

Aufgabe 3 - Zara Zackigs Zurueckkehr

Teilnahme-ID: 60302

Bearbeitet von
Florian Bange

25. April 2022

Inhaltsverzeichnis

1	Definition des XORs	2
2	Darstellung durch \mathbb{Z}_2 mit der Addition	2
3	Eigenschaften des XORs	2
4	Bitfolgen	2
5	Definition und Reduzierung der Aufgabe	3
6	Komplexitaet	4
7	Algorithmus 1: Loesung durch Bruteforce der Kombinationen	5
7.1	Laufzeit	7
8	Loesung durch ein Gleichungssystem	8
9	Loesung des Gleichungssystems mit bestimmtem Hamming-Gewicht	9
10	Algorithmus 2: Loesung durch Gausz-Verfahren und Bruteforce	9
10.1	Loesen des Gleichungssystems ueber \mathbb{Z}_2	9
10.2	Loesen der letzten Gleichung durch Bruteforce	10
10.3	Laufzeit	10
11	Implementierung	11
12	Aufgabenteil c - Beispiele	11
12.1	stapel0	11
12.2	stapel1	11
12.3	stapel2	12
12.4	stapel5	12
13	Aufgabenteil b	13
14	Quellcode	13
14.1	Erstellen der Matrix	13
14.2	Algorithmus 1	13
14.3	Algorithmus 2	13
15	Literatur	14

1 Definition des XORs

XOR bzw. \oplus sei zunaechst auf zwei Bits/Wahrheitswerte, wie folgt ueber die Gleichheit, definiert:

Sein a, b zwei Wahrheitswerte.

$$a \text{ XOR } b \iff a \oplus b = \neg(a \iff b)$$

Die dazugehoerige Wahrheitstabelle sieht wie folgt aus:

a	b	$a \iff b$	$\neg(a \iff b)$	a XOR b
0	0	1	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	0	0

Bzw. sieht die Verknuepfungstabelle des XORs so aus:

\oplus	0	1
0	0	1
1	1	0

2 Darstellung durch \mathbb{Z}_2 mit der Addition

Die Menge $\mathbb{Z}_2 = \{0, 1\}$ bildet zusammen mit der Addition eine abelsche Gruppe.

Die dazugehoerige Verknuepfungstabelle sieht wie folgt aus:

$+$	0	1
0	0	1
1	1	0

Wie zu erkennen ist, ist diese Verknuepfungstabelle identisch zu der des XORs.

Somit kann die Verknuepfung XOR mit der Addition in \mathbb{Z}_2 dargestellt werden.

3 Eigenschaften des XORs

Aufgrund dessen, dass das XOR mit der abelschen Gruppe $(\mathbb{Z}_2, +)$ dargestellt werden kann, gelten fuer das XOR die gleichen Eigenschaften, wie fuer die abelsche Gruppe $(\mathbb{Z}_2, +)$:

Seien a, b, c beliebige Wahrheitswerte (0, oder 1), bzw. $a, b, c \in \mathbb{Z}_2$.

1. Assoziativitaet: $(a \oplus b) \oplus c = a \oplus (b \oplus c)$
2. Neutrales Element 0: $a \oplus 0 = a$
3. Selbstinvers: $a \oplus a = 0$
4. Kommutativitaet: $a \oplus b = b \oplus a$

4 Bitfolgen

Bitfolgen bestehen aus mehreren aneinandergereihten Bits.

Eine Bitfolge b aus m Bits besteht aus den Bits b_1, \dots, b_m und laesst sich entweder darstellen als aneinandergereihte Bits:

$$b_1 \dots b_m$$

Oder als Vektor:

$$b = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

Die Bitfolge 0 - die Null-Bitfolge - sei definiert als der Null-Vektor.

Sprich

$$0 = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

Die jeweilige Laenge ergibt sich, wie beim Null-Vektor aus dem Zusammenhang.

Wird das XOR auf mehrere Bitfolgen angewendet, wird auf die Bits aller Bitfolgen an Stelle i nacheinander das XOR angewendet. Dies wird fuer alle Stellen i der Bitfolgen durchgefuehrt. Das jeweilige Ergebnis wird in der resultierenden Bitfolge an Stelle i notiert. Dafuer muessen alle mit dem XOR verbundenen Bitfolgen die gleiche Laenge haben.

Am sinnvollsten ist dazu die Darstellung der Bitfolgen als Vektoren zusammen mit der Vektoraddition fuer Vektoren aus \mathbb{Z}_2^m . Dies sieht allgemein wie folgt aus:

Fuer n Bitfolgen b_1, \dots, b_n mit je m Bits, wobei

$$b_i = \begin{bmatrix} b_{i,1} \\ \vdots \\ b_{i,m} \end{bmatrix}$$

ist, ist die entstehende Bitfolge u mit

$$u = b_1 + \dots + b_n,$$

wobei $+$ hier die Vektoraddition (fuer Vektoren aus \mathbb{Z}_2^m) ist.

Alternativ lassen sich diese Schreibweisen waehlen:

$$\begin{bmatrix} u_1 \\ \vdots \\ u_m \end{bmatrix} = \begin{bmatrix} b_{1,1} \\ \vdots \\ b_{1,m} \end{bmatrix} + \dots + \begin{bmatrix} b_{n,1} \\ \vdots \\ b_{n,m} \end{bmatrix}$$

Oder auch

$$u_1 = b_{1,1} + \dots + b_{n,1}$$

$$\vdots$$

$$u_n = b_{1,m} + \dots + b_{n,m}$$

Beispiel:

Moechte man folgende Bitfolgen mit dem XOR verbinden, geht dies, wie anschliessend in der Tabelle gezeigt.

