well-ordered A poset $(A, \preceq)$ is *well-ordered* if it is totally ordered and if every non-empty subset of A has a least element.

Types of Elements in a poset Let $(A; \preceq)$ be a poset, and $S \subseteq A$:

Minimal element of S : $\exists a \in S \; \forall b \in S : b \not\prec a$

Maximal element of S : $\exists a \in S \; \forall b \in S : b \not\succ a$

Least element of S : $\exists a \in S \; \forall b \in S : a \preceq b$

Greatest element of S : $\exists a \in S \; \forall b \in S : a \succeq b$

Lower bound of S : $\exists a \in A \; \forall b \in S : a \preceq b$

Upper bound of S : $\exists a \in A \; \forall b \in S : a \succeq b$

Greatest lower bound of S : a is the greatest element of the set of all lower bounds

Least upper bound of S : a is the least element of the set of all upper bounds

3.2.1 Hasse Diagrams

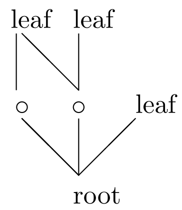
Covering An element b of a poset $(A, \prec)$ *covers* an element a if

$$a \prec b \;\wedge\; (\nexists \, c : a \prec c \wedge c \prec b)$$

Example $(\{1, 2, 3, 4, 5, 6, 7, 8\}, |)$ is a poset. $2|4$, but $2 \not| 8$, because $\exists c = 4$ such that $2|4 \wedge 4|8$.

Types of Elements in a Hasse diagram

Notation Since a Hasse diagram is constructed bottom-up, you can imagine it to be a reversed tree. Therefore, an element at the very bottom of a Hasse diagram will be called a *root* and elements that are not covered by any other elements are called *leafs*:



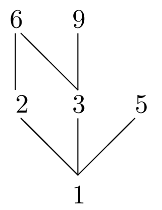
Least element : The root of the Hasse diagram.
If there are multiple roots, no least element exists in the poset

Greatest element : The leaf of the Hasse diagram.
If there are multiple leafs, no greatest element exists in the poset

Minimal element: The root of the Hasse diagram.
If there are multiple roots, then all roots are minimal elements of the poset

Maximal element : The leaf of the Hasse diagram.
If there are multiple leafs, then all leafs are maximal elements of the poset

Example The following is the Hasse diagram of the poset $(1, 2, 3, 5, 6, 9; |)$.



Least element : 1 (the root)

Greatest element : None (multiple leafs)

Minimal element: 1 (the root)

Greatest elements : 6,9,5 (the leafs)

3.2.2 Partial Order Relations

Partial Order Relation Let $(A, \preceq)$ and $(B, \sqsubseteq)$. The following relation $\leq$ defined on $A \times B$ is a *partial order relation*:

$$(a_1, b_1) \leq (a_2, b_2) \ :\Longleftrightarrow \ a_1 \preceq a_2 \ \wedge \ b_1 \sqsubseteq b_2$$

Lexicographical Order Relation Let $(A, \preceq)$ and $(B, \sqsubseteq)$. The following relation $\leq_{lex}$ defined on $A \times B$ is a *partial order relation*:

$$(a_1, b_1) \leq_{lex} (a_2, b_2) \ :\Longleftrightarrow \ a_1 \prec a_2 \ \vee (a_1 = a_2 \ \wedge \ b_1 \sqsubseteq b_2)$$

4 Functions

Image

$$f : A \to B \qquad f(A) \subseteq B \qquad f(A) \text{ is the image of } f$$

Surjective

$$f(A) = B \implies |f(A)| = |B|$$

Injective

$$|A| = |f(A)|$$

5 Combinatorics

5.1 Beschreibung

- Was ich nicht auswählen muss wird dividiert
- Was ich auswählen muss wird multipliziert

Beispiel Hamiltonkreise in vollständigem Graph: $n!$ Möglichkeiten, um Knoten zu durchlaufen. Ich muss kein Startknoten wählen $\implies \frac{n!}{n}$. Richtung spielt keine Rolle $\implies \frac{n!}{2n}$

5.2 Flowchart

1. Sind die Objekte, auf welche ich verteile oder welche ich nehme eindeutig gekennzeichnet? (z.B. Hosen sortiert nach, oder ich stelle Personen hinter *verschiedenen* Kassen)
   - JA: Ordered
   - NEIN: Unordered (z.B. gleichaussehnde Urnen)

5.3 Ordered Selection with Repetition

The number of ordered selections of length s with repetition out of n different objects is

$$n^s$$

Generic example There are n^k different words of length k in an alphabet consisting of n characters. A character can occur multiple times in a word (repetition).

