Komplexität von Code-Problemen

Ausarbeitung im Seminar "Komplexität"
am FG Theoretische Informatik / Formale Methoden
der Universität Kassel

Ahmad Lowejatan Noori

Sommersemester 2024

Zusammenfassung

Codes als Menge von Bitstrings fester Länge sind von enormer Wichtigkeit in der Datenübertragung. Minimale sowie überdeckende Codes werden durch den Radius und den Covering Radius formalisiert, in der die Metrik der Hamming-Distanzen Relevanz hat. In der Ausarbeitung werden das Minimum-Radius-Problem (MR) und das Maximum-Covering-Radius-Problem (MCR) untersucht und sowohl die Äquivalenz als auch die NP-Vollständigkeit beider Probleme gezeigt.

1 Einführung

In der Datenübertragungs- und Nachrichtentechnik spielen Codes eine entscheidende Rolle, um Informationen sicher und effizient zu übertragen. Analoge Signale werden durch Abtastung, Quantisierung und Kodierung digitalisiert, wobei die Daten in Bitstrings (Codewörter) umgewandelt werden. Ein Code ist eine Menge von Codewörtern, und die Kodierung stellt sicher, dass die Daten in einer Form vorliegen, die für die Übertragung geeignet ist. Während der Übertragung können jedoch durch Rauschen, Interferenzen oder andere Störungen Fehler auftreten, die dazu führen, dass empfangene Codewörter von den gesendeten abweichen. Um solche Fehler zu behandeln, haben sich Fehlerkorrektur- und Fehlererkennungsverfahren bewährt. Die Effektivität dieser Verfahren hängt von der Form des Codes ab. Dabei besteht ein Kompromiss zwischen minimalen Codes. Minimale Codes beanspruchen weniger Speicherbedarf und verursachen eine geringere Übertragungslast. Überdeckende Codes hingegen fügen zusätzliche Bits hinzu, um eine zuverlässigere Fehlererkennung und -korrektur zu ermöglichen, was jedoch die Effizienz in der Übertragung verringert. Diese Charakteristika lassen sich über den *Radius* bzw. dem *Covering Radius* eines Codes konkretisieren, für die entsprechende Entscheidbarkeitsprobleme formalisiert werden, deren NP-Vollständigkeit in dieser Ausarbeitung bewiesen wird. Das bedeutet, dass keine effizienten Algorithmen für die Entscheidbarkeit dieser Probleme bekannt sind. Zunächst werden einige theoretische Grundlagen erläutert, auf welche die kommenden Lemmata zurückgreifen. In Abschnitt 3 werden Radius und Covering Radius sowie die dazugehörigen Entscheidungsprobleme

aufgestellt. Zusätzlich wird die Äquivalenz beider Probleme bezüglich Polynomialzeitreduktionen bewiesen, um in Abschnitt 4 über die NP-Vollständigkeit von MR auf die NP-Vollständigkeit von MCR zu schließen. Abschnitt 4 thematisiert insbesondere die NP-Schwere von MR. Abschnitt 5 bietet einen kleinen Ausblick über ein weiteres Anwendungsgebiet. Die Darstellung der Ausarbeitung folgt den Erkenntnissen von Francis und Litman [3].

2 Vorbereitungen

Für Codes und Codewörter werden zunächst in 2.1 die notwendigen Notationen eingeführt. In 2.2 werden die notwendigen Grundlagen zu Metriken behandelt sowie eine Abbildung mit einer hilfreichen Eigenschaft definiert. Für den Beweis der NP-Schwere von MR werden in 2.3 Grundkenntnisse zu aussagenlogischen Formeln und das 3SAT-Problem aufgestellt.

2.1 Vektoren und Codes

Für $n \in \mathbb{N}$ wird eine Menge $C \subseteq \{0,1\}^n$ als Code und beliebige $v \in \{0,1\}^n$ als Vektoren bezeichnet. Bezuglich den Vektoren sind folgende Formalitäten relevant:

- v_i ist das i-te Bit von v mit $v \in \{0,1\}^n$ und $1 \leq i \leq n$.
- $v|_i^j$ ist der Subvektor $v_i \dots v_j$ für $1 \leq i < j \leq n$.
- Ein Block von v ist der 2-Bit-Subvektor $v|_{2i-1}^{2i}$ für ein i mit $1 \leq i \leq n$.
- Ein Doppelblock von v ist der 2-Bit-Subvektor $v|_{2i-1}^{2i}$ mit $v_{2i-1} = v_{2i}$.
- uv ist die Konkatenation von $u \in \{0,1\}^m, v \in \{0,1\}^n$ mit $n, m \in \mathbb{N}$.