1001, 1100, 1101

\oplus	1	0	0	1
\oplus	1	1	0	0
\oplus	1	1	0	1
$=$	1	0	0	0

Die zuvor beschriebene Vorgehensweise sieht fuer das Beispiel wie folgt aus:

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Weiter sei angemerkt, dass fuer das XOR mit Bitfolgen die gleichen Eigenschaften gelten, wie bei einzelnen Bits, da das XOR fuer einzelne Bits elementweise angewendet wird.

Es gilt also ebenfalls die Assoziativitaet, das Neutralelement 0, die Eigenschaft des Selbstinversen und die Kommutativitaet.

5 Definition und Reduzierung der Aufgabe

Das Problem der Bonusaufgabe „Zara Zackigs Zurueckkehr“ (oder kurz das ZZZ-Problem) laesst sich wie folgt formal definieren:

Gegeben sind n Bitfolgen der Laenge m , und eine Ganzzahl $k > 0$.

Fuer die n Bitfolgen ist gesucht die Menge an k Bitfolgen $\{s_1, \dots, s_k\}$, fuer welche eine weitere Bitfolge x exestiert, mit

$$s_1 \oplus \dots \oplus s_k = x.$$

Existiert eine solche Loesung nicht, soll die leere Menge das Ergebnis sein.

Sei das Problem „Null-Bitfolge“ wie folgt definiert:

Gegeben sind n Bitfolgen der Laenge m und eine Ganzzahl $k > 0$.

Das Problem lautet, k der n gegebenen Bitfolgen zu finden, bei welchen gilt

$$s_1 \oplus \cdots \oplus s_k = 0,$$

Existiert eine solche Loesung nicht, soll die leere Menge das Ergebnis sein.

Das Null-Bitfolge Problem laesst sich auf das ZZZ-Problem reduzieren, indem man die n gegebenen Bitfolgen und $k - 1$ als Eingaben fuer das ZZZ-Problem benutzt. Dadurch erhaelt man k der n Bitfolgen fuer welche gilt

$$s_1 \oplus \cdots \oplus s_{k-1} = s_k.$$

Das Null-Bitfolge Problem ist durch das Ergebnis des ZZZ-Problems ebenfalls geloest, da man die Gleichung

$$s_1 \oplus \cdots \oplus s_{k-1} = s_k$$

wie folgt umstellen kann:

Fuegt man zu beiden Seiten $\oplus s_k$ hinzu, erhaelt man

$$(s_1 \oplus \cdots \oplus s_{k-1}) \oplus s_k = s_k \oplus s_k.$$

Durch die Eigenschaft des Selbstinversen erhaelt man

$$(s_1 \oplus \cdots \oplus s_{k-1}) \oplus s_k = 0,$$

Weiter erhaelt man mit der Assoziativitaet

$$s_1 \oplus \cdots \oplus s_{k-1} \oplus s_k = 0.$$

Somit hat man k Bitfolgen gefunden, welche die Null-Bitfolge ergeben.

Fuer den Fall, dass die leere Menge das Ergebnis des ZZZ-Problems ist, gibt es ebenfalls keine Loesung fuer das Null-Bitfolge Problem, so das die leere Menge ebenfalls das Ergebnis ist.

Dass sich das neue Problem auf das ZZZ-Problem reduzieren laesst bedeutet, dass wenn das Null-Bitfolge Problem NP-schwer ist, auch das ZZZ-Problem NP-schwer ist.

Weiter sei gesagt, dass man das ZZZ-Problem ebenfalls auf das Null-Bitfolge Problem reduzieren kann.

Dazu benutzt man die n gegebenen Bitfolgen und $k + 1$ als Eingaben fuer das Null-Bitfolge Problem. Dadurch erhaelt man

$$s_1 \oplus \cdots \oplus s_{k+1} = 0.$$

Anschliessend kann man irgendeine der $k + 1$ gefundenen Bitfolgen auf beiden Seiten addieren und erhaelt

$$s_1 \oplus \cdots \oplus s_k \oplus s_{k+1} \oplus s_{k+1} = 0 \oplus s_{k+1}$$

$$\Leftrightarrow s_1 \oplus \cdots \oplus s_k \oplus 0 = \oplus s_{k+1}$$

$$\Leftrightarrow s_1 \oplus \cdots \oplus s_k = \oplus s_{k+1}.$$

Dadurch hat man k Bitfolgen erhalten fuer welche eine weitere Bitfolge existiert, bei welcher die vorausgesetzte Bedingung gilt.

Fuer den Fall, dass die leere Menge das Ergebnis des Null-Bitfolge Problems ist, gibt es ebenfalls keine Loesung fuer das Null-Bitfolge Problem, so das die leere Menge ebenfalls das Ergebnis ist.

Dass wiederum bedeutet, dass man das ZZZ-Problem loesen kann, indem man das Null-Bitfolge Problem loest.

6 Komplexitaet

Das ZZZ-Problem ist NP-schwer.

Diese Aussage wird nun bewiesen, indem gezeigt wird, dass das Null-Bitfolge Problem NP-schwer ist. Dies ist moeglich, da das Null-Bitfolge Problem bereits auf das ZZZ-Problem reduziert wurde.

Um zu zeigen, dass ein Problem L NP-hard ist muss jedes Problem in NP durch eine Polynomialzeitreduktion auf L reduziert werden koennen.

Um dies zu zeigen, kann man ein als NP-vollstaendiges Problem auf L reduzieren. Das bedeutet, dass L mindestens so schwer ist, wie das Problem von welchem reduziert wird.

Das Problem von welchem reduziert wird, soll hier das „Weight Distribution“ [2] oder auch „Subspace Weights“ [1] genannte Problem sein, welches in [1] als NP-vollstaendig bewiesen wurde:

Gegeben sind eine binaere $m \times n$ Matrix A und eine Ganzzahl $k > 0$.

