

Komplexität von Code-Problemen

Vortrag zum Seminar
“Komplexität”

FG Theoretische Informatik/Formale Methoden

Ahmad Lowejatan Noori

FB Elektrotechnik/Informatik, Universität Kassel

SoSe 2024

Codes

- Große Rolle in der Datenübertragungs- bzw. Nachrichtentechnik
- Digitalisierung analoger Signale
- Umwandlung von Daten in Bitstrings (Codewörtern)
- Fehlerkorrekturverfahren
- Minimaler Code: höhere Bit-Tiefe \leftrightarrow Überdeckender Code: Abdecken vieler Fehlerzustände

Code und Hamming-Ball

Eine Menge $C \subseteq \{0, 1\}^n$, $n \in \mathbb{N}$ von n -stelligen Binärstrings bezeichnen wir als **Code**.

Def.: $B_n(u, r)$ ist die Menge aller n -stelligen Binärstrings, die mit höchstens Hamming-Distanz r von einem zentralen Binärstring u erreicht werden können. (= **Hamming-Ball** um u)

Minimum Radius Problem

Der **Radius** von Code C , $R(C)$, ist das kleinste $r \in \mathbb{N}$, sodass gilt: $C \subseteq B_n(u, r)$ für irgendeinen Binärstring u .

Problem:

Eingabe: ein Code $C \subseteq \{0, 1\}^n$
und $k \in \mathbb{N}$

Frage: Ist $R(C) \leq k$?

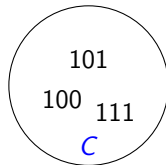


Abbildung: Beispiel für $C \subseteq \{0, 1\}^3$,
 $B_3(101, 1)$

Minimum Radius Problem

Der **Radius** von Code C , $R(C)$, ist das kleinste $r \in \mathbb{N}$, sodass gilt: $C \subseteq B_n(u, r)$ für irgendeinen Binärstring u .

Problem:

Eingabe: ein Code $C \subseteq \{0, 1\}^n$
und $k \in \mathbb{N}$

Frage: Ist $R(C) \leq k$?

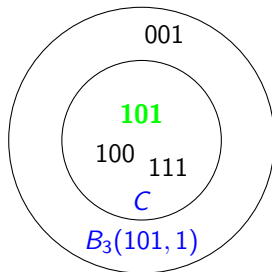


Abbildung: Beispiel für $C \subseteq \{0, 1\}^3$,
 $B_3(101, 1)$

Maximum Covering Radius Problem

Der **Covering Radius** von Code C , $CR(C)$, ist das kleinste $r \in \mathbb{N}$, sodass gilt
 $\{0, 1\}^n = \bigcup_{u \in C} B_n(u, r)$

Problem:

Eingabe: ein Code $C \subseteq \{0, 1\}^n$
und $k \in \mathbb{N}$

Frage: Ist $CR(C) \geq k$?

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: Beispiel für $C \subseteq \{0, 1\}^3$ und
alle $v \in B_3(u, 2)$ für ein $u \in C$

MR und MCR

Minimum Radius Problem (MR)

Eingabe: ein Code $C \subseteq \{0, 1\}^n$ und $k \in \mathbb{N}$

Frage: Ist $R(C) \leq k$?

Maximum Covering Radius Problem (MCR)

Eingabe: ein Code $C \subseteq \{0, 1\}^n$ und $k \in \mathbb{N}$

Frage: Ist $CR(C) \geq k$?

Äquivalenz von MR und MCR

Theorem 1: für alle $C \neq \emptyset, C \subseteq \{0,1\}^n : R(C) + CR(C) = n$

Beweisidee über die Form von CR :

- 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 Vektor $u \in C$, sodass dieser mit höchstens Hamming-Distanz $r_{\max} + 1$ jeden Vektor aus $\{0,1\}^n \setminus C$ überdeckt, und damit gilt

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

Äquivalenz von MR und MCR

$$R(C) + CR(C) = \min\{t \mid \exists u : C \subseteq B_n(u, t)\} + \\ (\max\{r \mid \exists v : C \cap B_n(v, r) = \emptyset\} + 1)$$

- Sei $v \in \{0, 1\}^n$, dann ist $B_n(v^c, n - r - 1)$ das Komplement von $B_n(v, r)$ in $\{0, 1\}^n$
- Durch **Bitflipping** hat v^c einen Abstand n zum Zentrum v , und erreicht mit höchstens Distanz $n - r - 1$ die restlichen Vektoren des Raums
- Mit **Maximierung** des Hamming-Balls $B_n(v, r)$ mit $B_n(v, r) \cap C = \emptyset$, **verkleinert** sich also auch der komplementäre Hamming Ball $B_n(v^c, n - r - 1)$, wobei $C \subseteq B_n(v^c, n - r - 1)$