2.2 Metriken und Bitverschiebungen

Der Abstand zweier Vektoren zueinander wird über die Hamming-Distanz gemessen. Die Hamming-Distanz d ist eine Metrik auf $\{0,1\}^n$ mit

$$d(u,v) = \sum_{i=1}^{n} \Phi(u_i, v_i) \text{ für } u, v \in \{0,1\}^n \text{ mit}$$

$$\Phi : \Sigma \times \Sigma \to \{0,1\}, \Phi(a,b) = \begin{cases} 0 & \text{wenn } a = b, \\ 1 & \text{sonst} \end{cases}$$

Eine Abbildung $d : X \times X \to \mathbb{R}_0^+$ heißt Metrik auf X, wenn für beliebige Elemente $x, y, z \in X$ gilt:

1. $d(x,y) \geq 0$
2. $d(x,y) = d(y,x)$
3. $d(x,y) \leq d(x,z) + d(z,y)$

4. $d(x, x) = 0$

Wenn d eine Metrik auf X ist, dann heißt (X, d) metrischer Raum (siehe [4] Kapitel: *Die Grundbegriffe*).
Der Hamming-Ball $B_n(u, r)$ ist definiert als

$$B_n(u, r) = \{v \in \{0, 1\}^n \mid d(u, v) \leq r\}$$

der auch als r-Ball um u bezeichnet wird.
Die Abbildung f zwischen zwei metrischen Räumen (X_1, d) und (X_2, d) mit

$$f : X_1 \to X_2 \text{ und } d(f(x), f(y)) = d(x, y)$$

wird Isometrie genannt. Wenn f zusätzlich bijektiv ist, dann ist f eine isometrische Isomorphie (siehe [4] Kapitel: *Vervollständigung metrischer Räume*).

Definition 1. *Definiere $S_i : \{0, 1\}^{2n} \to \{0, 1\}^{2n}$ als die Abbildung, die einen Vektor zirkulär um $2i - 2$ Bits nach rechts verschiebt für ein i mit $1 \leq i \leq n$.*

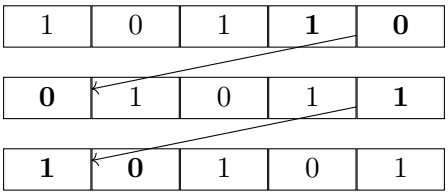

Abbildung 1: Ein Beispiel für $S_2(10110)$.

Lemma 1. *S_i ist ein isometrischer Isomorphismus vom metrischen Raum $(\{0, 1\}^{2n}, d)$ auf sich selbst.*

Beweis. Nach Def. muss gelten: (1) S_i ist eine Isometrie und (2) bijektiv.
(1) Sei $u, v \in \{0, 1\}^{2n}$ und k die Anzahl der Bits, die durch S_i zirkulär rechtsverschoben werden mit $k = 2i - 2$ und $1 \leq k \leq 2n - 2$. Es gilt

$$\begin{aligned}
d(S_i(u), S_i(v)) &= d(u_{2n-k+1}u_{2n-k+2} \dots u_{2n}u_1u_2 \dots u_{2n-k}, \\
&\qquad v_{2n-k+1}v_{2n-k+2} \dots v_{2n}v_1v_2 \dots v_{2n-k}) \\
&= \Phi(u_{2n-k+1}, v_{2n-k+1}) + \dots + \Phi(u_{2n}, v_{2n}) + \\
&\qquad \Phi(u_1, v_1) + \dots + \Phi(u_{2n-k}, v_{2n-k}) \\
&= \Phi(u_1, v_1) + \dots + \Phi(u_{2n-k}, v_{2n-k}) + \\
&\qquad \Phi(u_{2n-k+1}, v_{2n-k+1}) + \dots + \Phi(u_{2n}, v_{2n}) \\
&= \sum_{j=1}^{2n} \Phi(u_j, v_j) \\
&= d(u, v).
\end{aligned}$$

(2) Offensichtlich ist S_i bijektiv, denn die eindeutige Umkehrung S^{-1} ist lediglich eine zirkuläre Linksverschiebung um $2i - 2$ Bits. □

2.3 Das 3SAT-Problem

Eine Formel φ ist in konjunktiver Normalform (CNF), wenn φ die Form

$$\varphi = c^1 \wedge c^2 \wedge \cdots \wedge c^t$$

für $t \geq 1$ hat, wobei jeder der Klauseln $c^i, 1 \leq i \leq t$, die Form

$$c^i = l_{i,1} \vee \cdots \vee l_{i,n_i}$$

mit $n_i \geq 1$ hat, in der jeder Ausdruck $l_{i,j}, 1 \leq i \leq, 1 \leq j \leq n_i$, ein Literal (d.h. eine Variable oder negierte Variable) ist. φ ist eine 3CNF-Formel, wenn jede Klausel genau drei Literale enthält. Eine Belegung $\mathcal{I} : var \to \{0,1\}$ weist jeder Aussagenvariable einen Wahrheitswert 1 bzw. 0 zu. Unter einer Belegung wird eine Formel induktiv zu 1 oder 0 ausgewertet. Wenn es eine Belegung $\mathcal{I}$ gibt mit $\mathcal{I}(\varphi) = 1$, dann ist φ erfüllbar.

