

Mathematik für Informatiker: Diskrete Strukturen

Wichtel, Codes und Graphen

Jens Zumbärgel

Institut für Algebra
Fachbereich Mathematik
TU Dresden

WiSe 2016/17 · 21. Dez. 2016



Die Weihnachtswichtel

Der böse König hält drei Weihnachtswichtel gefangen.

Er setzt jedem eine rote oder eine grüne Zipfelmütze auf. Die Wichtel können ihre eigene Mütze nicht sehen, aber die Mützen der zwei anderen. Der König verkündet:

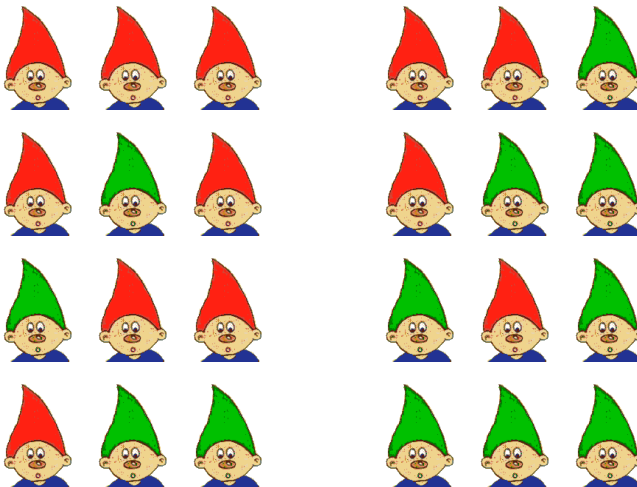
„Auf mein Signal darf jeder die Farbe seiner Mütze raten (oder schweigen). Wenn einer die richtige Antwort sagt, kommt ihr alle frei. Wenn aber eine falsche Antwort dabei ist, bleiben alle gefangen.“



Unter der Annahme, dass die Mützen zufällig gleichverteilt werden, wie können die Wichtel ihre Gewinnchance maximieren?

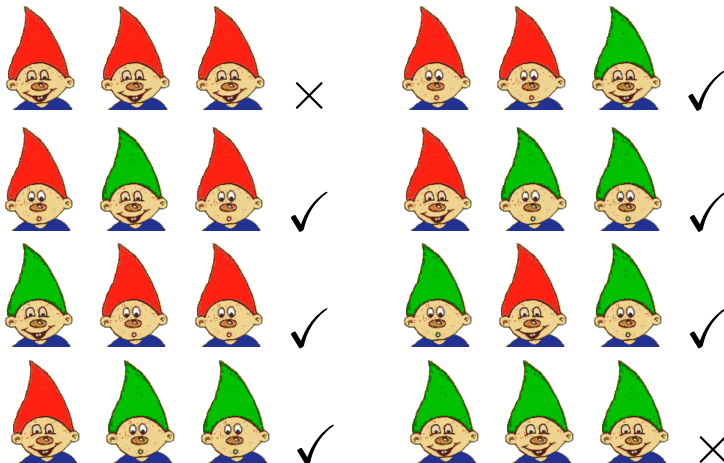
Zur Strategie

Es gibt acht gleichwahrscheinliche Konstellationen.



Die beste Strategie

Sieht ein Weihnachtswichtel, dass die anderen zwei Mützen die gleiche Farbe haben, so rät er die andere Farbe.



Die Wichtel kommen zu 75 % frei.

Und bei sieben Wichteln?

Der böse König hält nun sieben Weihnachtswichtel gefangen.

Er stellt sie in eine Reihe und setzt jedem eine rote oder eine grüne Zipfelmütze auf. Die Wichtel können ihre eigene Mütze nicht sehen, aber die Mützen der sechs anderen.

„Auf mein Signal darf jeder die Farbe seiner Mütze raten (oder schweigen). Wenn einer die richtige Antwort sagt, kommt ihr alle frei. Wenn aber eine falsche Antwort dabei ist, bleiben alle gefangen.“



Unter der Annahme, dass die Mützen zufällig gleichverteilt werden, wie können die Wichtel ihre Gewinnchance maximieren?

Es gibt eine Strategie, bei der die Wichtel zu 87,5 % frei kommen.

Zur Strategie

Es gibt 128 Konstellationen. Betrachte die folgenden 16 ausgewählten.



Die beste Strategie

Jede der 112 anderen Konstellationen hat folgende Eigenschaft:
Es gibt genau eine Position, so dass nach Auswechslung der Zipfelmütze eine der 16 ausgewählten Konstellationen entsteht.