5.4 Ordered Selection without Repetition

The number of ordered selections of length s without repetition out of n different objects is

$$n^{\underline{k}} = \frac{n!}{(n-s)!}$$

Example Mister Poss chooses 2 pairs of trousers sorted by their rating
If the number of ordered selections is the same as the number of different objects (namely n), then we simply have

$$n!$$

One can arrange n different items in $n!$ different ordered ways.

Example Mister Random wants to arrange his 3 kids for a photograph. For the first kid, he has 3 possibilities to arrange it. For the second kid, only 2 possibilities remain for the positioning. For the last kid, Mister X does not have a choice, since only 1 possibility remains. Therefore, we obtain $3 \cdot 2 \cdot 1 = 3!$ possibilities for the positioning of the 3 kids.

5.5 Unordered Selection with Repetition

The number of possibilities to store k elements away in n drawers is

$$\binom{k+n-1}{k} = \binom{k+n-1}{n-1}$$

Figurative

$$\underbrace{\underbrace{\circ\ \circ\ \circ}_{\text{1st drawer}} \mid \underbrace{\circ}_{\text{2nd drawer}} \mid \ldots \mid \underbrace{\circ\ \circ}_{n\text{th drawer}}}_{n-1 \text{ separation lines}}$$

Example If we want to store 20 pairs of socks away in 3 drawers, than we have $\binom{20+3-1}{3}$ possibilities to do so.

5.6 Unordered Selection without Repetition

The number of unordered selections of different subsets of length k from a set of length n is

$$\binom{n}{k}$$

Example There are $\binom{49}{6}$ possibilities to choose 6 numbers from 49 on a lottery ticket.

6 Countable and Uncountable Sets

Equivalent Sets

$$A \implies B \text{ is a bijection} \implies A \backsim B$$

(i) $\backsim$ is an equivalence relation

Countable Set

$$A \preceq \mathbb{N} \iff \exists\ A \implies \mathbb{N}\text{ , which is an injective mapping}$$

(i) $A \preceq B$ means B is *at least equipotent* to A

(ii) $\preceq$ is transitive: $A \preceq B \land B \preceq C \implies A \preceq C$

(iii) $A \preceq B \land B \preceq A \implies A \backsim B$

Uncountable Set

$$A \npreceq \mathbb{N} \land A \preceq B \implies B \npreceq \mathbb{N}$$

(i) If $A \subseteq B$ and B is uncountable, then so is A
Example: $(0,1) \subseteq \mathbb{R} \implies (0,1)$ is uncountable

7 Graphs

Isomorphism To check if two graphs $G = (V_G, E_G)$ and $K = (V_K, E_K)$ are isomorphic ($G \cong K$), verify the following properties in this order:

1. Check $|V_G| = |V_K|$. With $|V_G| \neq |V_K|$ you cannot define a bijection for the renaming of the vertices, resulting in $G \ncong K$
2. Check that both graphs have the same amount of vertices with the same degree. $\exists w \in V_G\colon deg(w) = x \land \forall l \in V_K : deg(l) \neq x \implies G \ncong K$
3. Check for cycles of length n. Let C_n be such a cycle of length n. If $C_n \sqsubseteq G \land C_n \not\sqsubseteq K \implies G \ncong K$
4. Now you can try to define a bijection $\pi : V_G \implies V_K$. If such a bijection exists, then $G \cong K$

8 Divisors and Division

8.1 Fracture

$\frac{a}{b}$ is the number that multiplied by b results in a:

$$b \cdot \frac{a}{b} = a$$

$a|\frac{a}{b}$ means that a number k exists, such that $\frac{a}{b} = k \cdot a$. In this case it is important to note that $\frac{a}{b}$ is just a symbol, meaning we cannot multiply both sides with b to remove the rational term from the equation.

Instead, one can show using the above mentioned definition that if $a \mid b \land c \mid \frac{b}{a}$ applies, then $c \mid b$ can be concluded as follows:

$$c \mid \frac{b}{a} \implies \exists\ d : \frac{b}{a} = c \cdot d \implies b = a \cdot \frac{b}{a} = acd = (ad)c \implies c \mid b$$

Although it's mentioned that $\frac{b}{a}$ is *only* a symbol, one can still make the following transformation:

$$b = acd \iff \frac{b}{c} = ad$$

8.2 Division Algorithm

For all integers a and $b \neq 0$ there exist unique integers q and r satisfying

$$a = q \cdot b + r \text{ and } r \in \{0, ..., b-1\}$$

q is called the *quotient*, and is the biggest possible multiple of b so that $q \cdot b$ is at most a.

r is called the *remainder*, and is often denoted as $R_b(a)$ or $a \bmod b$.