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

Äquivalenz von MR und MCR

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

Ersetze r mit $n - r' - 1$:

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

$$= \min\{t \mid \exists u : C \subseteq B_n(u, t)\} + \\ n - 1 - \min\{r' \mid \exists v : C \subseteq B_n(v, r')\} + 1$$

$$= n$$

Äquivalenz von MR und MCR

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

Ersetze r mit $n - r' - 1$:

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

$$= \min\{t \mid \exists u : C \subseteq B_n(u, t)\} + \\ n - 1 - \min\{r' \mid \exists v : C \subseteq B_n(v, r')\} + 1$$

$$= n$$

Äquivalenz von MR und MCR

Beh.: MR und MCR sind äquivalent

Bew.: Aus $R(C) + CR(C) = n$ folgt $R(C) \leq k \Leftrightarrow CR(C) \geq n - k$

- MCR und MR aufeinander reduzierbar
- Reduktionen offensichtlich polynomiell-zeitbeschränkt

\Rightarrow **Über MR** wird die NP-Vollständigkeit von **MCR** bewiesen

Eigenschaften von Doppelvektoren

Doppelvektoren sind Vektoren $v = (v_1 v_1 v_2 v_2 \dots v_n v_n) \in \{0, 1\}^{2n}$

Solche Vektoren haben eine spezielle Eigenschaft, die sich für die spätere Reduktion $3SAT \leq_p MR$ im Zuge der NP-Schwere als nützlich erweisen:

Eigenschaften von Doppelvektoren

Doppelvektoren sind Vektoren $v = (v_1 v_1 v_2 v_2 \dots v_n v_n) \in \{0, 1\}^{2n}$

Solche Vektoren haben eine spezielle Eigenschaft, die sich für die spätere Reduktion $3SAT \leq_p MR$ im Zuge der NP-Schwere als nützlich erweisen:

Lemma 2: Für alle $n > 0$ existiert eine Menge $Y \subseteq \{0, 1\}^{2n}$, sodass für alle $v \in \{0, 1\}^{2n}$ gilt:
 v ist ein Doppelvektor $\Leftrightarrow Y \subseteq B_{2n}(v, n)$

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

Doppelvektor ist Ball-Zentrum von Y

Lemma 2: v ist ein Doppelvektor $\Leftrightarrow Y \subseteq B_{2n}(v, n)$

Bew.:

\Rightarrow : Sei v ein Doppelvektor. Dann besteht dieser aus einer n -fachen Konkatenation von 00- und 11-Blöcken. Die Vektoren aus Y sind gleich lang und bestehen aus 01- oder 10-Blöcken. D.h. Hamming-Distanzen zum Doppelvektor sind 1 für jeden Block, also insgesamt n .

\Leftarrow : *Beweisidee:* Über Untermenge von Y zeigen, dass zwei Bits von v gleich sein müssen, dann verallgemeinern

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

Die ersten zwei Bits sind gleich

Beh. 1: Wenn $Y^1 \subseteq B_{2n}(v, n)$ für $v \in \{0, 1\}^{2n}$, dann sind die ersten zwei Bits gleich.

Beweisskizze:

- Die maximale Distanz von $v = (v_1 v_2 \dots v_{2n}) \in \{0, 1\}^{2n}$ zu jedem Element aus Y^1 ist höchstens n
- max. Distanz setzt sich zusammen aus:
 - (1) max. Distanz der ersten zwei Bits von $v \in \{0, 1\}^{2n}$ und ein $y \in Y^1$
 - (2) max. Distanz der restlichen $2n - 2$ Bits beider Vektoren

Die ersten zwei Bits sind gleich

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

Beweisskizze:

- Die maximale Distanz von $v = (v_1 v_2 \dots v_{2n}) \in \{0, 1\}^{2n}$ zu jedem Element aus Y^1 ist höchstens n
- max. Distanz setzt sich zusammen aus:
 - (1) max. Distanz der ersten **zwei** Bits von $v \in \{0, 1\}^{2n}$ und ein $y \in Y^1$
 - (2) max. Distanz der restlichen $2n - 2$ Bits beider Vektoren