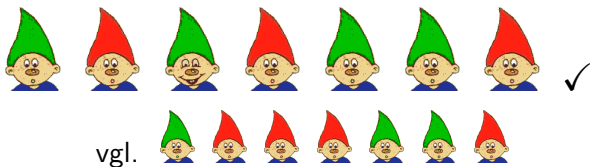
Die beste Strategie

Jede der 112 anderen Konstellationen hat folgende Eigenschaft:
Es gibt genau eine Position, so dass nach Auswechslung der Zipfelmütze eine der 16 ausgewählten Konstellationen entsteht.

Strategie: Bemerkt ein Wichtel, dass eine mögliche Farbe seiner Mütze eine ausgewählte Konstellation ergibt, so rät er die andere Farbe.

- Liegt eine der 16 ausgewählten Konstellation vor, so antworten alle 7 Wichtel falsch.
- In den 112 anderen Fällen antwortet genau ein Wichtel richtig!

Beispiel:



Ein besonderer Code

Es gibt 128 Vektoren in $\{0, 1\}^7$. Betrachte die folgenden 16 ausgewählten.

(0 0 0 0 0 0 0)	(1 1 1 1 1 1 1)
(1 1 0 1 0 0 0)	(0 0 1 0 1 1 1)
(0 1 1 0 1 0 0)	(1 0 0 1 0 1 1)
(0 0 1 1 0 1 0)	(1 1 0 0 1 0 1)
(0 0 0 1 1 0 1)	(1 1 1 0 0 1 0)
(1 0 0 0 1 1 0)	(0 1 1 1 0 0 1)
(0 1 0 0 0 1 1)	(1 0 1 1 1 0 0)
(1 0 1 0 0 0 1)	(0 1 0 1 1 1 0)

Die Menge dieser Vektoren heißt **Hamming-Code** C .

Er hat folgende besondere Eigenschaft:

Zu jedem Vektor $x \in \{0, 1\}^7 \setminus C$ gibt es genau eine Position $i \in [7]$, so dass $\tilde{x} := x \oplus e_i$ (Austausch der i -ten Ziffer) in C liegt.

Linearität und Minimalabstand von C

$$\begin{array}{ll} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Der Hamming Code C erfüllt $x \oplus y \in C$ für alle $x, y \in C$,
wobei $(x \oplus y)_i := x_i \oplus y_i := x_i + y_i \bmod 2$ („xor“) für $i \in [7]$.
Mit $\{0, 1\} = \mathbb{F}_2$ ist der Code also ein Untervektorraum von $\mathbb{F}_2^7$.
Man spricht dann von einem *linearen* Code.

Linearität und Minimalabstand von C

(0 0 0 0 0 0 0)	(1 1 1 1 1 1 1)
(1 1 0 1 0 0 0)	(0 0 1 0 1 1 1)
(0 1 1 0 1 0 0)	(1 0 0 1 0 1 1)
(0 0 1 1 0 1 0)	(1 1 0 0 1 0 1)
(0 0 0 1 1 0 1)	(1 1 1 0 0 1 0)
(1 0 0 0 1 1 0)	(0 1 1 1 0 0 1)
(0 1 0 0 0 1 1)	(1 0 1 1 1 0 0)
(1 0 1 0 0 0 1)	(0 1 0 1 1 1 0)

Der Hamming Code C erfüllt $x \oplus y \in C$ für alle $x, y \in C$,
wobei $(x \oplus y)_i := x_i \oplus y_i := x_i + y_i \bmod 2$ („xor“) für $i \in [7]$.
Mit $\{0, 1\} = \mathbb{F}_2$ ist der Code also ein Untervektorraum von $\mathbb{F}_2^7$.
Man spricht dann von einem *linearen* Code.

Der Code C hat *Minimalgewicht* 3, das heißt die kleinste Anzahl Einsen eines Codeworts $c \in C \setminus \{0\}$ ist drei. Es folgt, weil C linear ist, dass der *Minimalabstand* zwischen zwei Codewörtern drei Positionen ist.

Binäre lineare Codes

Die **Codierungstheorie** befasst sich mit der Konstruktion von Codes mit großem Minimalabstand, sowie fehlerkorrigierenden Decodierungsalgorithmen.

Definition

Ein *binärer linearer Code* ist ein Untervektorraum $C \subseteq \mathbb{F}_2^n$.