Example 1 $a = 7,\ b = 3,\ q = 2$ (since $3 \cdot 3 \rangle 7$ but $2 \cdot 3 \leq 7$) $, r = R_3(7) = 1$

Example 2

$$\begin{aligned}
&12x + 7y = 321 \\
&\implies 12x = 321 - 7y \\
&\implies 12x = (-1) \cdot y \cdot 7 + 321 \\
&\implies a = 12x,\ b = 7,\ q = (-1) \cdot y,\ \underline{r = 321 = R_7(12x)} \\
&\implies 12x \equiv_7 321 \\
&\implies R_7(12x) = R_7(321) \\
&\implies R_7(R_7(12) \cdot R_7(x)) = R_7(315 + 6) \\
&\implies R_7(R_7(12) \cdot R_7(x)) = R_7(R_7(315) + R_7(6)) \\
&\implies R_7(5x) = R_7(6) \\
&\implies 5x \equiv_7 6 \\
&\implies x = 4 \\
&\implies \text{As long as } y\rangle 0 :\ y = 321 - 12 \cdot (4 + k \cdot 7) \text{ with } k \in \mathbb{N}\backslash\{0\}
\end{aligned}$$

8.3 Modular Arithmetic

8.3.1 Coset

$$a \equiv_m b \iff R_m(a) = R_m(b)$$

8.3.2 Relatively Prime Numbers

Two numbers a and m are said to be *relatively prime* if the following equation holds:

$$a \equiv_m 1$$

8.3.3 Modular Congruence

$$a + k \cdot m \equiv_m b + k \cdot m \text{ for } k \in \mathbb{Z}$$

Examples

$$\begin{aligned}
10 \equiv_{11} 10 &\implies 10 \equiv_{11} -1 \\
8 \equiv_{10} 8 &\implies 8 \equiv_{10} -2 \\
8 \equiv_{20} 8 &\implies 8 \equiv_{20} -12 \\
-25 \equiv_3 -1 &\implies 2 \equiv_3 -1
\end{aligned}$$

8.3.4 Euclide: Unique Integerss

$$a = dq + r \iff a = dq + R_d(a)$$

8.3.5 Simplifying the Search for an Inverse When Calculating $R_m(a^b)$

$$a^b \equiv_m m - 1 \implies a^b \equiv_m -1 \implies a^{2 \cdot b} \equiv_m 1$$

Example: $2^5 \equiv_{11} -1 \implies 2^{10} \equiv_{11} 1$

8.4 Extended Euclidean Algorithm

The extended Euclidean algorithm (EEA) can be used to calculate $gcd(m, n)$ and find the multiplicative inverse for two integers when $gcd(m, n) = 1$ holds. It also offers a possibility to find two integers x and y that satisfy Bézout's identity:

$$gcd(m, n) = mx + ny$$

8.4.1 Calculate $gcd(m, n)$

Let m and n be two integers and $m\rangle n$. To calculate the $gcd(m, n)$ of both integers one can follow the following steps of the EEA:

Dividend	=	Quotient	·	Divisor	+	Reminder
m	=	q_1	·	n	+	r_1
n	=	q_2	·	r_1	+	r_2
$r1$	=	q_3	·	r_2	+	r_3
			...			
r_{n-2}	=	q_n	·	r_{n-1}	+	$\underline{\boldsymbol{r_n}}$
r_{n-1}	=	q_{n+1}	·	r_n	+	0

The calculation comes to an end once the reminder is 0. Once the algorithm has reached this step, the solution of $gcd(m, n)$ can be read off from the second to last equation:

$$gcd(m, n) = r_n$$

Example Calculate $gcd(17, 7)$:

$$
\begin{aligned}
17 &= 2 \cdot 7 + 3 \\
7 &= 2 \cdot 3 + 1 \\
3 &= 3 \cdot 1 + 0 \\
\implies gcd(17, 7) &= 1
\end{aligned}
$$

8.4.2 Solving Bézout's Identity $gcd(m, n) = mx + ny$

First calculate $gcd(m, n)$ using the previously explained steps:

Dividend	=	Quotient	$\cdot$	Divisor	+	Reminder
m	=	q_1	$\cdot$	n	+	r_1
n	=	q_2	$\cdot$	r_1	+	r_2
$r1$	=	q_3	$\cdot$	r_2	+	r_3
			...			
r_{n-2}	=	q_n	$\cdot$	r_{n-1}	+	$\underline{\boldsymbol{r_n}}$
r_{n-1}	=	q_{n+1}	$\cdot$	r_n	+	0