Die Entscheidungsfrage ist, ob es eine Menge an k Spalten aus A gibt, welche sich zum Null-Vektor aufaddieren.

Dieses Entscheidungsproblem laesst sich wie folgt durch Polynomialzeitreduktion zum ZZZ-Problem reduzieren:
Seien die Spalten der Matrix die Vektoren

$$\vec{v}_1, \dots, \vec{v}_n.$$

Diese Vektoren kann man als Bitfolgen interpretieren:

$$\vec{v}_i = \begin{bmatrix} v_{i,1} \\ \vdots \\ x_{i,m} \end{bmatrix}$$

wird zur Bitfolge

$$s_i = \vec{v}_i.$$

Somit erhaelt man die Bitfolgen

$$s_1, \dots, s_n.$$

Diese Bitfolgen und k kann man nun als Eingabe fuer das Null-Bitfolge Problem benutzen.

Dadurch erhaelt man k Bitfolgen, welche aufaddiert die Null-Bitfolge (bestehend aus m Nullen) ergeben oder die leere Menge.

Erhaelt man k Bitfolgen, so handelt es sich um eine Ja-Instanz, erhaelt man die leere Menge, handelt es sich um eine Nein-Instanz.

Dass es sich um eine Ja-Instanz handelt, wenn k Bitfolgen das Ergebnis des Null-Bitfolge Problem sind, liegt daran, dass jede der k Bitfolgen einer Spalte der Matrix entspricht. Somit gibt es k Spalten der Matrix, welche den Null-Vektor ergeben.

Dass es sich um eine Nein-Instanz handelt, wenn die leere Menge zurueckgegeben wurde, ergibt ebenfalls Sinn. Denn in dem Fall koennten keine k Bitfolgen, sprich keine k Spalten, gefunden werden, welche die Null-Bitfolge, bzw. den Null-Vektor, bilden.

Aufgrund dessen, dass das ZZZ-Problem NP-schwer ist, kann man davon ausgehen, dass kein Algorithmus existiert, welcher das Problem effizient loest, bzw. in Polynomialzeit laeuft.

Dennoch werden nun zwei Loesungsansaeetze vorgestellt, welche das Problem exakt, aber mit exponentieller Laufzeit loesen. Beide Loesungen werden das Null-Bitfolge Problem loesen, welches, wie bereits bewiesen, das ZZZ-Problem loest. Der erste Loesungsansatz basiert auf einem Bruteforceverfahren und der zweite auf dem Loesen eines linearen Gleichungssystems, welches in den Kapiteln „Loesung durch ein Gleichungssystem“ und „Loesung des Gleichungssystems mit bestimmtem Hamming-Gewicht“ erlaeutert wird.

7 Algorithmus 1: Loesung durch Bruteforce der Kombinationen

Das Null-Bitfolge Problem laesst sich loesen, indem alle moeglichen Kombinationen (ohne Wiederholung/Zuruecklegen) der Bitfolgen ausprobiert und ueberprueft werden.

Gegeben sind die n Bitfolgen der Laenge m :

$$b_1, \dots, b_n$$

Sowie die Anzahl an gesuchten Bitfolgen k .

Um bei diesem Loesungsweg effizient vorzugehen, werden nicht alle moeglichen Kombinationen erstellt, sondern alle Kombinationen von $\lfloor \frac{k}{2} \rfloor$ Bitfolgen (die abgerundete Haelfte von k , abgerundet auf die naechst kleinere Ganzzahl).

Sei

$$l = \lfloor \frac{k}{2} \rfloor.$$

Alle moeglichen Kombinationen der l Bitfolgen werden durchgegangen und das dazugehoerige XOR wird berechnet. Dadurch erhaelt man je ein Paar, bestehend aus den Indexen der gewaehlten Bitfolgen und der durch das XOR resultierenden Bitfolge:

$$(\{i_1, \dots, i_l\}, x),$$

wobei

$$x = b_{i_1} XOR \dots XOR b_{i_l}$$

ist.

Fuer jedes dieser Paare, welche durch die Kombinationen von l der n Bitfolgen entstehen, wird die Menge der Indexe in einer Liste gespeichert.

Dabei ist diese Liste ein Wert, assoziiert mit der Bitfolge.

Es entsteht also eine Tabelle, in welcher von Bitfolgen x zu Listen L_x gezeigt wird. Diese Listen (L_x) beinhalten stets alle Mengen (der Groesze l) an Indexen, dessen Bitfolgen x ergeben.

Der Pseudocode zu der Erstellung dieser Tabelle, welcher als Uebergabeparameter die Bitfolgen und l erhaelt, sieht wie folgt aus:

```

1: procedure CREATETABLE( $b_1 \dots, b_n, size$ )
2:    $table \leftarrow []$ 
3:    $firstCombination \leftarrow getFirstCombination(n, k)$ 
4:    $currentCombination \leftarrow firstCombination$ 
5:   while  $currentCombination \neq \emptyset$  do
6:      $x \leftarrow b_{currentCombination_1} XOR \dots XOR b_{currentCombination_{size}}$ 
7:      $L_x \leftarrow table[x]$ 
8:     if  $L_x = NULL$  then           ▷ After obtaining  $L_x$ , check if the list is empty. If so, create it and set it in table.
9:        $L_x \leftarrow []$ 
10:       $table[x] \leftarrow L_x$ 
11:    end if
12:     $L_x.append(currentCombination)$ 
13:     $currentCombination \leftarrow getNextCombination(currentCombination)$ 
14:  end while
15:  return  $table$ 
16: end procedure

```

In diesem Pseudocode sollen die Methoden `getFirstCombination` und `getNextCombination` je die erste Kombination und die naechste Kombination an Indexen der Bitfolgen zurueckgeben. Wenn die letzte Kombination erreicht ist, soll eine leere Menge zurueckgegeben werden.

