

In der Arbeit

- ▶ E. BERLEKAMP, R. McELIECE, H. VAN TILBORG,
On the inherent intractability of certain coding problems,
IEEE Transactions on Information Theory 24:384-386,1978.

zeigen die Autoren, dass gewisse Anforderungen, die bei der Decodierung linearer Codes ganz natürlich auftreten, leider Inkarnationen von NP-vollständigen Problemen sind,

- ▶ $A \in \mathbb{B}^{t \times s}$ sei $(t \times s)$ -Matrix über dem booleschen Ring \mathbb{B} .
- ▶ $\tilde{A} \in \mathbb{B}^{t(s+1) \times s(t+1)+t}$ sei gegeben durch

$$\tilde{A} = \left[\begin{array}{c|c} A & \\ \hline E_s & \\ E_s & E_{st+t} \\ \vdots & \\ E_s & \end{array} \right]$$

wobei E_s die $(s \times s)$ -Einheitsmatrix ist.

- ▶ Für $0 \leq k \leq s(t+1) + t$ seien q, r durch die Divisionseigenschaft von \mathbb{Z} :

$$k = q \cdot (t+1) + r \quad \text{mit} \quad 0 \leq q \leq s, 0 \leq r \leq t$$

- ▶ Die beiden folgenden Aussagen sind äquivalent:
 1. $\exists \mathbf{u} \in \mathbb{B}^s$ mit $\|\mathbf{u}\| = q, \|A \cdot \mathbf{u}\| = r$.
 2. $\exists \mathbf{v} \in \mathbb{B}^{s(t+1)+t}$ mit $\|\mathbf{v}\| = k, \|\tilde{A} \cdot \mathbf{v}\| = 0$.

- ▶ Beweis: Ist $\mathbf{v} \in \mathbb{B}^{s(t+1)+t}$ Spaltenvektor der Länge $s(t+1) + t$ und schreibt man

$$\mathbf{v} = \begin{bmatrix} \mathbf{v}' \\ \mathbf{v}'' \end{bmatrix} \quad \text{mit} \quad \mathbf{v}' \in \mathbb{B}^s, \mathbf{v}'' \in \mathbb{B}^{st+t},$$

so gilt

$$\tilde{A} \cdot \mathbf{v} = \begin{bmatrix} A \cdot \mathbf{v}' \\ \mathbf{v}' \\ \vdots \\ \mathbf{v} \end{bmatrix} \oplus \mathbf{v}''$$

1. \Rightarrow 2. Existiert ein \mathbf{u} wie angegeben, so setzt man

$$\mathbf{v} = \begin{bmatrix} \mathbf{u} \\ A \cdot \mathbf{u} \\ \mathbf{u} \\ \vdots \\ \mathbf{u} \end{bmatrix} \in \mathbb{B}^{s(t+1)+t}, \text{ d.h. } \mathbf{v}' = \mathbf{u}, \mathbf{v}'' = \begin{bmatrix} A \cdot \mathbf{u} \\ \mathbf{u} \\ \vdots \\ \mathbf{u} \end{bmatrix}$$

und erhält nach obiger Bemerkung

$$\tilde{A} \cdot \mathbf{v} = \begin{bmatrix} A \cdot \mathbf{u} \\ \mathbf{u} \\ \vdots \\ \mathbf{u} \end{bmatrix} \oplus \begin{bmatrix} A \cdot \mathbf{u} \\ \mathbf{u} \\ \vdots \\ \mathbf{u} \end{bmatrix} = \mathbf{0}$$

Ausserdem gilt

$$\|\mathbf{v}\| = \|A \cdot \mathbf{u}\| + (t+1)\|\mathbf{u}\| = k.$$

2. \Rightarrow 1. Existiert ein \mathbf{v} wie angegeben, so folgt aus

$$\mathbf{0} = \tilde{A} \cdot \mathbf{v} = \begin{bmatrix} A \cdot \mathbf{v}' \\ \mathbf{v}' \\ \vdots \\ \mathbf{v}' \end{bmatrix} \oplus \mathbf{v}'', \text{ dass } \mathbf{v}'' = \begin{bmatrix} A \cdot \mathbf{v}' \\ \mathbf{v}' \\ \vdots \\ \mathbf{v}' \end{bmatrix}.$$