Once the step right before the reminder equals 0 has been reached, the equation at this very step is rewritten such that all terms without r_n are moved to the left side:

$$r_{n-2} - q_n \cdot r_{n-1} = r_n$$

The previous equation to this one then will be altered in the same way, leaving the reminder r_{n-1} on the right side of the equal sign:

$$r_{n-3} - q_{n-1} \cdot r_{n-2} = r_{n-1}$$

Now that r_{n-1} has been defined, its definition can be used in the very first equation (which will be called the final equation from now on):

$$r_{n-2} - q_n \cdot r_{n-1} = r_n \implies r_{n-2} - q_n \cdot (r_{n-3} - q_{n-1} \cdot r_{n-2})$$

This steps have to be repeated for every equation that has been a result of the calculation of $gcd(m, n)$.

It is important to note that during these steps only the replacements should be made, and no terms should be changed, e.g. leave $4 \cdot (2 - 1)$.

Once the very first equation has been processed and used in the final equation, one will find both the numbers m and n to be part of it, since the first two equations when calculating $gcd(m, n)$ are $m = ...$ and $n = ...$

One now can start expanding the various multiplications that have resulted from the various replacements. Please note that any arithmetic operation involving m or n should be performed as follows, i.e. m and n should be treated like variables:

$$m = 3 \implies 3 \cdot (1 - m) = 3 \cdot (1 - 3) = 3 - 3 \cdot 3 = -2 \cdot 3$$

From the final form of the equation one can read off the wanted x and y values:

$$mx + ny = gcd(m, n)$$

Example Calculate $gcd(17, 7) = 17x + 7y$:

$$
\begin{aligned}
17 &= 2 \cdot 7 + 3 \\
7 &= 2 \cdot 3 + 1 \\
3 &= 3 \cdot 1 + 0 \\
\implies gcd(17, 7) &= 1
\end{aligned}
$$

$$
\begin{aligned}
7 - 2 \cdot 3 &= 1 \\
7 - 2 \cdot (17 - 2 \cdot 7) &= 1 \\
7 - 2 \cdot 17 + 4 \cdot 7 &= 1 \\
5 \cdot 7 - 2 \cdot 17 &= 1 \\
\implies x = -2, y &= 5
\end{aligned}
$$

Example Calculate $gcd(71, 12) = 71x + 12y$:

$$
\begin{aligned}
71 &= 5 \cdot 12 + 11 \\
12 &= 1 \cdot 11 + 1 \\
\implies gcd(71, 12) &= 1
\end{aligned}
$$

$$
\begin{aligned}
12 - 11 &= 1 \\
12 - (71 - 5 \cdot 12) &= 1 \\
6 \cdot 12 - 1 \cdot 71 &= 1 \\
\implies x = -1, y &= 6
\end{aligned}
$$

8.4.3 Calculate the Modular Multiplicative Inverse

Let m and n be two integers, such that $m\rangle n$. Using the EEA, it is possible to calculate the modular multiplicative inverses of m mod n and n mod m respectively:

1. Assure that $gcd(m, n) = 1$ by using the method described in 8.4.1.
2. Find x and y in Bézout's identity by using the method described in 8.4.2:

$$gcd(m, n) = m \cdot x + n \cdot y$$

Getting the Modular Multiplicative Inverses Once the x and y in Bézout's identity have been defined, the modular multiplicative inverses can be read off as follows:

1. The modular multiplicative inverse of n mod m is simply $R_m(y)$:

$$\begin{aligned} & R_m(m \cdot x + n \cdot y) = R_m(1) \\ \implies & R_m(n \cdot y) = R_m(1) \\ \implies & n \cdot y \equiv_m 1 \\ \implies & y \text{ is the modular multiplicative inverse of } n \bmod m \\ \implies & n \text{ is the modular multiplicative inverse of } y \bmod m \text{ (Commutativity)} \end{aligned}$$

2. The modular multiplicative inverse of m mod n is simply $R_n(x)$:

$$\begin{aligned} & R_n(m \cdot x + n \cdot y) = R_n(1) \\ \implies & R_n(m \cdot x) = R_n(1) \\ \implies & m \cdot x \equiv_n 1 \\ \implies & x \text{ is the modular multiplicative inverse of } m \bmod n \\ \implies & m \text{ is the modular multiplicative inverse of } x \bmod n \text{ (Commutativity)} \end{aligned}$$

Example Find the modular multiplicative inverse of 123 mod 43, such that $123 \cdot x \equiv_{43} 1$ holds:

$$\begin{aligned} 123 &= 2 \cdot 43 + 37 \\ 43 &= 1 \cdot 37 + 6 \\ 37 &= 6 \cdot 6 + 1 \\ \implies & gcd(123, 43) = 1 \end{aligned}$$

$$\begin{aligned} 37 - 6 \cdot 6 &= 1 \\ 37 - 6 \cdot (43 - 37) &= 1 \\ (123 - 2 \cdot 43) - 6 \cdot (43 - (123 - 2 \cdot 43)) &= 1 \\ 7 \cdot 123 - 20 \cdot 43 &= 1 \\ \implies & x = 7, y = -20 \end{aligned}$$

The modular multiplicative inverse of 123 mod 43 is $x = 7$.