Definition 1 (3SAT-Problem)
Eingabe: *Eine 3CNF-Formel φ.*
Frage: *Gibt es eine Belegung, die φ erfüllt?*

Das Cook-Levin-Theorem [1] besagt, dass 3SAT NP-Vollständig ist.

3 MR und MCR

In der Einführung wurden die Begriffe Radius und Covering Radius genannt. Der Radius $\mathrm{R}(C)$ eines Codes C ist das kleinste $r \in \mathbb{N}$, sodass ein $u \in \{0,1\}^n$ existiert mit $C \subseteq B_n(u,r)$. Der Covering Radius $\mathrm{CR}(C)$ eines Codes C ist das kleinste $r \in \mathbb{N}$, sodass $\{0,1\}^n = \bigcup_{u \in C} B_n(u,r)$.

3.1 Definitionen

Definition 2 (Minimum-Radius-Problem (MR))
Eingabe: *ein Code $C \subseteq \{0,1\}^n$ und $k \in \mathbb{N}$*
Frage: *Ist $R(C) \leq k$?*

Beispiel 1. In Abbildung 1 ist der Code C mit $C = \{101, 111, 100\}$ vollständig im 1-Ball um 101 enthalten. Der Radius von C beträgt damit 1 und folglich gilt hier sogar für alle $k \geq 1$, dass $\langle C, k \rangle$ eine gültige Ja-Instanz des Minimum Radius Problem wäre.

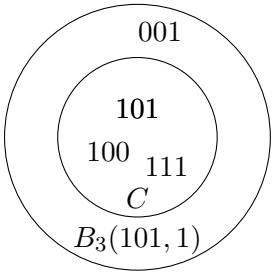

Abbildung 2: Ein Beispiel für $C \subseteq \{0,1\}^3$, $B_3(101,1)$.

Definition 3 (Maximum-Covering-Radius-Problem (MCR))
Eingabe: *ein Code* $C \subseteq \{0,1\}^n$ *und* $k \in \mathbb{N}$
Frage: *Ist* $CR(C) \geq k$*?*

Beispiel 2. Die Tabelle in Abbildung 2 veranschaulicht mit demselben Code C aus dem vorherigen Beispiel, wie die Vereinigung der 2-Bälle um die Codewörter vollständig den gesamten Raum $\{0,1\}^n$ abdecken (siehe die fett markierten Vektoren). Der Covering Radius von C beträgt damit 2 und folglich gilt hier für alle $k \leq 2$, dass $\langle C, k\rangle$ eine gültige Ja-Instanz des Maximum Covering Radius Problem wäre.

Code C	2-Ball
101	**000**, **001**, **011**, 100, 101, **110**, 111
100	000, 001, **010**, 100, 101, 110, 111
111	001, 010, 011, 100, 101, 110, 111

Abbildung 3: Eine beispielhafte Tabelle für $C \subseteq \{0,1\}^3$ und alle $v \in B_3(u,2)$ für ein $u \in C$.

3.2 Äquivalenz von MR und MCR

Sind beide Probleme zueinander äquivalent, so lassen sich beide aufeinander in höchstens polynomieller Zeit reduzieren. Die Reduktion folgt aus der Summe $\mathrm{R}(C) + \mathrm{CR}(C) = n$. Über die Äquivalenz kann mit der NP-Vollständigkeit von MR leicht die NP-Vollständigkeit von MCR gezeigt werden.

Lemma 2. *Sei* $u \in \{0,1\}^n$*, dann ist* $B_n(u^c, n-r-1)$ *das Komplement von* $B_n(u,r)$ *in* $\{0,1\}^n$*.*

Beweis.

$$\begin{aligned} v \notin B_n(u,r) &\Leftrightarrow d(u,v) > r \\ &\Leftrightarrow d(u^c,v) < n-r \\ &\Leftrightarrow v \in B_n(u^c, n-r-1) \end{aligned}$$

□

Lemma 3. *Für alle* $C \subseteq \{0,1\}^n$ *mit* $C \neq \emptyset$ *gilt:* $R(C) + CR(C) = n$*.*

Beweis. Sei r_{max} das größte r, sodass es ein $v \in \{0,1\}^n$ gibt mit $B_n(v,r) \cap C = \emptyset$.
Mit $r_{max}+1$ existiert nun ein $u \in \{0,1\}^n$ mit $u \in B_n(v, r_{max}+1) \cap C$, insbesondere also $u \in C$.
Daraus folgt, dass für alle $w \in \{0,1\}^n \setminus C$ gilt: $d(u,w) \leq r_{max}+1$,
also folgt daraus ebenfalls $\{0,1\}^n = \bigcup_{u \in C} B_n(u, r_{max}+1)$, und damit gilt

$$\begin{aligned} \mathrm{CR}(C) &= r_{max}+1 \\ &= max\{r \mid \exists v : C \cap B_n(v,r) = \emptyset\} + 1. \end{aligned}$$