Somit ist $\|\mathbf{v}''\| = \|A \cdot \mathbf{v}'\| + t \cdot \|\mathbf{v}'\|$ und daher

$$k = \|\mathbf{v}\| = \|\mathbf{v}'\| + \|\mathbf{v}''\| = (t+1) \cdot \|\mathbf{v}'\| + \|A \cdot \mathbf{v}'\|.$$

Wegen $0 \leq A \cdot \mathbf{v}' \leq t$ und der Divisionsbeziehung zwischen k, t, q und r folgt $\|\mathbf{v}'\| = q$ und $\|A \cdot \mathbf{v}'\| = r$.

► 3-DIM MATCHING (3DM)

- *Instanzen:* Eine Menge T und eine Menge von Tripeln $S \subseteq T \times T \times T$ mit $s = \#S \geq \#T = t$.
- *Frage:* Gibt es $M \subseteq S$ mit $\#M = t$, wobei sich je zwei verschiedene Tripel aus M in allen drei Komponenten unterscheiden sollen.
Anders gesagt: projiziert man die Tripel aus M auf ihre drei Komponenten, so tritt jedes Element von T in jeder der drei Komponentnen genau einmal auf.
- *Kommentar:* (3DM) ist ein wohlbekanntes \mathcal{NP} -vollständiges Problem. GAREY, JOHNSON *Computers and Intractability*, Freeman 1979, oder PAPADIMITRIOU, *Computational Complexity*, Addison-Wesley 1994.

► Beispiel mit $T = \{1, 2, 3, 4\}$

- $S = \{(1, 2, 2), (2, 4, 3), (3, 1, 4), (3, 3, 4), (4, 1, 2), (4, 3, 1)\}$ hat das Matching

$$M = \{(1, 2, 2), (2, 4, 3), (3, 1, 4), (4, 3, 1)\}.$$

- $S = \{(1, 3, 1), (1, 4, 2), (2, 1, 4), (2, 3, 3), (3, 4, 4), (4, 2, 3)\}$ hat kein Matching!

▶ LINEAR DECODING (LD)

- ▶ *Instanzen:* Matrix $H \in \mathbb{B}^{s,t}$, Vektor $\mathbf{s} \in \mathbb{B}^s$, Zahl $w \in \mathbb{N}$.
- ▶ *Frage:* Gibt es einen Vektor $\mathbf{x} \in \mathbb{B}^t$ mit $H \cdot \mathbf{x} = \mathbf{s}$ und mit $\|\mathbf{x}\| \leq w$?
- ▶ *Kommentar:* Der Vektor \mathbf{s} spielt die Rolle des Syndroms beim Decodieren linearer Codes. Dabei sucht man unter allen Vektoren, die dasselbe Syndrom \mathbf{s} liefern einen Vektor mit minimalem Gewicht: dies ist im Sinne der üblichen *maximum-likelihood-Decodierung* der wahrscheinlichste Fehlervektor. Kann man LD effizient lösen, so kann man durch systematisches Probieren mit $w = 1, 2, \dots$ auch den Fehlervektor von minimalem Gewicht finden, also das Decodierungsproblem für lineare Codes lösen.