This can be checked pretty easily:

$$\begin{aligned} & 123 \cdot 7 \equiv_{43} 1 \\ \implies & R_43(123) \cdot R_43(7) = R_43(1) \\ \implies & R_43(-6) \cdot R_43(7) = R_43(1) \\ \implies & R_43(-42) = R_43(1) \\ \implies & R_43(1) = R_43(1) \\ \implies & 1 \equiv_{43} 1 \end{aligned}$$

The modular multiplicative inverse of 43 mod 123 is $y = -20$ respectively.

8.5 Chinese Remainder Theorem

Let $m_1, m_2, ..., m_r$ be pairwise relatively prime integers.

Let $M = \prod_{i=1}^{r} m_i$.

For every list $a_1, a_2, ..., a_r$ with $0 \leq a_i < m_i$ for $1 \leq i \leq r$, the system of congruence equations

$$\begin{aligned} & x \equiv_{m_1} a_1 \\ & x \equiv_{m_2} a_1 \\ & ... \\ & x \equiv_{m_r} a_r \end{aligned}$$

for x has a unique solution x satisfying $0 \leq x < M$.

8.5.1 Steps for Solving the Congruence Equations Using the Chinese Remainder Theorem

1. Let there be a list of congruence equations of the following form:

$$x \equiv_{m_i} a_i \text{ for } 1 \leq i \leq r$$

2. If not already defined, calculate M:

$$M = \prod_{i=1}^{r} m_i$$

3. Let $M_i = M/m_i$. This implies $gcd(M_i, m_i) = 1$ and will be used to calculate N_i.
4. Solve $M_i N_i \equiv_{m_i} 1$ (read the tips below or use the Extended Euclidean Algorithm)
5. Calculate x:

$$R_M\Big(\sum_{i=1}^{r} a_i M_i N_i\Big)$$

6. If asked that a solution for x must be within a given interval, just subtract a multiple of M from x such that the resulting number lies within the defined interval.
7. If no interval is given, then there are infinite solutions in the form of $x + k \cdot M$ with $k \in \mathbb{Z}$

Tips

- In most cases you will not need to use the Extended Euclidean Algorithm to calculate N_i. If $M_i \cdot N_i \equiv m_i 1$ is given, one can try to add / subtract multiples of m_i from M_i and 1 to simplify the calculation of N_i.

  Examples

$$63 \cdot N_1 \equiv_5 1$$
$$3 \cdot N_1 \equiv_5 1$$
$$3 \cdot N_1 \equiv_5 6$$
$$N_1 = 2$$

$$88 \cdot N_2 \equiv_9 1$$
$$7 \cdot N_2 \equiv_9 1$$
$$7 \cdot N_2 \equiv_9 10$$
$$-2 \cdot N_2 \equiv_9 10$$
$$N_2 = -5 \implies N_2 = 4$$

- If an m_i is a rather big integer, and in result the corresponding N_i might therefore be big, too, one can simply subtract multiples of m_i from N_i. This will simplify the multiplication later when calculating x.

  Example

$$M_1 = 35, m_1 = 9, a_1 = 1$$
$$35 \cdot N_1 \equiv_9 1$$
$$N_1 = 8 \implies N_1 = -1$$
$$x = ... - 1 \cdot 1 \cdot 35... + ...$$

- If the a_is of the given congruence equations $x \equiv_{m_i} a_i$ are rather big integers, first simplify them either by subtracting multiples of m_i from a_i, or if a_i is a rather big power, just use the following rule:

$$a_i^k \equiv_{m_i} 1 \implies R_{m_i}(a^k) = 1$$

  Example

$$x \equiv_5 2^{119}$$

$$2^2 \equiv_5 -1 \implies 2^4 \equiv_5 1$$

$$\begin{aligned} R_5(2^{117}) &= R_5(2^{4\cdot 29+3}) = R_5(R_5(2^{4\cdot 29}) \cdot R_5(2^3)) \\ &= R_5(\underbrace{R_5(2^4) \cdot ... \cdot R_5(2^4)}_{29 \text{ times}} \cdot R_5(2^3)) \\ &= R_5(1 \cdot R_5(2^3)) = R_5(8) = 3 \end{aligned}$$