Nach Def. von R(C)

$$\begin{aligned}\mathrm{R}(C) + \mathrm{CR}(C) &= min\{t \mid \exists u : C \subseteq B_n(u,t)\} + \\ &\quad (max\{r \mid \exists v : C \cap B_n(v,r) = \emptyset\} + 1).\end{aligned}$$

Nach Lemma 2

$$\begin{aligned}&= min\{t \mid \exists u : C \subseteq B_n(u,t)\} + \\ &\quad max\{r \mid \exists v : C \subseteq B_n(v, n-r-1)\} + 1.\end{aligned}$$

Ersetze r mit $n - r' - 1$, dann gilt

$$\begin{aligned}&= min\{t \mid \exists u : C \subseteq B_n(u,t)\} + \\ &\quad max\{n - r' - 1 \mid \exists v : C \subseteq B_n(v,r')\} + 1 \\ &= min\{t \mid \exists u : C \subseteq B_n(u,t)\} + \\ &\quad n - 1 - min\{r' \mid \exists v : C \subseteq B_n(v,r')\} + 1 \\ &= n.\end{aligned}$$

□

Nach Theorem 1 gilt $\mathrm{R}(C) \leq k \Leftrightarrow \mathrm{CR}(C) \geq n - k$ und damit sind MR und MCR aufeinander reduzierbar. Die Reduktionen sind offensichtlich polynomiell zeitbeschränkt in der Größe der Eingabe $\langle C, k \rangle$.

4 MR ist NP-schwer

Um die NP-Vollständigkeit von MR zu zeigen, sodass über die Äquivalenz bezüglich Polynomialzeitreduktionen beider Probleme auf die NP-Vollständigkeit von MCR zurückgeführt werden kann, sind für die Reduktion 3SAT≤MR einige Mittel erforderlich. Intuitiv wird klar, dass eine erfüllbare Formel auf eine Art und Weise kodiert werden muss, sodass ein Code entsteht, dessen Radius genau dann eine passende obere Schranke hat. Die Klauseln einer Formel werden so kodiert, dass sie genau dann in einem Hamming-Ball mit dieser Schranke enthalten sind, wenn die Formel erfüllbar ist. Hierbei ist das Zentrum immer die erfüllende Belegung kodiert als ein Vektor, welcher die Klauselvektoren nur dann erreicht, wenn mindestens ein Literal in jeder Klausel erfüllt ist. Um aber zu versichern, dass nur erfüllbare Belegungen "ausgefiltert" werden, wenn der konstruierte Code mit einem Höchstradius gegeben ist, sind die Klauselvektoren als Teil des Codes nicht ausreichend. Mit der Hinzunahme einer bestimmten Menge zum Code, und somit auch zum Teil des genannten Hamming-Balls, wird erzwungen, dass das Zentrum stets eine erfüllende Belegung in Form eines Doppelvektors $v = (v_1 v_1 v_2 v_2 ... v_n v_n) \in \{0,1\}^{2n}$ ist.

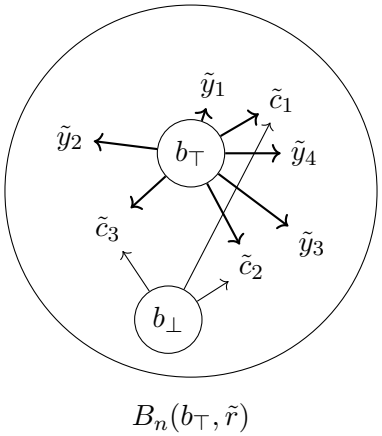

Abbildung 4: Die Intuition der Code-Struktur aus der Reduktion.

Beispiel 3. In Abbildung 4 ist die Struktur eines Codes C' mit $C' = \{\tilde{y}_1, \ldots, \tilde{y_4}, \tilde{c}_1, \ldots, \tilde{c}_3\}$ aus der beabsichtigten Reduktionsfunktion zu erkennen. Hierbei ist

- $b_\top$ eine erfüllende und $b_\bot$ eine nicht erfüllende Belegung, die passend kodiert sind.
- $\tilde{y}_i$ mit $i \in \{1, 2, 3, 4\}$ ein Vektor der selbst gewählten Menge, die die Auswahl von Zentren korrekt einschränkt.
- $\tilde{c}_j$ mit $i \in \{1, 2, 3\}$ die kodierte Klausel einer erfüllbaren 3CNF-Formel.

Die Pfeile stellen die Erreichbarkeit vom Zentrum im Sinne des Radius $\tilde{r}$ dar. Die konkrete Menge der Vektoren $\tilde{y}$ wird im nächsten Abschnitt konstruiert und ihr einschränkender Charakter bewiesen.