Dies wird in der While-Schleife ueberprueft, so dass alle Kombinationen einmal gewaehlt sein werden.

Des Weiteren ist wichtig, dass `currentCombination` eine Liste darstellen soll, welche ueber den Index aufgerufen wird (so, wie die Bitfolgen).

Die Tabelle „table“ soll hier, wie beschrieben, zeigen von Bitfolgen auf Listen an Mengen. Werte der Tabelle werden dabei ueber eckige Klammern (in welchen der Wert steht) aufgerufen.

Mit Hilfe dieser Tabelle kann man nun alle moeglichen Kombinationen an k Bitfolgen darstellen.

Dazu muss man unterscheiden, ob k eine gerade oder ungerade Zahl ist.

Ist k eine gerade Zahl, so wurden Kombinationen mit $\frac{k}{2}$ Elementen erstellt und man kann durch alle entstandenen Bitfolgen x iterieren und fuer jede Liste L_x (welche man durch x erhaelt) Folgendes tun:

Man sucht in der Liste nach zwei Mengen, welche disjunkt sind (also kein gleiches Element enthalten).

Hat man zwei Mengen in L_x gefunden, welche disjunkt sind, so hat man ebenfalls k Bitfolgen (bzw. deren Indexe) gefunden, welche die Null-Bitfolge darstellen. Das liegt daran, dass beide Mengen mit der Bitfolge x assoziiert sind (bzw., die, zu den Indexen gehoerenden Bitfolge, diese ergeben). Hat man nun zwei disjunkte Mengen, dessen Bitfolgen je x ergeben, so erhaelt man k Indexe an Bitfolgen ($k = 2 * \frac{k}{2}$, weil k hier gerade ist) welche, wenn man sie durch das XOR verbindet, die Null-Bitfolge ergeben, denn das XOR ist selbstinvers.

Der Pseudocode fuer diesen Fall sieht wie folgt aus:

```

1: procedure EVENK( $table$ )
2:   for  $x \in table.values$  do
3:      $L_x \leftarrow table[x]$ 
4:     for  $indexesA \in L_x$  do
5:       for  $indexesB \in L_x$  do
6:         if disjoint(indexesA, indexesB) then
7:           return merge(indexesA, indexesB)
8:         end if
9:       end for
10:    end for
11:  end for
12:  return  $NULL$ 
13: end procedure

```

Ist k ungrade, so wurden Kombinationen mit $\frac{k-1}{2}$ Elementen erstellt, so dass man, wuerde man die vorherige Vorgehensweise anwenden, nur $\frac{k-1}{2} * 2 = k - 1$ Bitfolgen erhalten, welche die Null-Bitfolge ergeben.

Somit muss eine zusaetzliche Bitfolge eingefuehrt werden. Die Vorgehensweise fuer ein ungrades k ist diese:

Man iteriert fuer jede der n Bitfolgen b_i durch alle entstandenen x der Kombinationen und wendet das XOR auf b_i und x an. Dadurch entsteht eine weitere Bitfolge $z = b_i XOR x$.

Fuer diese neue Bitfolge ueberprueft man, ob sie in der Tabelle enthalten ist. Ist dies der Fall, so wird versucht, zwei

Mengen aus L_x und L_z zu finden (eine aus L_x und eine aus L_z), fuer welche gilt, dass sie disjunkt sind und je nicht i enthalten.

Hat man solche zwei Mengen gefunden, so hat man $k = 1 + \frac{k-1}{2} * 2$ Bitfolgen gefunden, welche

$$0 = (b_i \text{ XOR } x) \text{ XOR } z = (b_i \text{ XOR } x) \text{ XOR } (b_i \text{ XOR } x)$$

ergeben, wobei 0 fuer die Null-Bitfolge steht.

Der Pseudocode fuer diesen Fall sieht wie folgt aus:

```

1: procedure ODDK( $b_1 \dots, n, table$ )
2:   for  $i \leftarrow 1$  to  $n$  do
3:     for  $x \in table.values$  do
4:        $z \leftarrow b_i \text{ XOR } x$ 
5:        $L_x \leftarrow table[x]$ 
6:        $L_z \leftarrow table[z]$ 
7:       if  $L_z \neq NULL$  then
8:         for  $indexesA \in L_x$  do
9:           for  $indexesB \in L_z$  do
10:            if  $disjoint(indexesA, indexesB, \{i\})$  then
11:              return  $merge(indexesA, indexesB, \{i\})$ 
12:            end if
13:          end for
14:        end for
15:      end if
16:    end for
17:  end for
18:  return  $NULL$ 
19: end procedure

```

In den beiden Pseudocodes sollen die Methoden `disjoint` ueberpruefen, ob Mengen disjunkt sind und die Methoden `merge` sollen Mengen verbinden (also vereinigen).

Weiter soll `table.values` die Werte (bzw. Schluessel) der Tabelle darstellen.

7.1 Laufzeit

Die (worst case) Laufzeit fuer diesen Algorithmus ist ...

1. fuer k grade

$$\begin{aligned}
 & \mathcal{O}\left(\binom{n}{\frac{k}{2}} * c^2 * k\right) \\
 &= \mathcal{O}\left(\binom{n}{\frac{k}{2}}\right) \\
 &= \mathcal{O}(n^{\frac{k}{2}})
 \end{aligned}$$

2. fuer k ungrade

$$\begin{aligned}
 & \mathcal{O}\left(\binom{n}{\frac{k-1}{2}} * n * c^2 * k\right) \\
 &= \mathcal{O}\left(\binom{n}{\frac{k-1}{2}} * n\right) \\
 &= \mathcal{O}(n^{\frac{k-1}{2} + 1}) \\
 &= \mathcal{O}(n^{\frac{k+1}{2}})
 \end{aligned}$$

Dabei ist c die durchschnittliche GroeÙe der Listen L_x .