$$x \equiv_5 2^{119} \implies \underline{x \equiv_5 3}$$

Example Let $M = 60 = 4 \cdot 5 \cdot 3$. Find an x in $0 \leq x \leq 60$ such that the following congruence equations hold:

$$x \equiv_4 1$$
$$x \equiv_3 2$$
$$x \equiv_5 3$$

1. Check that the m_1, m_2 and m_3 are pairwise relatively prime:

$$gcd(4,3) = 1$$
$$gcd(4,5) = 1$$
$$gcd(3,5) = 1$$

2. Calculate M_1, M_2 and M_3:

$$M_1 = M/m_1 = 60/4 = 15$$
$$M_2 = M/m_2 = 60/3 = 20$$
$$M_3 = M/m_3 = 60/5 = 12$$

3. Solve the following congruence equations separately:

$$15 \cdot N_1 \equiv_4 1$$
$$20 \cdot N_2 \equiv_3 1$$
$$12 \cdot N_3 \equiv_5 1$$

(i)

$$\begin{aligned} 15 \cdot N_1 &\equiv_4 1 \\ 3 \cdot N_1 &\equiv_4 1 && \text{(Subtract } 3 \cdot 4 \text{ from 15)} \\ 3 \cdot N_1 &\equiv_4 9 && \text{(Add } 2 \cdot 4 \text{ to 1)} \\ \underline{N_1 = 3} \end{aligned}$$

Using the EEA to calculate the multiplicative inverse:

$$\begin{aligned} 15 &= 3 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ &\implies gcd(15, 4) = 1 \end{aligned}$$

Actually, this follows directly from the fact that $M_i = M/m_i \implies gcd(M_i, m_i) = 1$. Nonetheless, this step is needed for the further steps in the calculation of the multiplicative inverse.

(ii)

$$\begin{aligned} 20 \cdot N_2 &\equiv_3 1 \\ 2 \cdot N_2 &\equiv_3 1 && \text{(Subtract } 6 \cdot 3 \text{ from 20)} \\ 2 \cdot N_2 &\equiv_3 4 && \text{(Add 3 to 1)} \\ \underline{N_2 = 2} \end{aligned}$$

(iii)

$$\begin{aligned} 12 \cdot N_3 &\equiv_5 1 \\ 2 \cdot N_3 &\equiv_5 1 && \text{(Subtract } 2 \cdot 5 \text{ from 12)} \\ 2 \cdot N_3 &\equiv_5 6 && \text{(Add 5 to 1)} \\ \underline{N_3 = 3} \end{aligned}$$

4. Calculate x:

$$\begin{aligned} &R_{4 \cdot 3 \cdot 5}(15 \cdot 3 \cdot 1 + 20 \cdot 2 \cdot 2 + 12 \cdot 3 \cdot 3) \\ &= R_{60}(233) \\ &= 53 \\ &\implies \underline{\underline{x = 53}} \end{aligned}$$

9 Algebra

9.1 An Overview

9.1.1 Algebra

An *algebra* or *algebraic structure* is a pair $\langle S; \Omega \rangle$ where S is a set (the *carrier* of the algebra) and $\Omega = (\omega_1, ..., \omega_n)$ is a list of operations on S. The set S is closed under all the operations in Ω.

9.1.2 Semigroup

A *semigroup* is an algebra $\langle S; * \rangle$ that satisfies the following axiom:

(i) *Associativity* $\forall a, b, c \in S : (a \cdot b) \cdot c = a \cdot (b \cdot c)$

9.1.3 Monoid

A *monoid* is an algebra $\langle S; *, e \rangle$ that satisfies the following axioms:

(i) *Associativity* $\forall a, b, c \in S : (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(ii) *Closure* $\forall a, b \in S : a \cdot b \in S$

(iii) *Identity element* $\exists e \in S : \forall a \in S : e \cdot a = a \cdot e = a$

It's important to note that a monoid may or may not contain inverse elements for some $a \in S$; a monoid does not have to satisfy this property.

9.1.4 Group

A *group* is an algebra $\langle S; *, e, ^{-1} \rangle$ that satisfies the following axioms (called the *group axioms*):

(i) *Associativity* $\forall a, b, c \in S : (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(ii) *Closure* $\forall a, b \in S : a \cdot b \in S$

(iii) *Identity element* $\exists e \in S \; \forall a \in S : e \cdot a = a \cdot e = a$

(iv) *Inverse element* $\forall a \in S \; \exists b \in S : a \cdot b = b \cdot a = e$

9.1.5 Subgroup

A subset H of a group $\langle S; *, e, ^{-1} \rangle$ is called *subgroup of G* if $\langle H; *, e, ^{-1} \rangle$ satisfies the group axioms (9.1.4).