Y^1	Erste zwei Bits	Letzte $2n - 2$ Bits
y_0	01	01 0101...01
y_1	10	10 1010...10
y_2	01	10 1010...10
y_3	10	01 0101...01

Die ersten zwei Bits sind gleich

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

Beweisskizze:

- Die maximale Distanz von $v = (v_1 v_2 \dots v_{2n}) \in \{0, 1\}^{2n}$ zu jedem Element aus Y^1 ist höchstens n
- max. Distanz setzt sich zusammen aus:
 - (1) max. Distanz der ersten **zwei** Bits von $v \in \{0, 1\}^{2n}$ und ein $y \in Y^1$
 - (2) max. Distanz der restlichen $2n - 2$ Bits beider Vektoren

Y^1	Erste zwei Bits	Letzte $2n - 2$ Bits
y_0	01	01 01 01...01
y_1	10	10 10 10...10
y_2	01	10 10 10...10
y_3	10	01 01 01...01

Die ersten zwei Bits sind gleich

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

Beweisskizze:

- Die maximale Distanz von $v = (v_1 v_2 \dots v_{2n}) \in \{0, 1\}^{2n}$ zu jedem Element aus Y^1 ist höchstens n
- max. Distanz setzt sich zusammen aus:
 - (1) max. Distanz der ersten **zwei** Bits von $v \in \{0, 1\}^{2n}$ und ein $y \in Y^1$
 - (2) max. Distanz der restlichen $2n - 2$ Bits beider Vektoren

Y^1	Erste zwei Bits	Letzte $2n - 2$ Bits
y_0	01	0101 01 ...01
y_1	10	1010 10 ...10
y_2	01	1010 10 ...10
y_3	10	0101 01 ...01

Die ersten zwei Bits sind gleich

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

Beweisskizze:

- Die maximale Distanz von $v = (v_1 v_2 \dots v_{2n}) \in \{0, 1\}^{2n}$ zu jedem Element aus Y^1 ist höchstens n
- max. Distanz setzt sich zusammen aus:
 - (1) max. Distanz der ersten **zwei** Bits von $v \in \{0, 1\}^{2n}$ und ein $y \in Y^1$
 - (2) max. Distanz der restlichen $2n - 2$ Bits beider Vektoren

Y^1	Erste zwei Bits	Letzte $2n - 2$ Bits
y_0	01	0101 01 ...01
y_1	10	1010 10 ...10
y_2	01	1010 10 ...10
y_3	10	0101 01 ...01

Offensichtlich gilt für (2) **mindestens** $n - 1$, da bei jedem 2-Bit-Block von v zu einem 2-Bit-Block von y eine Distanz von **mindestens 1** entsteht.

D.h. für (1) gilt höchstens **1**, und die ersten 2 Bits von v sind **00** bzw. **11**.

Alle Zwei-Bit-Blöcke sind gleich

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

Beweisskizze: Gilt über Beh. 1 und entsprechender **zirkulärer Bitverschiebung** nach rechts.

Definiere $Y = Y^1 \cup Y^2 \cup \dots \cup Y^n$.

Da $Y^i \subseteq B_{2n}(v, n)$ für alle i mit $1 \leq i \leq n$ gilt nach Beh. 2, dass v ein **Doppelvektor** sein muss, wenn Y im Raum $\{0, 1\}^{2n}$ Teil eines Hamming-Balls mit Radius n ist.

Alle Zwei-Bit-Blöcke sind gleich

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

Beweisskizze: Gilt über Beh. 1 und entsprechender **zirkulärer Bitverschiebung** nach rechts.

Definiere $Y = Y^1 \cup Y^2 \cup \dots \cup Y^n$.

Da $Y^i \subseteq B_{2n}(v, n)$ für alle i mit $1 \leq i \leq n$ gilt nach Beh. 2, dass v ein **Doppelvektor** sein muss, wenn Y im Raum $\{0, 1\}^{2n}$ Teil eines Hamming-Balls mit Radius n ist.