Die Laufzeit setzt sich also je zusammen, aus der Anzahl an Kombinationen und dem Durchlaufen der Listen, um die disjunkten Mengen zu finden. Je Ueberpruefung der Mengen, braucht es k Durchgaenge, um zu ueberpruefen, ob die Mengen disjunkt sind.

Der Faktor $c^2 * k$ wird hier ignoriert, da der Binomialkoeffizient deutlich schneller waechst als der Faktor.

Des Weiteren kann der Binomialkoeffizient zu einem exponentiellen Ausdruck umgeformt werden, da folgende Umformung durchgefuehrt werden kann:

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

$$\begin{aligned}
&= \frac{n * (n-1) * \dots * (n-k+1)}{k!} \\
&= \frac{1}{k!} * (n * (n-1) * \dots * (n-k+1)) \\
&< \frac{1}{k!} * n^k \\
&< n^k
\end{aligned}$$

Der Algorithmus hat also eine exponentielle Laufzeit und kann somit nur auf kleine n und k angewendet werden. Doch fuer solche Werte bietet er eine exakte Loesung.

8 Loesung durch ein Gleichungssystem

Fuer das zuvor beschriebene Null-Bitfolge Problem werden nun n Entscheidungsvariablen eingefuehrt: x_1, \dots, x_n . Diese koennen entweder 0 oder 1 annehmen. Ist die Entscheidungsvariable x_i mit $1 \leq i \leq n$ 1, so ist die i -te Bitfolge Teil der Loesung, andernfalls nicht.

Fuer eine gueltige Loesung muss folgendes Gleichungssystem mit m Gleichungen ueber \mathbb{Z}_2 geloest werden:

$$\begin{aligned}
a_{1,1} * x_1 + \dots + a_{n,1} * x_n &= 0 \\
&\dots \\
a_{1,m} * x_1 + \dots + a_{n,m} * x_n &= 0
\end{aligned}$$

Dabei stellen

$$a_{i,1}, \dots, a_{i,m}$$

die m Bits der i -ten Bitfolge dar.

Die Bits der gegebenen Bitfolgen werden also vertikal untereinander geschrieben und die Bitfolgen horizontal nebeneinander. Dabei erhaelt jede Spalte, also jede Bitfolge, eine Entscheidungsvariable.

Wodurch m (Anzahl der Bits) Reihen und n (Anzahl an Bitfolgen) Spalten entstehen.

Weiter muss

$$x_1 + \dots + x_n = k$$

in \mathbb{Z} (nicht in \mathbb{Z}_2 !) gelten.

Dadurch ist gegeben, dass exakt die benoetigte Anzahl an k Bitfolgen gewaehlt wird.

Dass eine Loesung fuer die zuvor beschriebenen Gleichungen ebenfalls eine Loesung fuer das Null-Bitfolge Problem ist, ist einfach zu zeigen:

Sein ohne Einschraenkung der Allgemeinheit x_1, \dots, x_k die k Entscheidungsvariablen, welche 1 annehmen und die Gleichungen erfuellen.

Nun lassen sich die zuvor beschriebenen Gleichungen je auf k Summanden reduzieren, welche zusammen 0 in \mathbb{Z}_2 ergeben. Diese Gleichungen sehen nun wie folgt aus:

$$\begin{aligned}
a_{1,1} + \dots + a_{k,1} &= 0 \\
&\dots \\
a_{1,m} + \dots + a_{k,m} &= 0
\end{aligned}$$

Jede Gleichung ist (wie in Kapitel 2 beschrieben) equivalent zum XOR angewandt auf mehrere Bits:

$$\begin{aligned}
a_{1,1} \oplus \dots \oplus a_{k,1} &= 0 \\
&\dots \\
a_{1,m} \oplus \dots \oplus a_{k,m} &= 0
\end{aligned}$$

Wie in Kapitel 4 beschrieben wurde ist dies wiederum gleichwertig zum XOR auf Bitfolgen. Hier bei den Bitfolgen 1 bis k , welche zusammen die Null-Bitfolge ergeben.

Somit wurden k Bitfolgen gefunden, welche, verknuepft durch das XOR, die Null-Bitfolge ergeben.

9 Loesung des Gleichungssystems mit bestimmtem Hamming-Gewicht

Nun ist die Aufgabe folgende Gleichungen ueber \mathbb{Z}_2 :

$$a_{1,1} * x_1 + \dots + a_{n,1} * x_n = 0$$

\dots

$$a_{1,m} * x_1 + \dots + a_{n,m} * x_n = 0$$

zu loesen.

Dieses Gleichungssystem ist aequivalent zu diesem:

$$A * \vec{x} = \vec{0}$$

mit

$$A = \begin{bmatrix} a_{1,1} & \dots & a_{n,1} \\ \vdots & & \vdots \\ a_{1,m} & \dots & a_{n,m} \end{bmatrix}$$

und

$$\vec{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Weiter muss die Gleichung

$$x_1 + \dots + x_n = k$$

ueber \mathbb{Z} gelten.

Die letzte Beschraenkung ($x_1 + \dots + x_n = k$) bedeutet, dass die Loesung \vec{x} des ersten Gleichungssystems genau k Einsen beinhalten muss.

