ETH Zürich, D-INFK
HS 2017, 6. November 2017

Prof. Ueli Maurer
Marta Mularczyk

# Diskrete Mathematik

# Solution 8

## 8.1 Diffie-Hellman

**a)** Let $g \in \langle \mathbb{Z}_n; \oplus \rangle$ be the generator, which Alice and Bob use as the basis. Alice chooses $x_A$ at random from $\{0, \ldots, n-1\}$ and sends $y_A = R_n(g \cdot x_A)$. Analogously, Bob chooses $x_B$ at random from $\{0, \ldots, n-1\}$ and sends $y_B = R_n(g \cdot x_B)$. The established shared key is $k_{AB} = R_n(g \cdot x_A \cdot x_B)$.

As shown in Example 5.26, we have $\gcd(g, n) = 1$. Therefore, Eve can use the Extended GCD algorithm to efficiently find an $a \in \mathbb{Z}$ such that $a \cdot g \equiv_n 1$. Then she can compute $k_{AB}$ using the eavesdropped messages $y_A$ and $y_B$ and Lemma 4.18 as follows: $k_{AB} = R_n(a \cdot y_A \cdot y_B)$. This is because

$$k_{AB} \equiv_n g \cdot x_A \cdot x_B \equiv_n g \cdot x_A \cdot (a \cdot g) \cdot x_B \equiv_n a \cdot (g \cdot x_A) \cdot (g \cdot x_B) \equiv_n a \cdot y_A \cdot y_B$$

**b)** No, Bob's conclusion is not correct. Even if two groups have the exact same structure, certain operations may be possible to compute much more efficiently in one of them than in the other.

Of course, it is possible to solve a given problem in any cyclic group by first applying an isomorphism, then finding a solution in $\langle \mathbb{Z}_n; \oplus \rangle$ and finally applying the inverse of the isomorphism to obtain a solution to the original problem. Since such isomorphism always exists, the above procedure always yields a correct solution. However, it is not clear whether the isomorphism or its inverse can be computed efficiently. Consider for example any cyclic group $G = \langle g \rangle$ of order $n$ and the isomorphism $\phi$ from $G$ to $\langle \mathbb{Z}_n; \oplus \rangle$ given by $\phi : g^i \mapsto i$. Computing $\phi$ corresponds exactly to solving the discrete logarithm problem in $G$.

## 8.2 Algebras

**a)** $\langle \mathbb{Z}; \star \rangle$ is neither a group nor a monoid, because $\star$ is not associative. The counterexample is the following:

$$2 \star (0 \star 0) = 2 \star 0 = 4 \neq 16 = 4 \star 0 = (2 \star 0) \star 0$$

**b)** $\langle \mathcal{P}(X); \cup \rangle$ is a commutative monoid but not a group.

Associativity and commutativity of $\cup$ follows directly from Theorem 3.4. We now have to prove that $\varnothing$ is the neutral element. Indeed, $\varnothing \in \mathcal{P}(X)$ by definition of the power set and for all $A \in \mathcal{P}(X)$, we have $A \cup \varnothing = \varnothing \cup A = A$. By the commutativity of $\cup$, the given algebra is a commutative monoid.

To prove that it is not a group, we give a counterexample to the third group axiom **G3**. Since $X \neq \varnothing$, there exists an $x \in X$. Therefore, $\{x\} \in \mathcal{P}(X)$. Assume for contradiction that there exists an inverse element of $\{x\}$, that is, assume that there exists an $A \in \mathcal{P}(X)$ such that $\{x\} \cup A = \varnothing$. But since $x \in \{x\} \cup A$, this is a contradiction.

### 8.3 Facts about groups

**a)** We have to show that any right neutral element is also a left neutral element. To this end, assume that $e$ is a right neutral element, that is, that $a * e = a$ for all $a \in G$. *(1 Point)*

It follows that *(1 Point)*

$$e * a \overset{\text{G3}}{=} (a * \widehat{a}) * a \overset{\text{G1}}{=} a * (\widehat{a} * a) \overset{\text{G3}}{=} a * e \overset{\text{G2'}}{=} a$$

An equally good solution would be to prove that both $a$ and $\widehat{(\widehat{a})}$ are inverses of $\widehat{a}$ and then argue that, by Lemma 5.2, they must be equal.

**b)** We have $(a * b) * (\widehat{b} * \widehat{a}) = e$, because:

$$(a * b) * (\widehat{b} * \widehat{a}) \overset{\text{G1}}{=} a * \Big(b * (\widehat{b} * \widehat{a})\Big) \overset{\text{G1}}{=} a * \Big((b * \widehat{b}) * \widehat{a}\Big) \overset{\text{G3}}{=} a * (e * \widehat{a}) \overset{\text{G2}}{=} a * \widehat{a} \overset{\text{G3}}{=} e$$

*(1 Point)*

Therefore, $\widehat{b} * \widehat{a}$ is the inverse of $a * b$. *(1 Point)*

**c)** Assume that $a * b = a * c$. It follows that

$$\begin{aligned} a * b = a * c &\overset{\text{G3}}{\Longrightarrow} \widehat{a} * (a * b) = \widehat{a} * (a * c) \\ &\overset{\text{G1}}{\Longrightarrow} (\widehat{a} * a) * b = (\widehat{a} * a) * c \\ &\overset{\text{G3}}{\Longrightarrow} e * b = e * c \\ &\overset{\text{G2}}{\Longrightarrow} b = c \end{aligned}$$

*(1 Point)*

### 8.4 Structure of groups

**a)** Assume that for all $x \in G$, we have $x * x = e$. We have to show that $a * b = b * a$ for all $a, b \in G$.

Note that if for any $x \in G$ we have $x * x = e$, then every element $x$ of $G$ is its own inverse: $x = \widehat{x}$. Therefore, for any $a, b \in G$ we have $a * b = \widehat{a * b} \overset{\text{Lemma 5.3}}{=} \widehat{b} * \widehat{a} = b * a$.

