DHBW Mannheim
angewandte Informatik - TINF21

Abgabe: 23.10.2022
Codierungstheorie

Lösung zu Übungsblatt 2

Aufgabe 1.

a) Zeigen Sie, dass die ISBN–10–Codierung Zahlendreher erkennt, dh. das folgendes gilt: Ist $a_1a_2 \dots a_9a_{10}$ ein korrekte ISBN–10–Code, werden zwei aufeinanderfolgende Positionen der Ziffernfolge $a_1a_2 \dots a_9a_{10}$ (die sich inhaltlich unterscheiden) vertauscht, und bezeichnet $\widetilde{a}_1\widetilde{a}_2 \dots \widetilde{a}_9\widetilde{a}_{10}$ die Zeichenfolge, die durch dieses Vertauschen entsteht, so passt $\widetilde{a}_{10}$ als Prüfsumme nicht mehr zu den Positionen $\widetilde{a}_1\widetilde{a}_2 \dots \widetilde{a}_8\widetilde{a}_9$.

Hinweis: Beachten Sie dabei, dass auch die Positionen 9 und 10 vertauscht werden können.

Lösung:

Zunächst beachten Sie, dass

$$\sum_{l=1}^{9} l \cdot a_l = a_{10} \mod 11$$

Das ist gleichbedeutend mit

$$\sum_{l=1}^{9} l \cdot a_l - a_{10} = 0 \mod 11$$

also, weil $-1 \equiv 10 \mod 11$, mit

$$\sum_{l=1}^{9} l \cdot a_l + 10 \cdot a_{10} = 0 \mod 11$$

bzw. mit

$$\sum_{l=1}^{10} l \cdot a_l = 0 \mod 11$$

Nachzurechnen ist, dass diese Bedingung nach einem Zahlendreher immer verletzt ist. Wir nehmen dazu an, dass die Positionen i und $i+1$ (für ein $i \in \{1, \dots, 9\}$ mit $a_i \neq a_{i+1}$) vertauscht sind, sodass wir also die neue Ziffernfolge $\widetilde{a}_1\widetilde{a}_2 \dots \widetilde{a}_9\widetilde{a}_{10}$ haben, für die gilt

$$\widetilde{a}_l = \begin{cases} a_{i+1} & \text{falls } l = i \\ a_i & \text{falls } l = i+1 \\ a_l & \text{sonst} \end{cases}$$

und wir haben zu zeigen, dass

$$\sum_{l=1}^{10} l \cdot \widetilde{a}_l \neq 0 \mod 11$$

Schreiben wir das aus, so ist zu zeigen

$$\sum_{l \neq i, i+1} l \cdot a_l + i \cdot a_{i+1} + (i+1) \cdot a_i \neq 0 \mod 11$$

Dazu formen wir diesen Ausdruck um:

$$\begin{aligned} \sum_{l \neq i, i+1} l \cdot a_l + i \cdot a_{i+1} + (i+1) \cdot a_i &= \sum_{l \neq i, i+1} l \cdot a_l + (i+1) \cdot a_{i+1} - a_{i+1} + i \cdot a_i + a_i \\ &= \sum_{l=1}^{10} l \cdot a_l + a_i - a_{i+1} \end{aligned}$$

Nun ist nach Voraussetzung

$$\sum_{l=1}^{10} l \cdot a_l = 0 \mod 11$$

und damit gilt

$$\sum_{l=1}^{10} l \cdot \widetilde{a}_l = \sum_{l=1}^{10} l \cdot a_l + a_i - a_{i+1} = a_i - a_{i+1} \mod 11$$

Da aber nun $a_i, a_{i+1} \in \{0, \ldots, 9, X = 10\}$ sind und voneinander verschieden sind, ist $a_i \neq a_{i+1} \mod 11$ und damit $a_i - a_{i+1} \neq 0 \mod 11$.

Also passt das Prüfzeichen nicht mehr zum Rest der Ziffernfolge.

b) Stimmt die Aussage aus Teil a) auch für die ISBN–13–Codierung?

Lösung:

Für die ISBN–13–Codierung stimmt diese Aussage nicht mehr. Betrachten wir dazu etwa das Buch mit der Buchkennung 978−3−662−53866−1. Dann gilt hierfür

$$9 + 8 + 6 + 2 + 3 + 6 + 1 + 3 \cdot (7 + 3 + 6 + 5 + 8 + 6) = 140 \equiv 0 \mod 10$$

sodass es sich also um einen korrekten ISBN–13–Code handelt (es gibt in der Tat ein Buch mit dieser Kennzeichnung). Vertauschen wir die Stellen 9 und 10, so erhalten wir 978−3−662−58366−1, und hierfür gilt

$$9 + 8 + 6 + 2 + 8 + 6 + 1 + 3 \cdot (7 + 3 + 6 + 5 + 3 + 6) = 130 \equiv 0 \mod 10$$

also auch das wäre ein korrekter Prüfcode. Die Prüfsumme hat also den Zahlendreher hier nicht erkannt.