9.1.6 Abelian

A group, monoid or semigroup $\langle S; * \rangle$ is called *commutative* or *abelian* if it satisfies the commutative property:

(i) *Commutative property* $\forall a, b \in S : a \cdot b = b \cdot a$

Good to know A group $\langle G; \cdot \rangle$ with $|G| = 1$ is always abelian.

9.1.7 Ring

A *ring* $\langle R; +, -, 0, \cdot, 1\rangle$ is an algebra with the following properties:

(i) $\langle R; +, -, 0\rangle$ is an abelian group

(ii) $\langle R; \cdot, 1\rangle$ is a monoid

(iii) *Distributive properties*

- $a \cdot (b + c) = a \cdot b + a \cdot c$ (left distributive property)
- $(b + c) \cdot a = b \cdot a + c \cdot a$ (right distributive property)

A ring is called *commutative* if multiplication satisfies the commutative property:

(i) *Commutative property* $\forall a, b \in R : a \cdot b = b \cdot a$

9.1.8 Integral Domain

An *integral domain* is a nontrivial commutative ring $\langle R; +, -, 0, \cdot, 1\rangle$ without zero divisors:

(i) $\forall a, b \in R : a \cdot b = 0 \implies a = 0 \vee b = 0$

9.2 Field

A *field* is a nontrivial commutative ring $\langle F; +, -, 0, \cdot, 1\rangle$ in which every nonzero element is a unit, i.e. $U(F) = F\backslash\{0\}$. Verbally, this means that every element except 0 has an (additive and multiplicative) inverse element in F.

A ring F is a field if and only if $\langle F\backslash\{0\}; \cdot, ^{-1}, 1\rangle$ is an abelian group.

A field is also an *integral domain*. For two polynomials a and b, both with degree m, the multiplication of $a^m x^m \neq 0$ and $b^m x^m \neq 0$ always yields a polynomial c of degree $m + m$: $c^{m+m} x^{m+m}$.

9.3 Groups

9.3.1 Finite Groups

Let G be a finite group:

(i) $|G|$ is called the *order* of G

(ii) Every element of the group G has finite order

(iii) $\langle a\rangle$ is the smallest subgroup of G: $\langle a\rangle = \{e, a, a^2, ..., a^{ord(a)-1}$

(iv) If $H \leq G$ is a subgroup of G, then the order of H divides the order of G: $|H| \mid |G|$

(v) The order of every element of G divides the order of G: $\forall a \in G : ord(a) \mid |G|$

(vi) $\forall a \in G : a^{|G|} = e$

(vii) The inverse element of g^i is $g^{|G|-i}$

Commutativity

(i) If $|G| = 1$, then G is commutative

(ii) If G is not commutative, then $|G|\rangle 1$

9.3.2 Cyclic Groups

Let $\mathbb{Z}_n$ be a cyclic group with n elements:

(i) If $a \in \mathbb{Z}_n$ is prime, then $ord(a) = |\mathbb{Z}_n| = n$

Inverse elements Let G be an infinite group. The inverse element of g^i is g^{-i}

Example of an infinite group $\langle \mathbb{Z}, +\rangle$

9.4 Rings

9.4.1 The Ring of Polynomials $R[x]$

The ring $R[x]$ is the ring of polynomials with coefficients from a ring R

9.4.2 The Ring of Polynomials $K[x]$

The ring $K[x]$ is the ring of polynomials with coefficients from a field K.

On why $K[x]$ is not a field Finding a multiplicative inverse of any polynomial in the field $K[x]$ is impossible.

Proof. Lets assume $K[x]$ is a field. Since the zero polynom is not part of the multiplicative group $\langle K\backslash\{0\}; \cdot, ^{-1}, 1\rangle$ of the field $K[x]$, the multiplication of two polynomials with a respective degree m and n yields a new polynomial with the degree $m + n$. Because of this fact, one cannot find an inverse polynom k^{-1} such that the multiplication with the respective polynom k results in the neutral element, namely the constant polynom 1 with degree 0. Therefore, $K[x]$ cannot be a field.

9.5 Fields

9.5.1 Galois Field

A field with q elements is denoted as $GF(q)$.

9.5.2 Working With Multiplicative Inverses In A Field $GF(q)$

Let $a, b \in GF(q)$ with $a < b$. Let the equation $a \cdot b^{-1}$ be part of this.

1. If it is the case to calculate , then first assure that $gcd(a,b) \neq 1 \wedge gcd(a,b) = b$ and then simply divide a with b.