**b)** In this proof we will use Definition 5.11 of a subgroup and refer to the individual properties (1), (2) and (3), specified in that definition. We will also refer to group axioms **G1**, **G2**, **G3** of $G$.

$\Longrightarrow$: Assume that $H$ is a subgroup of $G$. Then $H \neq \varnothing$, because $e \in H$ by (2). Moreover, take any $a, b \in H$. By (3), we have that $\widehat{b} \in H$ and, hence, by (1) it follows that $a * \widehat{b} \in H$.

$\Longleftarrow$: Assume that $H$ is a non-empty subset of $G$ such that $a * \widehat{b} \in H$ for all $a, b \in H$. We show that $H$ fulfills the definition of a subgroup:

**(2):** Since $H \neq \varnothing$, there exists an $a \in H$. Therefore, $e \overset{\text{G3}}{=} a * \widehat{a} \in H$ by assumption.

**(3):** Take any $a \in H$. Since we already showed that $e \in H$, we have $\widehat{a} \overset{\text{G2}}{=} e * \widehat{a} \in H$ by assumption.

**(1):** Take any $a, b \in H$. Since we already showed that $\widehat{b} \in H$, we have $a * b = a * \widehat{(\widehat{b})} \in H$ by assumption (here the equality follows from Lemma 5.3).

Since $H$ fulfills (1), (2) and (3), it is a subgroup of $G$.

### 8.5 Symmetries of a cube

**a)** First of all, one has to decide which corner of the sofa coincides with the corner of the room. For this, there are $8$ possibilities. Once this corner is set, there are $3$ edges coming out of this corner (one of them going up) and, hence, $3$ possibilities to place the sofa. Once the corner and the edge going up are fixed, the position of the sofa is fully defined. Thus, there are $24$ possibilities overall.

**b)** Let us first determine $|R|$. Assume that the sofa stands in the corner in a certain (arbitrary) position. After a rotation $b$, it may end up in one of the $24$ possible positions (this follows from Subtask a) ). Therefore, we can distinguish $24$ different rotations and $|R| = 24$.

It is possible to describe each element of $R$ as a rotation around single axis. To see this, consider all possible different rotations of a cube around an axis:

- Identity.
- Rotation around the centers of two opposite faces. There are $3$ pairs of opposite faces and for each pair there are $3$ possible rotations: by $90$, $180$ and $270$ degrees. Together, this gives $9$ rotations.
- Rotation around two opposite vertices. There are $4$ pairs of opposite vertices and for each pair there are $2$ possible rotations: by $120$ and $240$ degrees. Together, this gives $8$ rotations
- Rotation around the centers of two opposite edges. There are $6$ pairs of opposite edges and for each pair there is only one possible rotation: by $180$ degrees. Together, this gives $6$ rotations.

One can see (for example by drawing the cube after each rotation) that no two of the above rotations end up with the cube being in the same position. Since together we described $24$ rotations and $|R| = 24$, each element of $R$ corresponds to *exactly one* rotation.

**c)** $\langle R; \circ \rangle$ is a group. Since function composition is associative, $\circ$ is associative as well (this is because every rotation corresponds to a permutation of vertices). The neutral

element is the identity. Furthermore, every element has an inverse, namely a rotation around the same axis by $360$ degrees minus the original angle.

**d)** The operation $\circ$ is not commutative. Figure 1 illustrates that there exist rotations, which do not commute.

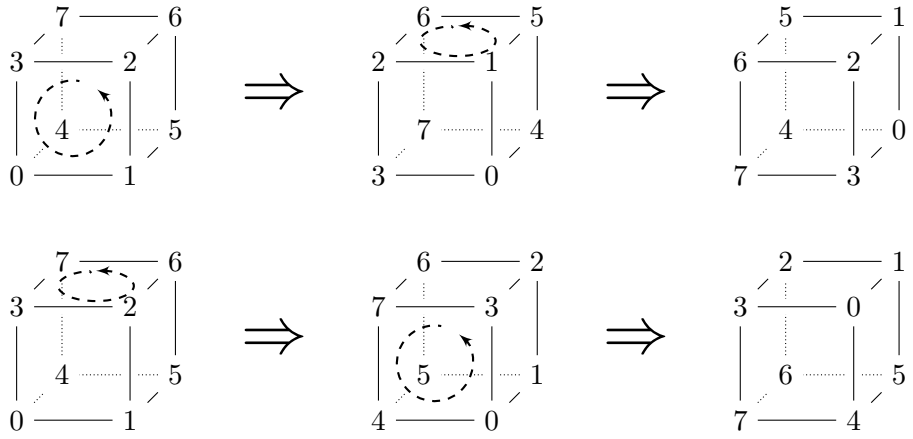


Figure 1: $\langle R; \circ \rangle$ is not commutative.