Generell gilt: Unterscheiden sich zwei aufeinanderfolgende Ziffern a_i und a_{i+1} in dem ISBN–13–Code um 5, so kann ein Zahlendreher nicht erkannt werden. Setzen wir dazu

$$s = \sum_{i=1}^{7} a_{2i-1} + \sum_{i=1}^{7} 3 \cdot a_{2i}$$

für die Prüfsumme des korrekten ISBN–13–Codes (so dass also $S \equiv 0 \bmod 10$), so gilt, falls i gerade ist

$$\widetilde{s} = \sum_{i=1}^{7} \widetilde{a}_{2i-1} + \sum_{i=1}^{7} 3 \cdot \widetilde{a}_{2i} = s + 2 \cdot a_{i+1} - 2 \cdot a_i$$

Daher gilt

$$\widetilde{s} - s = 2 \cdot (a_{i+1} - a_i)$$

und deshalb stimmen die beiden Prüfsummen modulo 10 überein, wenn $a_{i+1} - a_i$ ein Vielfaches von 5 ist. Entsprechend gilt für i ungerade

$$\widetilde{s} - s = 2 \cdot (a_i - a_{i+1})$$

und damit können auch hier Zahlendreher nicht erkannt werden, wenn sich a_i und a_{i+1} um 5 unterscheiden.

Aufgabe 2.

a) Für ein Buch werden als ISBN–10 bzw. als ISBN–13–Code folgende Zahlenfolgen übermittelt

$$\text{ISBN–10}: \ 3{-}8348{-}1927{-}X, \quad \text{ISBN–13}: \ 978{-}3{-}8348{-}1927{-}7$$

Überprüfen Sie, ob diese beiden Daten korrekt sein können.

Lösung:

Für den ISBN–10–Code erhalten wir

$$1 \cdot 3 + 2 \cdot 8 + 3 \cdot 3 + 4 \cdot 4 + 5 \cdot 8 + 6 \cdot 1 + 7 \cdot 9 + 8 \cdot 2 + 9 \cdot 7 = 232$$

Da

$$232 = 21 \cdot 11 + 1$$

wäre die passende Prüfziffer zu den ersten 10 Ziffern $p = 1$ und nicht $a_{10} = X(= 10)$ wie hier angegeben. Es trat also entweder bei der Übermittlung der ersten neun Ziffern oder der der Prüfziffer ein Fehler auf, die Daten sind daher nicht korrekt übermittelt worden.

Für den ISBN–13–Code gilt

$$9+8+8+4+1+2+7+3\cdot(7+3+3+8+9+7)=150\equiv 0 \mod 10$$

Die Prüfsummenbedingung ist also erfüllt und spricht nicht gegen die Korrektheit der Daten.

b) Die neun informationstragenden Positionen eines Buches sind 3−662−47973. Bestimmen Sie den ISBN–10- und den ISBN–13–Code dieses Buches (Buchkennung für ISBN–13: 978).

Lösung:

Zur Bestimmung des ISBN–10–Codes berechnen wir

$$s=1\cdot 3+2\cdot 6+3\cdot 6+4\cdot 2+5\cdot 4+6\cdot 7+7\cdot 9+8\cdot 7+9\cdot 3=249$$

Damit gilt

$$249=22\cdot 11+7$$

also erhalten wir die Prüfziffer $a_{10}=7$ und damit ist der ISBN–10–Code dieses Buches 3−662−47973−7.

Zur Bestimmung des ISBN–13–Codes ist $a_{13}\in\{0,\ldots,9\}$ so zu bestimmen, dass $s+a_{13}$ durch 10 teilbar ist, wobei

$$s=9+8+6+2+7+7+3\cdot(7+3+6+4+9+3)=135$$

Daher ist $a_{13}=5$ zu wählen und wir erhalten für dieses Buch den ISBN–13–Code 978−3−662−47973−5.

