

Übung 11

Nachbesprechung

$$3.4.) a^q = \left(\sum_{k=1}^n 1_q \right)^q \stackrel{(*)}{=} \sum_{k=1}^n 1_q^q$$

(*) Subtask 3

Um Resultat aus Teilaufgabe 3.3.) anzuwenden muss gelten:

- $n \geq 1$ (Spezialfall $a=0$)
- q ist Charakteristik vom Körper $\mathbb{Z}_q$ (kleinste n , so dass $n \cdot q = 0$)

Fehler korrigierende Codes

Anwendung: z.B. Daten werden verschickt über WLAN in Form von bits.

Es kann zu Übertragungsfehler kommen: Daten fehlen oder kommen verändert an

Alice 0001 $\xrightarrow{\text{⚡}}$ 0000 Bob

Idee: wir wollen mehr bits mitschicken, um Fehler erkennen oder korrigieren zu können z.B. Alice verdoppelt jedes bit 00 00 00 11

Def. (n, k) -Kodierfunktion: Injektive Funktion $E: A^k \rightarrow A^n$, die eine Nachricht auf ein Codewort abbildet. ($n-k$ zusätzliche Symbole für Redundanz)

$C = \text{Im}(E)$ ist die Menge aller Codewörter

z.B. $0001 \mapsto 00\ 00\ 00\ 11$ (ineffizient) für $E: \{0,1\}^4 \rightarrow \{0,1\}^8$

Hamming Distanz zwischen zwei Strings ist die Anzahl an Stellen, an denen sich beide Strings unterscheiden.

Minimale Distanz von C ist die kleinste Hamming Dist. zwischen zwei $x, y \in C$.

Minimale Distanz von C ist $2t+1$

$\Leftrightarrow$ es können $\leq 2t$ Fehler erkannt werden

$\Leftrightarrow$ es können $\leq t$ Fehler korrigiert werden

Logik

Beweissystem $\Pi = (S, P, \tau, \phi)$

- S Aussagen
- P Beweise von Aussagen $s \in S$
- $\tau: S \rightarrow \{0,1\}$ Funktion die angibt, ob Aussage $s \in S$ wahr ist
- $\phi: S \times P \rightarrow \{0,1\}$ Funktion die den Beweis verifiziert
 $\phi(s,p) = 1$ heisst, dass p ein gültiger Beweis für s ist

Bsp. $\Pi = (S, P, \tau, \phi)$

$S = \mathbb{N}$ Aussagen

$\tau(s) = 1 \Leftrightarrow s$ ist keine PZ für $s \in S$

$P = \mathbb{N}$ Beweise

$\phi(s,p) = 1 \Leftrightarrow p|s$ und $1 < p$ und $p < s$

z.B. $\tau(6) = 1$ und 2 ist ein gültiger Beweis, da $\phi(6,2) = 1$

Beweissystem $\Pi = (S, P, \tau, \phi)$ ist **sound / korrekt**, wenn für jedes $s \in S$ gilt: wenn $\tau(s) = 0$, dann existiert kein $p \in P$ mit $\phi(s,p) = 1$.
Es existiert kein Beweis für eine falsche Aussage.

Beweissystem $\Pi = (S, P, \tau, \phi)$ ist **complete / vollständig**, wenn für jedes $s \in S$ gilt: wenn $\tau(s) = 1$, dann existiert ein $p \in P$ mit $\phi(s,p) = 1$.
Für jede korrekte Aussage existiert ein Beweis.

Aufg. Gib ein Beweissystem, welches korrekt ist, aber nicht vollständig
 $\Pi = (S, P, \tau, \phi)$, wobei
 $S = P = \{0,1\}$
 $\tau(s) = 1$ für alle $s \in S$
 $\phi(s,p) = 0$ für alle $s \in S$ und $p \in P$

Bsp. Gib ein korrektes und vollständiges Beweissystem an für Aussagen der Form "F ist erfüllbar", wobei F eine Aussagenlogische Formel ist und nur die atomaren Formeln A, B und C beinhaltet.

Sei $S = P = \{0,1\}^*$. Alle möglichen Symbole in F sind $\Sigma = \{A, B, C, \wedge, \vee, \neg, (,)\}$, und wir können jedes Symbol als Element aus $\{0,1\}^3$ verschlüsseln

e.g. $A \mapsto 000, B \mapsto 001 \dots$ #bits in S

Wir definieren $\tau(s) = 1 \Leftrightarrow |s| = 3 \cdot k$ für ein $k \in \mathbb{N}$ und s verschl. eine syntaktisch korrekte aussagenlogische Formel, die erfüllbar ist und nur A, B und C verwendet

Wir definieren $\phi(s,p) = 1 \Leftrightarrow$

- 1.) s ist eine syntaktisch korrekte aussagenlogische Formel und beinhaltet nur atomare Formeln A, B und C
- 2.) $|p| = 3$
- 3.) Die drei bits aus p beschreiben eine Interpretation A für Variablen A, B und C und die von s verschlüsselte Formel ist wahr unter p

Aufg. Seien Π_1 und Π_2 wieder zwei Beweissys. Wir verbinden sie zu einem neuen Beweissystem: $\Pi_3 = (S_1 \times S_2, P_1 \times P_2, \tau_3, \phi_3)$, wobei

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

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

Beweise oder widerlege: Π_3 ist vollständig $\Rightarrow \Pi_1$ oder Π_2 ist vollständig

Gegenbsp. Sei $S_1 = S_2 = \{s\}$, $P_1 = P_2 = \{p\}$, $\tau_1(s) = \tau_2(s) = 1$ und $\phi_1(s, p) = \phi_2(s, p) = 0$. Dann gilt $\tau_3(s, s) = 0$ und $\phi_3((s, s), (p, p)) = 0$. Π_3 ist vollständig, da kein $(s, s) \in S_1 \times S_2$ mit $\tau_3(s, s) = 1$ existiert. Weder Π_1 , noch Π_2 ist vollständig, da $\tau_1(s) = \tau_2(s) = 1$, aber kein $p' \in P_1$ existiert mit $\phi_1(s, p') = 1$ oder $\phi_2(s, p') = 1$.