4.1 Doppelvektoren

Von einer konstruierten Menge $Y \subseteq \{0,1\}^{2n}$ wird bewiesen, dass ein beliebiger Vektor $v \in \{0,1\}^n$ genau dann ein Doppelvektor ist, wenn Y in dem n-Ball um v enthalten ist. Y wird konstruiert als

$$Y := \{(01)^n, (10)^n\} \cup \bigcup_{i=1}^{n} \{(01)^{i-1}10(01)^{n-i}\} \cup \bigcup_{i=1}^{n} \{(10)^{i-1}01(10)^{n-i}\}.$$

Die Untermenge Y^i mit $Y = \bigcup_{i=1}^{n} Y^i$ wird konstruiert als

$$Y^i := \{(01)^n, (10)^n, (01)^{i-1}10(01)^{n-i}, (10)^{i-1}01(10)^{n-i}\}.$$

Mit genauerem Blick enthält Y^i lediglich alle Folgen fester Länge von 01 bzw. 10 Bitblöcken mit höchstens einem komplementären Block an der Stelle des i-ten Blocks. Y betrachtet alle diese Folgen mit höchstens einem komplementären Block an beliebiger Stelle. Es wird ersichtlich, dass dieser Aufbau für das Zentrum v, dessen n-Ball Y^i enthält, an dem i-ten Block einen Doppelblock erzwingt.

Fakt 1. *Für beliebige $u_1, u_2 \in \{0,1\}^n$ und $v_1, v_2 \in \{0,1\}^m$ mit $n, m \in \mathbb{N}$ gilt:*

$$d(u_1v_1, u_2v_2) = d(u_1u_2) + d(v_1v_2).$$

Lemma 4. *Wenn $Y^1 \subseteq B_{2n}(v, n)$ für ein $v \in \{0,1\}^{2n}$, dann sind die ersten zwei Bits von v gleich.*

Beweis. Sei $Y^1 \subseteq B_{2n}(v, n)$. Nach Definition folgt, dass jeder Vektor zu $y \in Y$ eine Distanz von höchstens n zu v hat. Nach Fakt 1 lässt sich die Höchstdistanz in zwei weitere aufteilen, nämlich als $d(v|_1^2, y|_1^2) + d(v|_3^{2n}, y|_3^{2n}) \leq n$. Nach der Definition von Y können die Subvektoren $y|_1^2$ und $y|_3^{2n}$ in dieser Summe konkretisiert werden mit

$$max\{d(v|_1^2, 10), d(v|_1^2, 01)\} + max\{d(v|_3^{2n}, (01)^{n-1}), d(v|_3^{2n}, (10)^{n-1})\} \leq n.$$

Da bei einem beliebigen Block in $v|_3^{2n}$ (d.h. 00, 01, 10 oder 11) eine Hamming-Distanz von mindestens 1 zu einem Block an derselben Position in $(01)^{n-1}$ bzw. $(10)^{n-1}$ besteht, gilt nach Fakt 1, dass $max\{d(v|_3^{2n}, (01)^{n-1}), d(v|_3^{2n}, (10)^{n-1})\} \geq n - 1$, und damit

$$max\{d(v|_1^2, 10), d(v|_1^2, 01)\} \leq 1.$$

Also ist $v|_1^2$ ein Doppelblock. □

Lemma 4 lässt sich leicht über die Abbildung S_i erweitern. S_i verschiebt zirkulär die Bits eines Vektors um $2i - 2$ Bits bzw. um $i - 1$ Blöcke nach rechts. Mit genauerem Blick auf die Mengen Y^1 und Y^i wird sofort klar, dass

$$Y^i = S_i(Y^1).$$

Lemma 5. *Wenn $Y^i \subseteq B_{2n}(v, r)$ für $v \in \{0,1\}^{2n}$, dann ist $v_{2i-1} = v_{2i}$.*

Beweis. Aus Lemma 1 ist bekannt, dass S_i eine isometrische Isomorphie, also eine distanzen-erhaltende, bijektive Abbildung ist.

Damit gilt

$$Y^i \subseteq B_{2n}(v, n) \Leftrightarrow Y^1 \subseteq B_{2n}(S_i^{-1}(v), n).$$

Daraus folgt

$$\text{für alle } v \in \{0,1\}^{2n} : v_{2i-1} = v_{2i} \Leftrightarrow (S_i^{-1}(v))_1 = (S_i^{-1}(v))_2.$$

Nach Lemma 4 folgt damit, wenn $Y^i \subseteq B_{2n}(v, r)$ für ein $v \in \{0,1\}^{2n}$, dann $v_{2i-1} = v_{2i}$ □

Eines der zwei wichtigsten Lemmata für die Reduktion ist nun die am Anfang benannte Eigenschaft der Doppelvektoren:

Lemma 6. *Für alle $n > 0$ und $v \in \{0,1\}^n$ gilt:*

$$v \text{ ist ein Doppelvektor gdw. } Y \subseteq B_{2n}(v, n)$$

und Y kann in Polynomialzeit bezüglich n konstruiert werden.