Aufgabe 3. Wir betrachten Information, die in 5 Zahlen a_1, a_2, a_3, a_4 und a_5 mit $a_i\in\{0,\ldots,12\}$ abgelegt ist. Für die Speicherung werden zwei Kontrollzahlen $a_6,a_7\in\{0,\ldots,12\}$ hinzugefügt, so dass gilt

1. Die Zahl $a_1+a_2+a_3+a_4+a_5+a_6+a_7$ ist durch 13 teilbar.
2. Die Zahl $12\cdot a_1+10\cdot a_2+8\cdot a_3+6\cdot a_4+4\cdot a_5+2\cdot a_6+a_7$ ist durch 13 teilbar.

Beim Auslesen erhalten Sie die Zahlenfolge (10, 9, 7, 9, 4, 8, 11).

- Handelt es sich um eine fehlerfrei ausgelesene Information?

Lösung:

Wir erhalten die beiden Prüfsummen

$$\mathrm{PS}_1=10+9+7+9+4+8+11=58=6 \mod 13$$

(womit schon klar ist, dass die Daten nicht fehlerfrei ausgelesen wurden) und

$$\mathrm{PS}_2 = 12 \cdot 10 + 10 \cdot 9 + 8 \cdot 7 + 6 \cdot 9 + 4 \cdot 4 + 2 \cdot 8 + 1 \cdot 11 = 363 = 12 \mod 13$$

Auch die zweite Prüfsumme ist $\neq 0$ und zeigt erneut, dass die Daten fehlerhaft ausgelesen wurden.

- Versuchen Sie gegebenenfalls, die Information zu rekonstruieren, wenn Sie annehmen, dass maximal ein Fehler beim Auslesen aufgetreten ist.

  Lösung:

  Wir gehen vor wie in der Vorlesung und suchen zunächst mal die fehlerhafte Stelle. Dazu benutzen wir wieder die Tatsache, dass in der zweiten Prüfsumme jede Position ein anderes Gewicht hat. Aus diesen Gewichtungen ergeben sich die folgenden Prüfsummenverhältnisse (immer $\mod 13$ gerechnet).

Fehler an der Stelle 1:	Prüfsumme 2	$\equiv$	$12 \cdot$ Prüfsumme 1
Fehler an der Stelle 2:	Prüfsumme 2	$\equiv$	$10 \cdot$ Prüfsumme 1
Fehler an der Stelle 3:	Prüfsumme 2	$\equiv$	$8 \cdot$ Prüfsumme 1
Fehler an der Stelle 4:	Prüfsumme 2	$\equiv$	$6 \cdot$ Prüfsumme 1
Fehler an der Stelle 5:	Prüfsumme 2	$\equiv$	$4 \cdot$ Prüfsumme 1
Fehler an der Stelle 6:	Prüfsumme 2	$\equiv$	$2 \cdot$ Prüfsumme 1
Fehler an der Stelle 7:	Prüfsumme 2	$\equiv$	$1 \cdot$ Prüfsumme 1

  Beachten werden muss dabei, dass wir modulo 13 rechnen, und modulo 13 gilt

  $$12 = 2 \cdot 6 \mod 13$$

  (da 13 eine Primzahl ist, gilt damit automatisch, dass nicht noch ein anderes Verhältnis erfüllt sein kann, da alle möglichen Faktoren teilerfremd zu 13 sind). Das zeigt, dass wir einen Fehler an der Stelle 6 haben (und die anderen 6 Stellen korrekt sind). Setzen wir x für a_6, so ergibt sich aus der ersten Prüfsumme, dass

  $$10 + 9 + 7 + 9 + 4 + x + 11 = 50 + x$$

  durch 13 teilbar sein muss. Daraus folgt, dass $a_6 = x = 2$ sein muss. Damit ergibt sich die korrekte Zahlenfolge

  $$c = (10,\ 9,\ 7,\ 9,\ 4,\ 2,\ 11))$$

  bzw. nach Weglassen der beiden Prüfzahlen die Nachricht

  $$m = (10,\ 9,\ 7,\ 9,\ 4)$$

Aufgabe 4. Wir betrachten einen $[n,k]_2$–Code, dh. einen Code der Länge n und der logarithmischen Kardinalität k über einem Alphabet $\mathbb{A}$ mit 2 Elementen (also z.B. $\mathbb{A} = \{0,1\}$). Für ein Element $c \in C$ bezeichnen wir mit $B(c)$ die Menge aller Elemente von $\mathbb{A}^n$, die sich von c höchstens an einer Position (oder gar keiner) unterscheiden.

a) Zeigen Sie, dass $B(c)$ genau $n+1$ Elemente hat.