Y kann in **poly. Zeit** konstruiert werden, da

$$|Y| = |\{(01)^n, (10)^n\} \cup \bigcup_{i=1}^n \{(01)^{i-1}10(01)^{n-i}\} \cup \bigcup_{i=1}^n \{(10)^{i-1}01(10)^{n-i}\}| = 2n + 2$$

MR ist NP-Vollständig

Theorem 2: Das Minimum Radius Problem ist NP-Vollständig

1. $MR \in NP$:

- Zeuge: $v \in \{0, 1\}^n$ als Zentrum eines Radius- k Balls, der C enthält
- offensichtlich **polynomiell-längenbeschränkt** in der Größe der Eingabe $\langle C, k \rangle$
- Verifizierer rechnet und prüft Distanzen zum Zeugen durch in $\mathcal{O}(|C|)$

MR ist NP-Vollständig

Theorem 2: Das Minimum Radius Problem ist NP-Vollständig

1. MR \in NP:

- Zeuge: $v \in \{0, 1\}^n$ als Zentrum eines Radius- k Balls, der C enthält
- offensichtlich **polynomiell-längenbeschränkt** in der Größe der Eingabe $\langle C, k \rangle$
- Verifizierer rechnet und prüft Distanzen zum Zeugen durch in $\mathcal{O}(|C|)$

2. MR ist NP-schwer

Wir zeigen: $3SAT \leq MR$

Idee:

- Jede Klausel aus 3CNF φ durch einen Vektor in $\{0, 1\}^{2n}$ repräsentieren
- Erfüllende Belegung als **Hamming-Ball-Zentrum**: **Doppelvektor**
- Zusammenhänge zwischen Klauselvektoren und Zentrum so kodieren, dass der Code C mit minimalem Radius k einer erfüllenden Belegung von φ entspricht

Kodierung der Klauseln

Für eine Klausel c über den Variablen x_1, \dots, x_n definieren wir den Vektor $\hat{c} \in \{0, 1\}^{2n}$ folgendermaßen:

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

Definiere $\Pi : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$; $v_1 v_2 \dots v_n \mapsto v_1 v_1 v_2 v_2 \dots v_n v_n$.

Beh. 3: Sei $\varphi = c_1 \wedge \dots \wedge c_t$ eine 3CNF Formel über die Variablen x_1, \dots, x_n , dann gilt für beliebige $v \in \{0, 1\}^n$

$$\{\hat{c}_1, \dots, \hat{c}_t\} \subseteq B_{2n}(\Pi(v), n+1) \Leftrightarrow \text{die Belegung } v \text{ erfüllt } \varphi$$

Hierbei wird Belegung v mit $\top = 1$ und $\perp = 0$ kodiert.

Literalblöcke und Belegung

Beh. 3: Sei $\varphi = c_1 \wedge \dots \wedge c_t$ eine 3CNF Formel über die Variablen x_1, \dots, x_n , dann gilt für beliebige $v \in \{0, 1\}^n$

$$\{\hat{c}_1, \dots, \hat{c}_t\} \subseteq B_{2n}(\Pi(v), n+1) \Leftrightarrow \text{die Belegung } v \text{ erfüllt } \varphi$$

Intuition:

- Jeder Vektor \hat{c} hat **drei** 11- oder 00-Blöcke und $n - 3$ 01-Blöcke

Beispiel:

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

φ'	x_1	x_2	x_3	x_4	x_5
\hat{c}_0	00	00	11	01	01
\hat{c}_1	01	11	01	11	00
$\Pi(v)$	00	11	00	00	11
$\mathcal{I}(\varphi')$	\perp	\top	\perp	\perp	\top

Literalblöcke und Belegung

Beh. 3: Sei $\varphi = c_1 \wedge \dots \wedge c_t$ eine 3CNF Formel über die Variablen x_1, \dots, x_n , dann gilt für beliebige $v \in \{0, 1\}^n$

$$\{\hat{c}_1, \dots, \hat{c}_t\} \subseteq B_{2n}(\Pi(v), n+1) \Leftrightarrow \text{die Belegung } v \text{ erfüllt } \varphi$$

Intuition:

- Jeder Vektor \hat{c} hat **drei** 11- oder 00-Blöcke und $n - 3$ 01-Blöcke
- Hamming-Distanz von $\Pi(v)$ zu den $n - 3$ 01-Blöcken: $n - 3$

Beispiel:

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

φ'	x_1	x_2	x_3	x_4	x_5
\hat{c}_0	00	00	11	01	01
\hat{c}_1	01	11	01	11	00
$\Pi(v)$	00	11	00	00	11
$\mathcal{I}(\varphi')$	\perp	\top	\perp	\perp	\top

Literalblöcke und Belegung

Beh. 3: Sei $\varphi = c_1 \wedge \dots \wedge c_t$ eine 3CNF Formel über die Variablen x_1, \dots, x_n , dann gilt für beliebige $v \in \{0, 1\}^n$

$$\{\hat{c}_1, \dots, \hat{c}_t\} \subseteq B_{2n}(\Pi(v), n+1) \Leftrightarrow \text{die Belegung } v \text{ erfüllt } \varphi$$