Jeder k -dimensionale lineare Code $C \subseteq \mathbb{F}_2^n$ kann als Lösungsmenge

$$C = \{x \in \mathbb{F}_2^n \mid Hx = 0\}$$

einer $r \times n$ -Matrix H über $\mathbb{F}_2$ (mit $r \geq n-k$) beschrieben werden, der sog. *Kontrollmatrix*, engl. „parity-check matrix“.

Kontrollmatrix des Hamming-Codes

Der Hamming-Code $C \subseteq \mathbb{F}_2^7$ ist ein linearer Code.

Es gilt $\dim C = 4$, und C ist Lösungsmenge $\{x \in \mathbb{F}_2^7 \mid Hx = 0\}$ der Matrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Das heißt $(x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in \mathbb{F}_2^7$ ist ein Codewort in C genau dann, wenn die Gleichungen

$$x_1 + x_3 + x_4 + x_5 = 0$$

$$x_2 + x_4 + x_5 + x_6 = 0$$

$$x_3 + x_5 + x_6 + x_7 = 0$$

gelten (Arithmetik in $\mathbb{F}_2$, das heißt modulo 2).

Codes und Graphen

Ein Graph $G = (V, E)$ heißt *bipartit*, falls

- Knoten $V = A \dot{\cup} B$ mit disjunkten Mengen A und B ,
- Kanten $E \subseteq \{\{a, b\} \mid a \in A, b \in B\}$.

Jede Kontrollmatrix $H = (h_{ji}) \in \mathbb{F}_2^{r \times n}$ definiert

- 1) einen linearen Code $C = \{x \in \mathbb{F}_2^n \mid Hx = 0\}$,
- 2) einen bipartiten Graphen $G = (V, E)$ mit

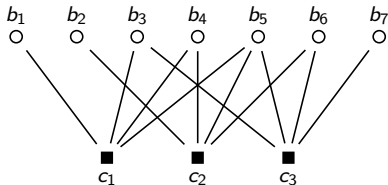
$$V = \{b_1, \dots, b_n\} \dot{\cup} \{c_1, \dots, c_r\},$$

$$E = \{\{b_i, c_j\} \mid h_{ji} = 1\},$$

genannt *Tanner-Graph* (b_i „Bitknoten“, c_j „Kontrollknoten“).

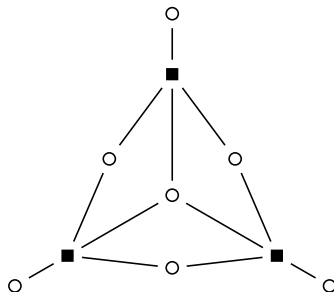
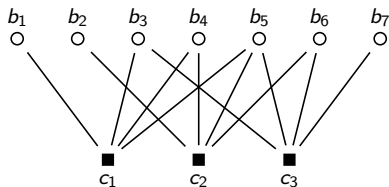
Graph des Hamming-Codes

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$



Graph des Hamming-Codes

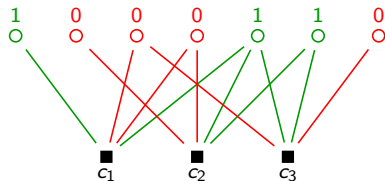
$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$



Graph des Hamming-Codes

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

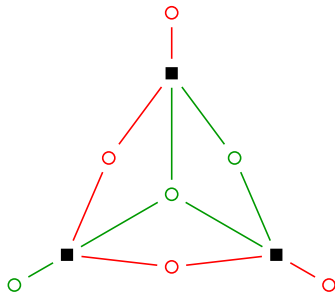
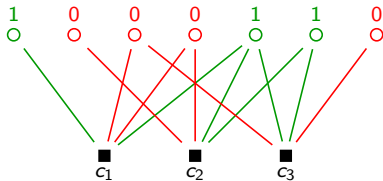
$$x = (1\ 0\ 0\ 0\ 1\ 1\ 0) \in \mathcal{C}$$



Graph des Hamming-Codes

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$$x = (1\ 0\ 0\ 0\ 1\ 1\ 0) \in C$$



Decodierung

Sei $C \subseteq \mathbb{F}_2^n$ ein linearer Code mit $\dim C = k$. Wir können also $|C| = 2^k$ verschiedene Nachrichten codieren.