Beweis. Betrachte Y als $Y = \bigcup_{i=1}^{n} Y^i$.
$\Rightarrow$: Sei v ein Doppelvektor und $y \in Y$.
Ein beliebiger Block aus v ist ein Doppelblock, und aus y entweder 01 oder 10. Daraus folgt $d(v_{2i-1}v_{2i}, y_{2i-1}y_{2i}) = 1$ für jedes $i \in \{1, \ldots, n\}$. Mehrfaches Anwenden von Fakt 1 ergibt $d(v, y) = n$, also $Y \subseteq B_{2n}(v, n)$.
$\Leftarrow$: Sei $Y \subseteq B_{2n}(v, n)$.
Nach Def. von Y gilt $Y^i \subseteq B_{2n}(v, n)$ und nach Lemma 5 folgt direkt, dass $v_{2i-1} = v_{2i}$ für jedes $i \in \{1, \ldots, n\}$.

Y kann in Polynomialzeit bezüglich n konstruiert werden, denn

$$\begin{aligned}
|Y| &= |\{(01)^n, (10)^n\} \cup \bigcup_{i=1}^{n} \{(01)^{i-1}10(01)^{n-i}\} \cup \bigcup_{i=1}^{n} \{(10)^{i-1}01(10)^{n-i}\}| \\
&= \underbrace{|\{(01)^n, (10)^n\}|}_{2} + \underbrace{|\bigcup_{i=1}^{n} \{(01)^{i-1}10(01)^{n-i}\}|}_{n} + \underbrace{|\bigcup_{i=1}^{n} \{(10)^{i-1}01(10)^{n-i}\}|}_{n} \\
&= 2n + 2.
\end{aligned}$$

□

4.2 Die Reduktion

Zum Nachweis der NP-Vollständigkeit von MR muss gezeigt werden, dass das Problem sowohl in NP liegt als auch NP-schwer ist. Für die NP-Schwere wird 3SAT auf MR reduziert. In 4.2.1 wird zunächst die Kodierung der Klauseln definiert als *Gadget* für die tatsächliche Reduktionsfunktion in 4.2.2. Zusätzlich wird im nächsten Abschnitt ein wichtiges Korollar abgeleitet, welches die kodierten Klauseln in Zusammenhang mit einer erfüllenden Belegung für die dazugehörige Formel setzt, sodass zusammen mit Lemma 6 in 4.2.2 die Korrektheit der Reduktion bewiesen wird.

4.2.1 Kodierung der Klauseln

Für eine Klausel c aus einer 3CNF-Formel φ über die Variablen $x_1, \ldots, x_n$ wird der Vektor $\hat{c} \in \{0,1\}^{2n}$ definiert mit

$$\text{für alle } i \in \{1, \ldots, n\},\ \hat{c}_{2i-1}\hat{c}_{2i} = \begin{cases} 00 & \text{wenn } c \text{ das Literal } \neg x_i \text{ enthält,} \\ 11 & \text{wenn } c \text{ das Literal } x_i \text{ enthält,} \\ 01 & \text{sonst.} \end{cases}$$

Eine Klausel c aus enthält genau 3 Literale, daher besteht $\hat{c}$ aus genau 3 Doppelblöcken, und $n - 3$ Blöcken mit den Bits 01.
Definiere $\Pi : \{0,1\}^n \to \{0,1\}^{2n}; v_1v_2...v_n \mapsto v_1v_1v_2v_2...v_nv_n$. Angemerkt sei hier, dass Π eine Bijektion von der Menge $\{0,1\}^n$ auf die Menge aller Doppelvektoren in $\{0,1\}^{2n}$ ist.

Die Belegung einer 3CNF φ über den Variablen $x_1, \ldots, x_n$ wird als Vektor $v \in \{0,1\}^n$ kodiert, wobei das i-te Bit die Belegung der Variable x_i ist.

Lemma 7. *Sei c eine Klausel aus einer 3CNF-Formel φ über die Variablen $x_1, \ldots, x_n$. Dann gilt für beliebige $v \in \{0,1\}^{2n}$:*

$$\hat{c} \in B_{2n}(\Pi(v), n+1) \Leftrightarrow \textit{die Belegung } v \textit{ erfüllt } c.$$

Beweis. Sei o.B.d.A. c eine Klausel über die Variablen x_1, x_2 und x_3. Fakt 1 impliziert, dass

$$d(\Pi(v), \hat{c}) = d(\Pi(v)|_1^6, \hat{c}|_1^6) + d(\Pi(v)|_7^{2n}, \hat{c}_7^{2n}).$$

Da $\Pi(v)$ ein Doppelvektor ist und die letzten $2n-6$ Bits bzw. die letzten $n-3$ Blöcke von $\hat{c}$ aus 01 Bits bestehen, gilt für alle $i \in \{4, \ldots, n\} : d(\Pi(v)|_{2i-1}^{2i}, \hat{c}|_{2i-1}^{2i}) = 1$. Mehrfaches Anwenden von Fakt 1 ergibt $d(\Pi(v)|_7^{2n}, \hat{c}|_7^{2n}) = n-3$.
Da die Variablen x_1, x_2 und x_3 in $\hat{c}$ vorkommen, besteht $\hat{c}|_1^6$ ausschließlich aus Doppelblöcken, also gilt dann

$$d(\Pi(v)|_1^6, \hat{c}|_1^6) \leq 4 \Leftrightarrow \text{es gibt ein } i \in \{1,2,3\}, \text{ sodass } (\Pi(v))_{2i-1}(\Pi(v))_{2i} = \hat{c}_{2i-1}\hat{c}_{2i}.$$