Intuition:

- Jeder Vektor \hat{c} hat **drei** 11- oder 00-Blöcke und $n - 3$ 01-Blöcke
- Hamming-Distanz von $\Pi(v)$ zu den $n - 3$ 01-Blöcken: $n - 3$
- Ein Block von $\Pi(v)$ muss mit **mindestens einem** der drei 11- oder 00-Blöcke übereinstimmen

Beispiel:

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

φ'	x_1	x_2	x_3	x_4	x_5
\hat{c}_0	00	00	11	01	01
\hat{c}_1	01	11	01	11	00
$\Pi(v)$	00	11	00	00	11
$\mathcal{I}(\varphi')$	\perp	\top	\perp	\perp	\top

Literalblöcke und Belegung

Beh. 3: Sei $\varphi = c_1 \wedge \dots \wedge c_t$ eine 3CNF Formel über die Variablen x_1, \dots, x_n , dann gilt für beliebige $v \in \{0, 1\}^n$

$$\{\hat{c}_1, \dots, \hat{c}_t\} \subseteq B_{2n}(\Pi(v), n+1) \Leftrightarrow \text{die Belegung } v \text{ erfüllt } \varphi$$

Intuition:

- Jeder Vektor \hat{c} hat **drei** 11- oder 00-Blöcke und $n - 3$ 01-Blöcke
- Hamming-Distanz von $\Pi(v)$ zu den $n - 3$ 01-Blöcken: $n - 3$
- Ein Block von $\Pi(v)$ muss mit **mindestens einem** der drei 11- oder 00-Blöcke übereinstimmen
- Hamming-Distanz von $\Pi(v)$ zu den drei 11- oder 00-Blöcken: **höchstens 4**

Beispiel:

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

φ'	x_1	x_2	x_3	x_4	x_5
\hat{c}_0	00	00	11	01	01
\hat{c}_1	01	11	01	11	00
$\Pi(v)$	00	11	00	00	11
$\mathcal{I}(\varphi')$	\perp	\top	\perp	\perp	\top

Von 3CNF zu Code

- 3CNF $\varphi = c_1 \wedge \dots \wedge c_t$, Variablen x_1, \dots, x_n
- Sei unser konstruiertes Y nun aus $\{0, 1\}^{2(n+1)}$

Wir definieren Code $C_\varphi \subseteq \{0, 1\}^{2(n+1)}$ wie folgt:
 $C_\varphi = Y \cup \{\hat{c}_1 00, \dots, \hat{c}_t 00\}$

C_φ ist offensichtlich berechenbar in **poly. Zeit** aus φ .

Erinnerung

Beh. 3: $\{\hat{c}_1, \dots, \hat{c}_t\} \subseteq B_{2n}(\Pi(v), n+1) \Leftrightarrow$
die Belegung v erfüllt φ

Lemma 2: v ist ein Doppelvektor $\Leftrightarrow Y \subseteq$
 $B_{2n}(v, n)$

Von 3CNF zu Code

3SAT \leq MR: φ ist erfüllbar $\Leftrightarrow R(C_\varphi) \leq n + 1$

\Rightarrow :

Sei φ erfüllbar. Dann existiert eine erfüllende Belegung $v \in \{0, 1\}^n$.

- Nach **Lemma 2**:
 $Y \subseteq B_{2(n+1)}(\Pi(v)00, n + 1)$
- Nach *Beh. 3*:
 $\{\hat{c}_1, \dots, \hat{c}_t\} \subseteq B_{2n}(\Pi(v), n + 1)$
- also auch $\{\hat{c}_100, \dots, \hat{c}_t00\}$
 $\subseteq B_{2(n+1)}(\Pi(v)00, n + 1)$

Folglich $C_\varphi = Y \cup \{\hat{c}_100, \dots, \hat{c}_t00\} \subseteq B_{2(n+1)}(\Pi(v)00, n + 1)$, also $R(C_\varphi) \leq n + 1$

\Leftarrow :

Sei $b \in \{0, 1\}^{2(n+1)}$ Zentrum eines Balls mit Radius $n + 1$, in dem C_φ enthalten ist.