Informationsübertragung mit Fehlern:

$$x \in C \xrightarrow{\text{⚡}} y \in \mathbb{F}_2^n \mapsto x$$

Das (exakte) **Decodierungsproblem** lautet:

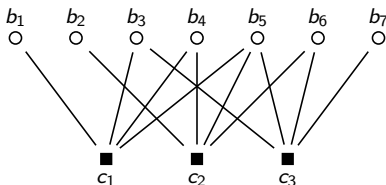
Finde zu $y \in \mathbb{F}_2^n$ das *wahrscheinlichste* Codeword $x \in C$, d. h. welches minimalen Abstand $|\{i \mid x_i \neq y_i\}|$ hat.

Dies ist ein schwieriges Problem!

(Für allgemeine binäre lineare Codes NP-vollständig.)

Decodierung via Message-Passing

Es gibt effiziente iterative Verfahren, die auf dem Tanner-Graph operieren.



- 1 Die Bitknoten erhalten Werte des empfangenen Vektors.
- 2 Jeder Bitknoten schickt seinen Wert zu den benachbarten Kontrollknoten.
- 3 Jeder Kontrollknoten berechnet daraus eine neue Abschätzung und schickt diese zurück zu den benachbarten Bitknoten.
- 4 Die Bitknoten aktualisieren ihre Werte; wiederhole von Schritt 2.

Konkret: Sum-Product-Algorithmus (SPA)

Sei $H = (h_{ji})$ eine $r \times n$ -Kontrollmatrix für C mit Tanner-Graphen G_H .

- Sei $I := \{b_1, \dots, b_n\}$ und $J := \{c_1, \dots, c_r\}$.
- Seien $J_i := N(b_i) \subseteq J$ und $I_j := N(c_j) \subseteq I$ die Nachbarknoten in G_H .
- Sei C_j der *lokale Code* definiert durch den Kontrollknoten c_j .

Konkret: Sum-Product-Algorithmus (SPA)

Sei $H = (h_{ji})$ eine $r \times n$ -Kontrollmatrix für C mit Tanner-Graphen G_H .

- Sei $I := \{b_1, \dots, b_n\}$ und $J := \{c_1, \dots, c_r\}$.
- Seien $J_i := N(b_i) \subseteq J$ und $I_j := N(c_j) \subseteq I$ die Nachbarknoten in G_H .
- Sei C_j der *lokale Code* definiert durch den Kontrollknoten c_j .

Input $y \in \mathbb{F}_2^n$. Lokale Werte $\gamma_i(b) := \Pr(x_i = b \mid y_i)$.

Aktualisierungsregel der Nachrichten:

$$\mu_{ij}^{\text{neu}}(b) := \gamma_i(b) \cdot \prod_{j' \in J_i \setminus \{j\}} \mu_{j'i}(b) \quad (b \in \mathbb{F}_2)$$

$$\mu_{ji}^{\text{neu}}(b) := \sum_{\substack{x|_{I_j} \in C_j \\ x_i = b}} \prod_{i' \in I_j \setminus \{i\}} \mu_{i'j}(x_{i'})$$

Endwerte $\mu_i(b) := \gamma_i(b) \cdot \prod_{j \in J_i} \mu_{ji}(b)$.

Offene Forschungsfragen

- 1) Für welche Codes bzw. Tanner-Graphen löst der Sum-Product-Algorithmus das Decodierungsproblem?
- 2) Wie konstruiert man dafür gute Codes via Tanner-Graphen?

Offene Forschungsfragen

- 1) Für welche Codes bzw. Tanner-Graphen löst der Sum-Product-Algorithmus das Decodierungsproblem?

Teilantwort: Für Bäume.

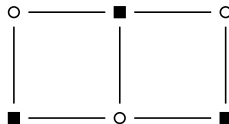
- 2) Wie konstruiert man dafür gute Codes via Tanner-Graphen?

Teilantwort: Mit sog. „Expander-Graphen“.

Beispiel: Problem der Kreise

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

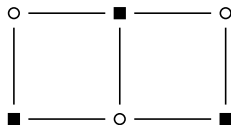
$$\mathcal{C} = \{(000)\}$$



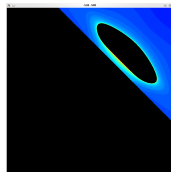
Beispiel: Problem der Kreise

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

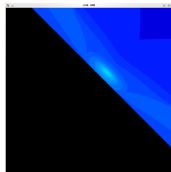
$$C = \{(\textcolor{red}{0} \textcolor{red}{0} \textcolor{red}{0})\}$$