Syntax und Semantik

Syntax definiert welche Zeichenfolgen als Formeln gelten

Bsp. $\forall x(A \neq B)$ oder $(A \wedge B$ sind syntaktisch inkorrekt, also keine Formeln

Semantik definiert eine Funktion, welche alle Elemente in einer Formel erkennt, die frei vorkommen

Bsp. $A \wedge B$

A und B sind frei (In Aussagenl. alle Var.)

$P(x)$

P und x

$\forall x P(x) \wedge Q(x)$

P, Q und zweites x

↑ gebunden ↑ frei

u gehört nicht dazu

Eine Interpretation heisst passend, wenn sie allen freien Elementen einen Wert zuweist
(passende)

Eine Interpretation A heisst Modell für F, falls F wahr ist unter A

Aufg. Finde ein Modell für $F = (\underline{A} \vee \underline{B}) \rightarrow (\neg \underline{A} \wedge \underline{B})$ A, B frei

A mit $A(A) = A(B) = 0$

oder A' mit $A'(A) = 0$ und $A'(B) = 1$

Aufg. Wenn F und G Formeln sind, so dass $\neg F$ und $F \vee G$ erfüllbar sind, dann ist G erfüllbar.

Gegenbsp. Sei $F = A$ und $G = A \wedge \neg A$. Seien A_1 und A_2 Interpretationen mit $A_1(A) = 1$ und $A_2(A) = 0$. Dann gilt $A_2(\neg F) = 1$ und $A_1(F \vee G) = 1$, also sind $\neg F$ und $F \vee G$ erfüllbar, aber G ist unerfüllbar, da $A(A) = 1$ und $A(A) = 0$ nicht gleichzeitig wahr sein kann

Kalkül

Beinhaltet Ableitungsregeln um Formeln herzuleiten

Ein Kalkül K ist korrekt, wenn für alle M und F gilt $M \vdash_K F \Rightarrow M \models F$

Ein Kalkül K ist vollständig, wenn für alle M und F gilt $M \models F \Rightarrow M \vdash_K F$

Aufg. Kalkül K hat folgende Regeln: $\Delta F \rightarrow G, F \vdash \vdash_{R1} G$

$$\emptyset \vdash_{R2} F \rightarrow (G \rightarrow F)$$

$$\emptyset \vdash_{R3} (F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H))$$

Ist K korrekt?

Müssen überprüfen, ob R_1, R_2, R_3 korrekt sind.

Also ob für alle $F \vdash_R G$ auch $F \models G$ gilt.

$\emptyset \vdash_R G$ heisst G ist Tautologie

$\Delta F, G \vdash_R H$ heisst $F \wedge G \models H$

R1:	F	G	$F \rightarrow G$	$(F \rightarrow G) \wedge F$	G
	0	0	1	0	0
	0	1	1	0	1
	1	0	0	0	0
	1	1	1	1	1

Ja, die Regel R_1 ist korrekt

(das gleiche für R_2, R_3 beweisen)

Aufg. Kalkül: $\Delta \neg F \vdash \vdash_{R1} F \rightarrow G$

$$\emptyset \vdash_{R2} F \rightarrow (G \rightarrow F)$$

Kann man $\emptyset \vdash A \rightarrow A$ im Kalkül zeigen? Nein

Angenommen $A \rightarrow A$ kann aus $\emptyset$ geschlossen werden, dann müsste R_1 die letzte Regel sein, die angewendet worden ist, da R_2 nicht matched. Um R_1

anzuwenden ist jedoch $\neg A$ als Prämisse nötig. $\neg A$ kann jedoch nicht aus diesen Regeln geschlossen werden, da alle rechten Seiten die Form $F \rightarrow G$ haben.

Also ist das Kalkül nicht vollständig.

Aufg.

$$\{F \rightarrow G, F\} \vdash_{R_1} G$$

Kalkül K:

 $\emptyset$ $\vdash_{R_2}$

$$F \rightarrow (G \rightarrow F)$$

gleiche Form

 $\emptyset$ $\vdash_{R_3}$

$$(F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H))$$

$$\rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H))$$

Leite $A \rightarrow A$ in K her von $\emptyset$

$$\begin{array}{c} \begin{array}{c} (R_3) \\ \hline G \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)) \\ (R_1) \end{array} \quad \begin{array}{c} \hline G \\ (R_2) \end{array} \\ \hline (A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A) \quad \begin{array}{c} \hline A \rightarrow (A \rightarrow A) \\ (R_2) \end{array} \\ \hline A \rightarrow A \quad (R_1) \end{array}$$

wobei $G := A \rightarrow ((A \rightarrow A) \rightarrow A)$