- $Y \subseteq B_{2(n+1)}(b, n + 1)$
- Nach **Lemma 2**:
 b ist also Doppelvektor
- Sei $b' \in \{0, 1\}^{2n}$ wie b ohne den letzten 00/11-Block, dann existiert $v \in \{0, 1\}^n$ mit $\Pi(v) = b'$
- $\{\hat{c}_100, \dots, \hat{c}_t00\} \subseteq B_{2(n+1)}(b, n + 1)$
- also auch $\{\hat{c}_1, \dots, \hat{c}_t\} \subseteq B_{2n}(\Pi(v), n + 1)$

Folglich ist v nach *Beh. 3* eine erfüllende Belegung und damit φ erfüllbar.

MCR ist NP-Vollständig

Beh.: Das **Maximum Covering Radius Problem** ist NP-Vollständig

Bew.: folgt sofort aus **Äquivalenz** von **MCR** und **MR** und **NP-Vollständigkeit** von **MR**



Ausblick

- Weiteres Anwendungsgebiet:
Consensussequenz in der Genetik
- Def.: Funktionell wichtige DNA- oder Proteinsequenz, die bei verschiedenen Organismen weitgehend übereinstimmt, aber **nicht** identisch ist
- Viele “effiziente” Algorithmen sind metaheuristisch

Beispiele für Metaheuristiken

1. Bestimme eine Startlösung L
2. Definiere eine *Nachbarschaft* von zu L “ähnlichen” Lösungen
3. Suche diese Nachbarschaft vollständig ab und bestimme die beste Lösung

Literatur

-  Frances, M., Litman, A. On covering problems of codes. Theory of Computing Systems 30, 113–119 (1997). <https://doi.org/10.1007/BF02679443>
-  Festa, P., Pardalos, P.M. Efficient solutions for the far from most string problem. Ann Oper Res 196, 663–682 (2012). <https://doi.org/10.1007/s10479-011-1028-7>

Hamming-Distanz

- Codes sind nicht nur auf binärem Alphabet beschränkt
- $\Sigma = \{c_1, c_2, \dots, c_k\}, u, v \in \Sigma^m$
- $d(u, v) = \sum_{i=1}^m \Phi(u_i, v_i)$
- $\Phi : \Sigma \times \Sigma \rightarrow \{0, 1\}, \Phi(a, b) = \begin{cases} 0 & \text{wenn } a = b, \\ 1 & \text{sonst.} \end{cases}$

Fakten über Hamming-Distanzen

1. Seien u_1, u_2 und v_1, v_2 Binärstrings mit $|u_1| = |u_2|$ und $|v_1| = |v_2|$, dann gilt
$$d(u_1 v_1, u_2 v_2) = d(u_1, u_2) + d(v_1, v_2)$$
2. Für beliebige $u, v \in \{0, 1\}^n$: $d(u, v) + d(u^c, v) = n$

Hamming-Ball Komplement

Beh.: Sei $v \in \{0,1\}^n$, dann ist $B_n(v^c, n - r - 1)$ das Komplement von $B_n(v, r)$ in $\{0,1\}^n$

Bew.:

$$v \notin B_n(v, r) \Leftrightarrow d(u, v) > r \quad (1)$$

$$\Leftrightarrow d(u^c, v) < n - r \quad (2)$$

$$\Leftrightarrow v \in B_n(u^c, n - r - 1) \quad (3)$$

(2) folgt aus $d(u, v) + d(u^c, v) = n$

Zirkuläre Rechtsverschiebung

Sei $S_i : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ die zirkuläre Rechtsverschiebung eines Vektors um $2i - 2$ Bits. Für $i = 1, \dots, n$ definieren wir $Y^i = S_i(Y^1)$.

Beh. 2: Wenn $Y^i \subseteq B_{2n}(v, n)$ für $v \in \{0,1\}^{2n}$, dann ist $v_{2i} = v_{2i-1}$
Bew.:

- S_i ist ein Isomorphismus, also auch eine bijektive (distanzen-erhaltende) Abbildung
- Folglich gilt für alle i :
 $Y^i \subseteq B_{2n}(v, n) \Leftrightarrow Y^1 \subseteq B_{2n}(S_i^{-1}(v), n)$
- Es gilt also auch für beliebige $v \in \{0,1\}^{2n} : v_{2i-1} = v_{2i} \Leftrightarrow (S_i^{-1}(v))_1 = (S_i^{-1}(v))_2$. (nach Beh. 1)

Beispiel:
2-Bit-Verschiebung

1	0	1	1	0
0	1	0	1	1
1	0	1	0	1

Erinnerung

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