   Example

   $$2, 4 \in GF(7)$$
   $$2 \cdot x = 4$$
   $$x = 4 \cdot 2^{-1} = 4/2 = 2$$

2. If $gcd(a,b) = 1$, just solve $b \cdot x \equiv_q 1$ for x. x will be the multiplicative inverse b^{-1}.

Note: This is just a mnemonic, since it is known that the division operation is not part of a field's set of operations, and also only holds when $gcd(a,b) = b$.

10 Logik

- Korrekte Kalküle: Wahrheitstabelle aufstellen. Wenn Modell für Vorbedingung, dann muss es auch ein Modell für die Konklusion sein.
- Erfüllbar: Ein Modell existiert, also eine Belegung, die die Formel erfüllt.
- Gültig: Tautologie
- **Syntax**: F Formel, G Formel, dann ist $F \oplus G$ eine Formel
  Semantik:
  $$\mathcal{A}(F \oplus G) = \begin{cases} 1, & \text{falls } \mathcal{A}(F) = 1 \wedge \mathcal{A}(G) = 0 \\ 0, & \text{sonst} \end{cases}$$
- Man unterscheidet zwischen *Terme* und *Formeln*
  - Terme: Funktionen (Funktionssymbole), freie Variablen
  - Formeln: Prädikate inkl. $\forall, \exists$. Formeln der Art $F \wedge G, F \vee G, \neg G$
- Die Identität (=) kann nur auf Terme angewendet werden!
- $F \models G \iff G$ ist eine Folgerung von F, d.h. alle Modelle von F sind auch Modelle von G
- *Passend*: Eine Struktur I heisst *passend*, wenn diese alle Prädikate, freien Variablen, Funktionen und zusätzlich das Universum für eine Formel definiert
- Pränexform: $F = Q_1 y_1 Q_2 y_2 \ldots Q_k y_k \hat{F}$. In $\hat{F}$ darf kein Quantor vorkommen. Vorgehen: Substitution, falls freie Variable gleich benannt ist wie Quantorvariable.
- Skolemform: Ersetze alle Existenzquantoren mit Funktionssymbole, also $F = \forall y_1 \forall y_2 ... \forall y_n \exists x G \implies F := \forall y_1 \forall y_2 ... \forall y_n G\left[x/f\left(y_1, ..., y_n\right)\right]$

11 Tipps zur Prüfung

11.1 Logik

11.1.1 Universum nicht vergessen

Wird verlangt, Aussagen formal durch Prädikate zu schreiben, so sollte man nie vergessen, das Universum $\mathcal{U}$ zu definieren. Beispiel: $\mathcal{U} = \mathbb{R}$

11.2 Relationen

11.2.1 Matrixdarstellung

Sei M_ρ die Matrixdarstellung der Relation ρ und $\hat{\rho}$ die Inverse eben dieser Relation; dann gilt

$$M_{\hat{\rho}} = M_\rho^T$$

Für den Eintrag m_{ij} der Matrix M_ρ gilt:

$$m_{ij} = 1 \iff i \; \rho \; j$$

11.3 Algebra

11.3.1 Schnelle Möglichkeit um Untergruppen festzustellen

Beispiel: Finde alle Untergruppen von $\langle \mathbb{Z}_{18}, \oplus \rangle$.

1. Alle teilerfremden Zahlen zu 18 bilden Untergruppen der gleichen Ordnung: $\langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle = \mathbb{Z}_{18}$
2. Teilt Zahl x die Zahl 18, so bildet $\langle x \rangle$ eine Untergruppe von $\mathbb{Z}_{18}$ mit $\frac{18}{x}$ Elementen
3. Für die restlichen Zahlen gilt: Sei $d = \text{gcd}(y, 18) \implies \text{ord}(y) = \frac{18}{d} \implies \langle y \rangle$ ist Untergruppe mit $\frac{18}{d}$ Elementen.
   Beispiel: $\text{gcd}(15, 18) = 3 \implies \text{ord}(15) = 6(6 \cdot 15 = 90 \implies 90 \text{mod} 18 = 0 \checkmark) \implies$ $\langle 15 \rangle$ ist Untergruppe mit 6 Elementen

11.4 Zahlentheorie, modulare Arithmetik

11.4.1 Anzahl Nullteiler in einem Ring

Sei $\langle \mathbb{Z}_m, \oplus, \odot \rangle$ gegeben. Die Anzahl Nullteiler ist nun $m - \varphi(m) - 1$.
Es gilt $\varphi(m) = \varphi(n) \cdot \varphi(o)$ und $\varphi(p^k) = p^{k-1} \cdot (p-1)$ mit p prim.