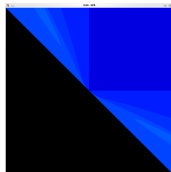
Sei $\lambda_i := \log \frac{\Pr(x_i=0|y_i)}{\Pr(x_i=1|y_i)}$ (also $\lambda_i > 0$ tendiert zu $x_i = 0$, $\lambda_i < 0$ zu $x_i = 1$)



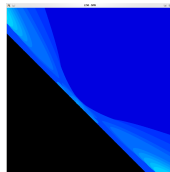
$\lambda_3 = -5$



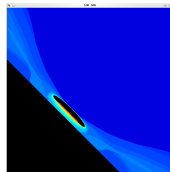
$-2,5$



0



$2,5$



5

Verhalten von SPA für $\lambda \in [-5, 5]^3$ (schwarz = Misserfolg)

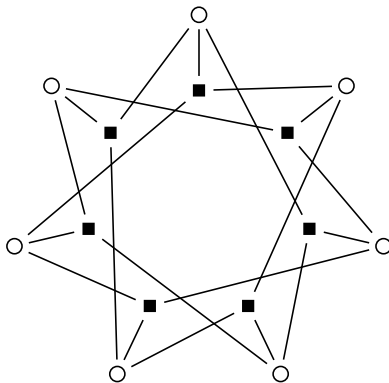
Konstruktion guter Codes

Wir suchen (Tanner-)Graphen derart, dass

- 1) keine kurzen Kreise existieren:
der *Gurt* (engl. „girth“), d. h. die kleinste Länge eines Kreises, sei also groß
- 2) die „Expander“-Eigenschaft gilt:
für jede Menge $S \subseteq I$ von Bitknoten sei die Zahl der benachbarten Kontrollknoten $|N(S)| \geq c|S|$ (mit $c > 0$) „groß“ im Vergleich zu $|S|$

Diese Eigenschaften sind gegensätzlicher Natur.

Beispiel Gurt 6



$$V := \{b_0, \dots, b_6\} \cup \{c_0, \dots, c_6\}$$

$$E := \{\{b_i, c_j\} \mid j - i \in \{0, 1, -2\}\} \text{ (Indizes mod 7)}$$

Graphen aus Gruppen

Sei $p > 2$ eine Primzahl und sei

$$G := \mathrm{SL}_2(\mathbb{Z}_p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}_p^{2 \times 2} \mid ad - bc = 1 \right\}.$$

Dann ist $(G, \cdot)$ mit Matrixprodukt eine Gruppe der Ordnung $|G| = p^3 - p$.

Graphen aus Gruppen

Sei $p > 2$ eine Primzahl und sei

$$G := \mathrm{SL}_2(\mathbb{Z}_p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}_p^{2 \times 2} \mid ad - bc = 1 \right\}.$$

Dann ist $(G, \cdot)$ mit Matrixprodukt eine Gruppe der Ordnung $|G| = p^3 - p$.

Betrachte $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \in G$.

$$V := \{b_g, \tilde{b}_g \mid g \in G\} \cup \{c_g \mid g \in G\}$$

$$E := \left\{ \{b_g, c_h\} \mid hg^{-1} \in \{A^2, ABA^{-1}, B\}\right\} \\ \cup \left\{ \{\tilde{b}_g, c_h\} \mid hg^{-1} \in \{A^{-2}, AB^{-1}A^{-1}, B^{-1}\}\right\}$$

Graphen aus Gruppen

Sei $p > 2$ eine Primzahl und sei

$$G := \mathrm{SL}_2(\mathbb{Z}_p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}_p^{2 \times 2} \mid ad - bc = 1 \right\}.$$

Dann ist $(G, \cdot)$ mit Matrixprodukt eine Gruppe der Ordnung $|G| = p^3 - p$.

Betrachte $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \in G$.

$$V := \{b_g, \tilde{b}_g \mid g \in G\} \cup \{c_g \mid g \in G\}$$

$$E := \left\{ \{b_g, c_h\} \mid hg^{-1} \in \{A^2, ABA^{-1}, B\} \right\} \\ \cup \left\{ \{\tilde{b}_g, c_h\} \mid hg^{-1} \in \{A^{-2}, AB^{-1}A^{-1}, B^{-1}\} \right\}$$

Satz

Der Graph (V, E) hat Gurt $\geq \log_{1+\sqrt{2}}\left(\frac{p}{2}\right) - 1$.

Für $p = 7$ erhalten wir zum Beispiel einen hervorragenden Code C der Länge $n = 672$ und Dimension $\dim C = 336$.

Schöne Weihnachtsferien!