Da in \mathbb{Z}_2 Eins das einzige Element ungleich Null ist, ist die Beschraenkung aequivalent dazu, dass

$$wt(\vec{x}) = k$$

sein muss.

Wobei $wt(\vec{u})$ das Hamming-Gewicht von \vec{u} ist, welches definiert ist als die Anzahl an Elementen eines Vektors, welche nicht 0 sind, bzw.

$$wt(\vec{u}) = |\{i \in \{1, \dots, n\} : e_i \neq 0\}|$$

fuer einen Vektor \vec{u} mit den Elementen e_1, \dots, e_n .

Es gilt also eine Loesung \vec{x} des linearen Gleichungssystems

$$A * \vec{x} = \vec{0}$$

zu finden mit

$$wt(\vec{x}) = k,$$

wobei das Gleichungssystem ueber \mathbb{Z}_2 ist.

10 Algorithmus 2: Loesung durch Gausz-Verfahren und Bruteforce

In diesem Kapitel wird das zuvor beschriebene Problem angegangen, indem zunaechst das Gleichungssystem in \mathbb{Z}_2 geloest und anschliessend nach einer Loesung der Loesungsmenge gesucht wird, welche die Bedingung des Hamming-Gewichts erfuehlt.

10.1 Loesen des Gleichungssystems ueber \mathbb{Z}_2

Die zu loesenden Gleichungen lassen sich wie folgt mit Matrix und Vektoren darstellen:

$$A * \vec{x} = \vec{0}$$

Es ist also das homogene System zu A ueber \mathbb{Z}_2 zu loesen.

Aufgrund dessen, dass \mathbb{Z}_2 ein Koerper ist, laesst sich zum Loesen des Gleichungssystems ueber \mathbb{Z}_2 das Gausz-Verfahren

verwenden.

Dadurch erhaelt man eine Loesungsmenge, welche wie folgt aussieht:

$$\left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \vec{v}_1 * x_1 + \cdots + \vec{v}_n * x_n \right\}$$

Falls x_i mit $1 \leq i \leq n$ keine freie Variable ist, ist $\vec{v}_i = \vec{0}$.

10.2 Loesen der letzten Gleichung durch Bruteforce

Zuletzt ist die Loesung der Loesungsmenge zu finden, welche ein Hamming-Gewicht von k hat.

Dazu kann man bei Loesungsmengen mit kleiner Anzahl an freien Variablen alle moeglichen Kombinationen (ohne Wiederholung/Zuruecklegen) ausprobieren.

Dabei sollte man beachten, dass man niemals mehr als k Variablen auswaehlen darf, da bei jedem Vektor, welcher gewaehlt wird mindestens eine Variable aktiviert wird, welche nicht durch einen anderen Vektor wieder deaktiviert werden kann. Diese Variablen sind die freien Variablen.

Wichtig ist dabei, dass man fuer jede Anzahl i mit $1 \leq i \leq \min(k, f(A))$ an ausgewaehlten freien Variablen alle Kombinationen (ohne Wiederholung/Zuruecklegen) probiert. Wobei $f(A)$ die Anzahl an freien Variablen der Loesungsmenge des homogenen Gleichungssystems zu A darstellt.

Sei

$$r = \min(k, f(A)),$$

so muss man durch dieses Verfahren

$$\binom{f(A)}{1} + \cdots + \binom{f(A)}{r}$$

moegliche Belegungen ausprobieren. Denn der untere Wert des Binomialkoeffizienten darf nicht groeszer als der obere Wert sein, weil man (in diesem Fall) nicht mehr freie Variablen auswaehlen kann, als da sind.

Fuer jede Belegung u der freien Variablen kann man nun den resultierenden Vektor \vec{u} berechnen, indem alle durch u ausgewaehlten Vektoren der Loesungsmenge addiert werden. Nun muss nun ueberprueft werden, ob

$$wt(\vec{u}) = k$$

gilt.

Ist dieser Vektor gefunden, so hat man stets eine Loesung des homogenen Systems mit k benutzen Spalten/Vektoren.

10.3 Laufzeit

Dieses Verfahren hat eine Laufzeit von

$$\mathcal{O}(p(A)) + \mathcal{O}\left(\binom{f(A)}{1} * 1 * n\right) + \cdots + \mathcal{O}\left(\binom{f(A)}{r} * r * n\right).$$

Dabei stellt p ein Polynom dar, welches fuer das Gausz-Verfahren benoetigt wird.

$\binom{f(A)}{1} + \cdots + \binom{f(A)}{r}$ ist erneut die Anzahl an moeglichen Kombinationen. Fuer jede dieser Kombinationen aus q ($1 \leq q \leq r$) muessen maximal q Vektoren der Loesungsmenge addiert werden, um zu ueberpruefen, ob die Kombination eine gueltige Loesung darstellt. Dadurch entsteht eine Laufzeit von maximal $\mathcal{O}(q * n)$ pro Ueberpruefung einer Kombination. Denn die Vektoren haben die Laenge n .

Aufgrund dessen, dass $\mathcal{O}\left(\binom{n}{k}\right)$ sich, wie zuvor erlaeutert, zu $\mathcal{O}(n^k)$ umformen laesst, ergibt sich

$$\mathcal{O}(p(A)) + \mathcal{O}(f(A)^1 * 1 * n) + \cdots + \mathcal{O}(f(A)^r * r * n).$$

Da der letzte Summand deutlich schneller waechst als die ersten, ist die Laufzeit

$$\mathcal{O}(f(A)^r * r * n).$$

Da $r * n$ hier ein pseudopolynomieller Faktor der exponentiellen Laufzeit ist, kann er ebenfalls ignoriert werden, so dass die finale Laufzeit

$$\mathcal{O}(f(A)^r)$$

ist.