Nach Konstruktion von $\hat{c}$ ist eine Übereinstimmung beider Blöcke $(\Pi(v))_{2i-1}(\Pi(v))_{2i}$ und $\hat{c}_{2i-1}\hat{c}_{2i}$ genau dann gegeben, wenn es ein $i \in \{1,2,3\}$ gibt mit $v_i = \hat{c}_{2i}$. Das ist äquivalent dazu, dass mindestens ein Literal erfüllt ist mit $v_i = \mathcal{I}(x_i) = 0$, wenn $\neg x_i$ in c, oder $v_i = \mathcal{I}(x_i) = 1$, wenn x_i in c vorkommt. □

Korollar 1. *Sei $\varphi = c^1 \wedge \ldots \wedge c^t$ eine 3CNF über die Variablen $x_1, \ldots, x_n$, dann gilt für beliebige $v \in \{0,1\}^n$:*

$$\{\hat{c}^1, \ldots \hat{c}^t\} \subseteq B_{2n}(\Pi(v), n+1) \Leftrightarrow \textit{die Belegung } v \textit{ erfüllt } \varphi.$$

Das ist eine direkte Konsequenz von Lemma 7.

Beispiel 4. In Abbildung 5 wird Korollar 1 anhand der 3CNF-Beispielformel φ' veranschaulicht. Die fett markierten Blöcke zeigen eine Übereinstimmung eines Blocks von $\Pi(v)$ mit einem Block aus mindestens einem Vektor $\hat{c}^j$ mit $j \in \{0,1\}$. Dabei ist $\mathcal{I}(x_1) = 0$, weil $\neg x_1$ in c^1, und analog $\mathcal{I}(x_2) = 1$, weil x_2 in c^2 vorkommt. Mit diesen Belegungen sind die Klauseln bereits erfüllt.

$$\varphi' = (\neg x_1 \vee \neg x_2 \vee x_3) \wedge (x_2 \vee x_4 \vee \neg x_5)$$

φ'	x_1	x_2	x_3	x_4	x_5
$\hat{c}^1$	**00**	00	11	01	01
$\hat{c}^2$	01	**11**	01	11	00
$\Pi(v)$	**00**	**11**	00	00	11
$v = \mathcal{I}(\varphi')$	**0**	**1**	0	0	1

Abbildung 5: Das Beispiel für Korollar 1.

4.2.2 Von der 3CNF-Formel zum Code

Mit Korollar 1 und Lemma 6 gibt es nun die Mittel, im Zuge der NP-Schwere einen Code C_φ aus einer 3CNF-Formel φ zu konstruieren, der den Anforderungen der Reduktion gerecht wird.

Theorem 1. *Das Minimum-Radius-Problem ist NP-Vollständig.*

Beweis. MR ist in NP, denn der Zeuge $v \in \{0,1\}^n$ mit $C \subseteq B_n(v,k)$ ist offensichtlich polynomiell längenbeschränkt in der Größe der Eingabe $\langle C, k\rangle$. Der Verifizier rechnet und prüft die Hamming-Distanzen für alle $c \in C$ zu v durch und akzeptiert nur dann, wenn alle Distanzen höchstens k betragen, sonst verwirft er. Offensichtlich ist der Verifizierer polynomiell zeitbeschränkt in $\mathcal{O}(|C|)$.
Für die NP-Schwere wird 3SAT auf MR reduziert. Die Reduktionsfunktion wendet folgende Konstruktion an: Gegeben sei als Eingabe eine 3CNF-Formel $\varphi = c^1 \wedge \ldots \wedge c^t$ über die Variablen $x_1, \ldots, x_n$. Erweitere die Konstruktion von Y um einen Block, sodass $Y \subseteq \{0,1\}^{2(n+1)}$ und definiere Code $C_\varphi \subseteq \{0,1\}^{2(n+1)}$ mit

$$C_\varphi := Y \cup \{\hat{c}^1 00, \ldots, \hat{c}^t 00\}.$$

Für die Korrektheit der Reduktion ist zu zeigen, dass

$$\varphi \text{ ist erfüllbar} \Leftrightarrow R(C_\varphi) \leq n+1$$

$\Rightarrow$: Angenommen φ ist erfüllbar. Dann gibt es eine Belegung $v \in \{0,1\}^n$, die φ erfüllt. Mit dem Doppelvektor $\Pi(v)00$ gilt nach Lemma 2, dass