Lösung:

Wir schreiben $c = (c_1, \ldots, c_n)$. Ist dann $d = (d_1, \ldots, d_n) \in B(c)$, so gilt eine von den beiden folgenden Varianten

1. $c = d$ (liefert ein Element von $B(c)$)
2. d unterscheidet sich von c an genau einer Stelle. Dafür gibt es genau n Positionen, an denen sich d von c unterscheidet. Unterscheidet sich d von c an einer Stelle i, so gibt es für d dann aber nur noch eine Möglichkeit. Da das Alphabet nur 2 Element hat, muss bei d an der Stelle i genau das Element von $\mathbb{A}$ stehen, dass nicht c_i ist (an den anderen Stellen stimmt d sowieso mit c überein). Damit gibt es hier für d genau n Möglichkeiten

Insgesamt erhalten wir also, dass $B(c)$ genau $n+1$ Elemente hat.

b) Zeigen Sie: Hat C den Minimalabstand $d \geq 3$ und sind c, c' zwei Elemente aus C mit $c \neq c'$, so gilt

$$B(c) \cap B(c') = \emptyset$$

Lösung:

Ist $d = (d_1, \ldots, d_n)$ eine Element von $B(c)$, so unterscheidet es sich von c höchstens an einer Stelle.

Falls $d = c$, so ist d sicherlich nicht in $B(c')$, denn c und c' unterscheiden sich mindestens an drei Stellen.

Wir können also annehmen, dass sich d von c genau an einer Stelle, etwa der Stelle i, unterscheiden. Wäre d zusätzlich noch in $B(c')$, so würde sich d auch von c' an höchstens einer Stelle unterscheiden, also entweder an keiner oder an einer Stelle j. Damit könnte sich aber dann c' von c nur noch an höchstens 2 Stellen unterscheiden (nämlich an denen, an denen sich d von c bzw. d von c' unterscheidet, also i bzw. i und j), ein Widerspruch zur Voraussetzung.

Daher gibt es kein $d \in B(c) \cap B(c')$, also $B(c) \cap B(c') = \emptyset$.

Etwas formaler können wir auch wie folgt argumentieren:

Für zwei Elemente $a, b \in \mathbb{A}^n$ betrachten wir

$$\Delta(a,b) = \{i \in \{1,\ldots,n\} \mid a_i \neq b_i\}$$

also die Menge der Indizes, an denen a und b verschieden sind. Dann gilt offensichtlich

$$d(a,b) = |\Delta(a,b)|$$

Außerdem gilt für drei Elemente a, b, c:

$$\Delta(a,c) \subseteq \Delta(a,b) \cup \Delta(b,c)$$

(hier muss nicht Gleichheit herrschen, denn eine Änderung von a nach b kann von b nach c wieder rückgängig gemacht werden). Damit gilt

$$d(a,c) = |\Delta(a,c)| \leq |\Delta(a,b) \cup \Delta(b,c)| \leq |\Delta(a,b)| + |\Delta(b,c)| = d(a,b) + d(a,c)$$

Wenden wir das auf $d \in B(c) \cap B(c')$ an, so erhalten wir

$$3 \leq d(c,c') \leq (d(c,d) + d(d,c') \leq 1 + 1 = 2$$

ein Widerspruch. Also ist $B(c) \cap B(c') = \emptyset$.

c) Zeigen Sie, dass es keinen $[5,3]_2$–Code C gibt, der Minimalabstand $d = d(C) = 3$ hat.

Hinweis: Nehmen Sie an, dass es so einen Code gibt und benutzen Sie Teil b) und c), um diese Annnahme zum Widerspruch zu führen.

Lösung:

Wir nehmen an, dass es einen $[5,3]_2$–Code C gibt, der Minimalabstand $d = d(C) = 3$ hat. Dann hat dieser Code $m = 2^3 = 8$ Element, ist also eine achtelementige Teilmenge von $\{0,1\}^5$, wobei $\{0,1\}^5$ selbst genau $2^5 = 32$ Elemente hat.

Zu jedem $c \in C$ betrachten wir nun $B(c) \subseteq \{0,1\}^5$. Nach Teil a) hat jedes dieser $B(c)$ genau $5 + 1 = 6$ Elemente, und nach Teil b) schneiden sich die $B(c)$ für unterschiedliche $c \in C$ nicht. Damit hat aber die Menge

$$M = \bigcup_{c \in C} B(c)$$

genau $8 \cdot 6 = 48$ Elemente (denn für die Durchschnitte ist nichts abzuziehen).

Da aber $M \subseteq \{0,1\}^5$, kann M höchstens 32 Elemente haben, ein Widerspruch.

Also kann es keinen $[5,3]_2$–Code C geben, der Minimalabstand $d = d(C) = 3$ hat.