Dieser Loesungsweg hat also ebenbenfalls eine exponentielle Laufzeit und laesst sich nur anwenden, wenn die Loesungsmenge des homogenen System der Matrix klein genug ist, bezueglich der Anzahl an freien Variablen.

Dies laesst sich aber durch das Gausz-Verfahren schnell herausfinden.

Ist die Loesungsmenge allerdings klein genug, so kann eine exakte Loesung berechnet werden.

11 Implementierung

Das Program wurde in Java 8 und objektorientiert geschrieben.

Dazu gibt es eine Klasse „BitSequence“, welche eine Bitfolge darstellt. Sie speichert ein Array an booleans, welches die Bits darstellt und dessen Laenge als Attribute. Des Weiteren besitzt sie zwei Konstruktoren, welche (1) ein boolean Array und (2) einen String als Uebergabeparamether bekommen. Bei dem Konstruktor, welcher einen String erhaelt, soll dieser String ein binaerer String sein, welcher in ein boolean Array umgewandelt wird. Die BitSequence Klasse hat des Weiteren die Methoden „xor“, „getBit“ und „getSize“, welche je das XOR mit einer weiteren Bitfolge der selben Laenge erzeugen, einen Bit an einem bestimmten Index im boolean Array zurueckgeben und die Laenge der Bitsequence zurueckgeben. Auszerdem implementiert die Klasse das Comparable Interface, wodurch sie vergleichbar ist und sie ueberschreibt die equals und hashCode Methoden, durch Methoden, welche je den Inhalt der Objekte vergleichen und einen hashCode, basierend auf den Bits der Bitfolge, zurueckgeben.

Das ZZZ-Problem wird ebenfalls durch eine Klasse dargestellt, welche die Werte n , k und m , sowie eine Liste der gegebenen Bitfolgen als Attribute besitzt. Diese Klasse („ZZZProblem“) besitzt ebenfalls eine Methode zum Erstellen einer Matrix, wie sie in Kapitel „Loesung des Gleichungssystems mit bestimmtem Hamming-Gewicht“ beschrieben ist.

Fuer das Loesen des homogenen Systems einer Matrix, sowie fuer die Klassen, welche Matrizes und Vektoren darstellen wurde die JLinAlg Java-Bibliothek benutzt. Beim Loesen eines homogenen Systems erzeugt die Java-Bibliothek dabei ein Array aus Vektoren aus \mathbb{Z}_2^n (Vector<F2>[]) Des Weiteren ermoeoglicht sie, dass Rechnen (auch mit Vektoren und Matrix) im Koerper \mathbb{Z}_2 .

Eine weitere Wichtigkeit der Umsetzung ist, dass das Programm zwischen den Algorithmen abwaeagt, oder keinen waehlt, je nach der Eingabe.

Denn ist die Eingabe zu grosz, wird das Programm aufgrund der exponentiellen Laufzeit zu lange brauchen.

Genauer wird zunaechst die Matrix passend zur Eingabe erstellt. Ist die Anzahl an freien Variablen kleiner als 4, so wird der zweite Algorithmus verwendet. Andernfalls wird ueberprueft, ob $k \leq 4$ ist. In dem Fall wird Algorithmus 1 benutzt. In jedem anderen Fall ist das Programm nicht im Stande, die Loesung zu berechnen.

12 Aufgabenteil c - Beispiele

Nun folgen die Loesungen des Programms fuer die Eingaben der bwinf website.

In folgender Tabelle ist dargestellt, welcher Algorithmus welche Eingabe loesen kann:

Eingabe	Algorithmus 1	Algorithmus 2
stapel0	Ja	Ja
stapel1	Ja	Ja
stapel2	Nein	Ja
stapel3	Nein	Nein
stapel4	Nein	Nein
stapel5	Ja	Nein

In den folgenen Subsektionen sind die Ergebnisse angegeben. Fuer jede Eingabe sind die Indexe und die wirklichen Bitfolgen aufgelistet. Zusaetzlich ist die benoetigte Zeit in Millisekunden angegeben.

12.1 stapel0

Zeit: 21ms

Indexe: [2, 3, 5, 9, 11]

Bitfolgen:

```
00111101010111000110100110011001
11111110001011010001000000110111
11010111111010111101101111110000
10101100111111011010100011100000
10111000011001110000101010111110
```

12.2 stapel1

Zeit: 2ms

Indexe: [1, 2, 4, 6, 7, 9, 11, 14, 15]

Bitfolgen:

```
00100000111100111110111101111100
```

```

11010011010110110101001101010111
00110100001010100100001111010010
11110011101011001001000010111110
0011011000011010110101111111010
11110111100100010100100001001110
00100011100111011010111011100011
1100011111010110100000101110100
00010001110100110001111101100100

```

12.3 stapel2

Zeit: 32ms

Indexe: [9, 20, 26, 53, 57, 71, 76, 78, 89, 95, 99]

Bitfolgen:

```

011010111010001101110100011000001100000110001101011000101110111001100110111
10111011100110101101111000011110111011101011111100111,

```

```

001010111110001010110101101111001001100000000000110100110011110110010110010
00010001101010110110010101110100100001011100011010001,

```

```

10101011000001101100000101111111100110001100111001010110111110110001111111
0111110100011111101000000101101101111111010011011110,

```

```

100000000001001001100110010001100000000001010101101001001000010001110101101
10101010010101000101110101100101000110010100100111011,

```

```

001010000110000100101110111010110110101110001001001101011110110111101111001
01100001001110010100001101001110001000100010011111100,

```

```

110000110001001101110001011001001011010101100110110101011010010000111101000
10001001010000110010101010010001100010001101110100000,

```

```

101011111100100100101001111011000100111110000101010011001000011110001000100
10010011010010101011111101011000001111110000000111011,