$$Y \subseteq B_{2(n+1)}(\Pi(v)00, n+1)$$

denn Lemma 2 ist wirksam für alle $n > 0$, also insbesondere für $n+1$.
Aufgrund der Erfüllbarkeit von φ folgt aus Korollar 1 5, dass $\{\hat{c}^1, \ldots, \hat{c}^t\} \subseteq B_{2n}(v, n+1)$. Nach Fakt 1 gilt für beliebige $u, v \in \{0,1\}^n : d(u,v) = d(u00, v00)$, und damit

$$\{\hat{c}^1 00, \ldots, \hat{c}^t 00\} \subseteq B_{2(n+1)}(\Pi(v)00, n+1)$$

Nach Def. von C_φ ist $C_\varphi \subseteq B_{2(n+1)}(\Pi(v)00, n+1)$.

$\Leftarrow$: Angenommen $R(C_\varphi) \leq n+1$. Dann gibt es $b \in \{0,1\}^{2(n+1)}$ mit $C \subseteq B_{2(n+1)}(b, n+1)$. Nach Def. von C_φ muss auch gelten, dass $Y \subseteq B_{2(n+1)}(b, n+1)$. Nach Lemma 2 folgt daraus, dass b ein Doppelvektor ist. Da Π eine Bijektion zwischen $\{0,1\}^n$ und der Menge aller Doppelvektoren in $\{0,1\}^{2n}$ ist, gibt es ein $v \in \{0,1\}^n$ mit $\Pi(v) = b|_1^{2n}$.
Nach Def. von C ist auch $\{\hat{c}^1 00, \ldots, \hat{c}^t 00\} \subseteq B_{2(n+1)}(b, n+1)$, sodass mit Fakt 1 folgt, dass

$$\{\hat{c}^1, \ldots, \hat{c}^t\} \subseteq B_{2n}(\Pi(v), n+1).$$

Nach Korollar 1 erfüllt die Belegung v die 3CNF-Formel φ.

Die Reduktion ist offensichtlich polynomiell zeitbeschränkt, denn

- die Konstruktion von Y ist nach Lemma 6 polynomiell zeitbeschränkt.
- die Konstruktion von $\{\hat{c}^1 00, \ldots, \hat{c}^t 00\}$ folgt aus der mehrfachen Anwendung der Klausel-Kodierung, welche Vektoren $\hat{c}$ der Länge 2n produziert, indem pro Variable in φ ein Block in $\hat{c}$ erzeugt wird: die Abbildung wird $(n \cdot t)$-mal angewendet.

□

Theorem 2. *Das Maximum Covering Radius Problem ist NP-Vollständig*

Beweis. Nach Theorem 1 ist bekannt, dass sowohl MR $\leq_p$ MCR als auch MCR $\leq_p$ MR. Aus MCR $\leq_p$ MR und MR $\in$ NP folgt, dass MCR $\in$ NP. Aus 3SAT $\leq_p$ MR $\leq_p$ MCR folgt, dass MCR NP-schwer ist. □

5 Ausblick

Eine alternative Interpretation des Minimum-Radius-Problems besteht darin, zu bestimmen, welcher String die kürzeste Hamming-Distanz zu allen anderen Strings einer bestimmten Menge aufweist. Ein bekanntes Anwendungsgebiet des Closest-String-Problems ist das Finden einer Consensussequenz in der Genetik [2]. Eine Consensussequenz ist eine funktionell wichtige DNA- oder Proteinsequenz, die bei verschiedenen Organismen weitgehend übereinstimmt, jedoch nicht identisch ist. Ein konkretes Beispiel ist folgendes: Bei der Erstellung von Gensonden (DNA- oder RNA-Moleküle) für bakterielle Infektionen geht es darum, eine spezielle DNA-Sequenz zu finden, die in allen DNA-Sequenzen einer Gruppe verwandter krankheitserregender Bakterien vorkommt, aber nicht in der DNA des Wirts (z.B. eines Menschen). Diese Sonden binden dann an diese spezifischen Zielsequenzen. Wird eine Bindung angezeigt, bedeutet das, dass mindestens eine der bakteriellen Spezies im Wirt vorhanden ist [2]. Die effizienten Algorithmen zur Lösung des Closest-String-Problems basieren häufig auf Metaheuristiken.

Literatur

[1] Cook, S. A.: *The complexity of theorem-proving procedures.* Proceedings of the third annual ACM symposium on Theory of computing, 1971. `https://api.semanticscholar.org/CorpusID:7573663`.

[2] Festa, P. und P. M. Pardalos: *Efficient solutions for the far from most string problem.* Annals of Operations Research, 196:663 – 682, 2011. `https://api.semanticscholar.org/CorpusID:18596656`.

[3] Frances, M. und A. Litman: *On covering problems of codes.* Theory of Computing Systems, 30:113–119, 1997. `https://api.semanticscholar.org/CorpusID:30005764`.

[4] Jänich, K.: *Topologie.* Springer Berlin, Heidelberg, 1996, ISBN 978-3-662-10576-4.