▶ EXACT MINIMUM DISTANCE (EMD)

- ▶ *Instanzen:* Matrix $H \in \mathbb{B}^{s,t}$, Zahl $w \in \mathbb{N}$.
- ▶ *Frage:* Gibt es einen Vektor $\mathbf{x} \in \mathbb{B}^t$ mit $H \cdot \mathbf{x} = \mathbf{0} \in \mathbb{B}^s$ und $\|\mathbf{x}\| = w$?
- ▶ Für einen linearen Code, gegeben durch die Kontrollmatrix H ist die Minimaldistanz das minimale Gewicht der vom Nullvektor verschiedenen Codevektoren. Gefragt wird hier, ob es einen Codevektor vom Gewicht w in dem durch H definierten Code gibt.
- ▶ *Kommentar:* Es ist (scheinbar) nicht bekannt, ob das analoge Problem, aber mit der Anforderung $\|\mathbf{x}\| \leq w$, \mathcal{NP} -vollständig ist.

- ▶ Offensichtlich: $3DM, LD, EMD \in \mathcal{NP}$
- ▶ Zeigen: $3DM \leq_p LD$ und $3DM \leq_p EMD$
- ▶ Damit sind auch LD und EMD \mathcal{NP} -vollständig.

- ▶ (T, S) sei Instanz von 3DM mit $T = \{1, 2, \dots, t\}$.

- ▶ Zuordnung

$$T \ni a \mapsto \vec{\mathbf{e}}_a \in \mathbb{B}^t$$

(als Spaltenvektor geschrieben)

- ▶ Zuordnung

$$T \times T \times T \ni \mathbf{a} = (a_1, a_2, a_3) \mapsto \vec{\mathbf{a}} = \begin{bmatrix} \vec{\mathbf{e}}_{a_1} \\ \vec{\mathbf{e}}_{a_2} \\ \vec{\mathbf{e}}_{a_3} \end{bmatrix} \in \mathbb{B}^{3t}$$

- ▶ Zuordnung

$$S = \{\mathbf{a}, \mathbf{b}, \dots, \mathbf{z}\} \subseteq T \times T \times T \mapsto A_S = \begin{bmatrix} \vec{\mathbf{a}} & \vec{\mathbf{b}} & \dots & \vec{\mathbf{z}} \end{bmatrix} \in \mathbb{B}^{3t \times s}$$

► Übersetzung der Beispiele in Matrixschreibweise

- $S = \{(1, 2, 2), (2, 4, 3), (3, 1, 4), (3, 3, 4), (4, 1, 2), (4, 3, 1)\}$
- $M = \{(1, 2, 2), (2, 4, 3), (3, 1, 4), (4, 3, 1)\}$

$$A_S = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \quad A_S \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

Lösung \mathbf{x} mit $\|\mathbf{x}\| \leq 4$: $[1 \ 1 \ 1 \ 0 \ 1 \ 0]^t$.

- $S = \{(1, 3, 1), (1, 4, 2), (2, 1, 4), (2, 3, 3), (3, 4, 4), (4, 2, 3)\}$

$$A_S = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \quad A_S \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

hat keine Lösung $\mathbf{x} \in \mathbb{B}^6$ mit $\|\mathbf{x}\| \leq 4$.

► Reduktion $3DM \leq_p LD$

$$(T, S) \mapsto (A_S, \vec{\mathbf{1}}, t)$$

Das Tripelsystem (T, S) enthält genau ein Matching M , wenn Instanz $(A_S, \vec{\mathbf{1}}, t)$ von LD eine Lösung hat, wobei $\vec{\mathbf{1}} \in \mathbb{B}^{3t}$ der Spaltenvektor mit 1en in allen Komponenten ist,

► Reduktion $3DM \leq_p EMD$

Dies geht ganz analog, wobei statt A_S die Matrix

$$\widetilde{A}_S \in \mathbb{B}^{3t(s+1) \times 3t(s+1)+s}$$

verwendet wird, Obige Überlegung zu booleschen Matrizen mit $(t, q, r) = (3t, t, 3t)$, also mit Zielvektor \mathbf{x} vom Gewicht $k = t(3t + 1) + 3t = 3t^2 + 4t$ zeigt, dass

$$(T, S) \mapsto (\widetilde{A}_S, 3t^2 + 4t)$$

die gesuchte Reduktion leistet,