```

```

11011110000101001101111100110000111010011011101111010111101101110110100
01001101101100111010001000011000001010111100101111111,

```

```

011010010010110001010011111111010110000010001011001110101001010110110001000
00001100001100011010110101011110110100000100101001011,

```

```

0111011001111000111001111000110111101001010000001000001011000010100011101
01000000011010011000011010010110110100101111101101000,

```

```

111011101010111001111011110001110011011110110101010111110001101000110100011
00000111101000010001100100000011101100010001011101000

```

12.4 stapel5

Zeit: 591ms

Indexe: [77, 185, 163, 167, 70]

Bitfolgen:

```

1101010001001101000111111110000110100010100111000100001001011011
1010000110101100101110111001100011011110111111010111000101111110
1010111011001100100110001100110001011101001000000011011111100100
0101111111000111000000101111100010111010110101000100000011001000
1000010011101010001111100100110110011011100101010100010000001001

```

13 Aufgabenteil b

In Aufgabenteil b ist gefragt, wie man mithilfe der 11 gefundenen Karten am naechsten Wochenende das naechste Haus aufsperrern kann, ohne dafuer mehr als zwei Fehlversuche zu benoetigen.

Diese Aufgabenstellung wird nun mit dem allgemeineren Problem angegangen, dass es n Haeuser gibt, so dass $n + 1$ Karten gefunden werden.

Sein zunaechst die Folge

$$W = (w_1, \dots, w_n)$$

die Karten der in der Aufgabenstellung erwaehten (aufsteigend sortierten) Codeworte und x die Sicherungskarte.

Weiter seien die gefundenen Karten

$$K = (k_1, \dots, k_{n+1}).$$

Nun seien die Karten

$$S = (s_1, \dots, s_{n+1})$$

K aufsteigend sortiert.

W , K und S sollen hier Folgen sein.

Da davon ausgegangen wird, dass die $n + 1$ richtigen Karten gefunden wurden, besteht S aus W und x .

Wichtig ist dabei, dass W innerhalb von S immer noch dieselbe Reihenfolge hat, da die Karten in beiden Folgen aufsteigend sortiert sind.

Somit wurde ausschliesslich die zusaetzliche Karte x in die Folge W hinzugefuegt, wodurch S entsteht.

Sei der Index, an welchem x zu W hinzugefuegt wurde, j , wobei $1 \leq j \leq n + 1$ gilt, so dass x innerhalb der Folge oder rechts an die Folge hinzugefuegt wird.

Dadurch verschieben sich alle Karten mit einem Index $i \geq j$ um eins nach rechts, so dass eine Karte w_i nun an Index $i + 1$ ist (so fern $i \geq j$). Die restlichen Karten (mit $i < j$) bleiben an ihrer Position.

Die Folge saehe dann wie folgt aus:

$$(w_1, \dots, w_{j-1}, x, w_j, \dots, w_n)$$

In dieser Folge ist zu erkennen, dass x am Index j liegt. Rechts von q sind die Elemente e_j, \dots, e_n , welche nun alle eine Position nach rechts gesetzt wurden (der Index in der Folge hat sich je um 1 erhoeht). Somit hat die Liste nun eine Laenge von $n + 1$.

Dementsprechend gibt es fuer jeden Index i eines Codewortes w_i ($1 \leq j \leq n$) zwei Moeglichkeiten, entweder w_i ist in S an Position i oder an Position $i + 1$. Je nachdem, ob $i < j$ bzw. $i \geq j$ ist.

Das bedeutet, dass man fuer das Haus k ebenfalls zwei Moeglichkeiten fuer das Codewort hat, entweder s_k oder s_{k+1} .

Zusammengefasst muss man also die $n + 1$ gefundenen Karten sortieren und kann anschliessend das Haus k mit dem Schluessel an Index k und $k + 1$ der sortierten Karten suchen. Dies haelt die Bedingung ein, dass maximal 3 Versuche benoetigt werden duerfen.

Auf die gegebene Aufgabe laesst sich dieses Verfahren einfach uebertragen, indem die 11 gefundenen Karten sortiert werden und fuer jedes Haus k ebenfalls die Karten k und $k + 1$ probiert werden.

14 Quellcode

Nun folgt der Quellcode der wichtigsten Teile des Programs.

14.1 Erstellen der Matrix

Diese Methode ist Teil der „ZZZProblem“ Klasse und erstellt aus dem gegebenen ZZZ-Problem eine Matrix, wie sie in Kapitel „Loesung des Gleichungssystems mit bestimmtem Hamming-Gewicht“ beschrieben ist.

14.2 Algorithmus 1

Die folgenden Methoden sind Teil der Klasse, welche den Algorithmus 1 implementiert.

14.3 Algorithmus 2

Loesen des homogenen Systems

Diese Methode loest das homogene System einer Matrix mit Hilfe der JLinAlg Java-Bibliothek und loest somit den ersten Teil des zweiten Algorithmus.

Bruteforcing der richtigen Loesung der Loesungsmenge

Diese Methoden loesen den zweiten Teil des zweiten Algorithmus, indem sie die Loesung mit dem Hamming-Gewicht „weight“ in einer gegebenen Loesungsmenge suchen.

Diese Loesungsmenge ist gegeben als ein Array aus Vektoren aus \mathbb{Z}_2^n (Vector<F2>[]).

15 Literatur

1. Elwyn R. Berlekamp, Robert J. McEliece and Henk C.A. van Tilborg, On the inherent intractability of certain coding problems, 1978
2. Rod G. Downey, Michael R. Fellows, Alexander Vardy and Geoff Whittle, The parametrized complexity of some fundamental problems in coding theory, 1999