Idee der Berechnung von Automorphismengruppen von Codes nach J. Leon von Gabriele Nebe

Sei $C \leq \mathbf{F}_2^n$ ein linearer binärer Code der Dimension m. Dann ist die **Automorphismengruppe**

$$\mathrm{Aut}(C) = \{\pi \in S_n \mid \pi(C) = C\} = \mathrm{Stab}_{S_n}(C)$$

der Stabilisator von C unter der Operation der symmetrischen Gruppe S_n auf der Menge aller m-dimensionalen Teilräume von $\mathbf{F}_2^n$. Dieser kann prinzipiell mit dem Bahnenalgorithmus berechnet werden. In der Praxis ist die Bahn C^{S_n} jedoch zu lang damit der Bahnenalgorithmus mit vertretbarem Aufwand durchläuft.

Die Idee von Leon ist ein gewisses backtracking, wie ich Ihnen im Beispiel des Hammingcodes der Länge 7 vorgemacht habe.

Generalvoraussetzung. C sei gegeben durch eine Erzeugermatrix $G = (I_m, A) \in \mathbf{F}_2^{m\times n}$. Wir nehmen an, dass

$$(\star)\text{die Spalten von } G \text{ paarweise verschieden}$$

sind. Unter dieser Voraussetzung gilt

Satz 1. Die Abbildung

$$\mathrm{Aut}(C) \to \mathrm{GL}(C), \pi \mapsto \tilde{\pi} := \pi_{|C}$$

ist injektiv.

Beweis. Ist $\pi \in \mathrm{Aut}(C)$, so ist die Abbildung

$$\tilde{\pi} : C \to C, (c_1, \ldots, c_n) \mapsto (c_{\pi(1)}, \ldots, c_{\pi(n)})$$

ein wohldefinierter linearer Automorphismus von C und $\tilde{}$ ist ein Gruppenhomomorphismus. Es ist $\tilde{\pi} = \mathrm{id}_C$, genau dann, wenn jedes Codewort von C festgelassen wird. Wegen der Generalvoraussetzung $(\star)$, gibt es aber zu je zwei verschiedenen Indizes $i \neq j \in \{1, \ldots, n\}$ ein $c \in C$ mit $c_i \neq c_j$. Da $\tilde{\pi}(c) = c$ kann also $\pi(i)$ nicht gleich j sein. Diese Überlegung gilt für jedes $j \neq i$, also muss $\pi(i) = i$ sein (für jedes i). q.e.d.

Sims hat in der algorithmischen Gruppentheorie das Konzept der **base** für Permutationsgruppen $\Sigma \leq S_n$ eingeführt.

Definition 2. Sei $\Sigma \leq S_n$. Eine Teilmenge $B \subseteq \{1, \ldots, n\}$ heißt **base** für Σ, falls

$$\bigcap_{b\in B} \mathrm{Stab}_\Sigma(b) = \{1\}.$$

Bemerkung. Der Sinn einer base ist es, zu Erkennen, wann zwei Elemente in Σ gleich sind (bzw. zusammen mit den **strong generators**, die ich hier nicht definiert habe, zu testen, ob ein Element der S_n in Σ liegt). Sind $\sigma_1, \sigma_2 \in \Sigma$, so gilt

$$\sigma_1 = \sigma_2 \Leftrightarrow \sigma_1(b) = \sigma_2(b) \text{ für alle } b \in B.$$

Denn dann ist $\sigma_1\sigma_2^{-1} \in \bigcap_{b\in B} \mathrm{Stab}_\Sigma(b)$.

Satz 3. Unter der Generalvoraussetzung ist $\{1, \ldots, m\}$ eine base für $\mathrm{Aut}(C)$.

Beweis. Ist $\pi \in \mathrm{Aut}(C)$ mit $\pi(1) = 1, \ldots, \pi(m) = m$, so lässt $\tilde{\pi} \in \mathrm{GL}(C)$ die m Basisvektoren (die Zeilen der Erzeugermatrix) fest, ist also die Identität, und somit auch $\pi = 1$ wegen Satz 1. q.e.d.

Leon sucht nun Automorphismen π von C, indem er die möglichen Bilder $\pi(1), \ldots, \pi(m)$ durchläuft und suksessive die Stabilisatoren der ersten k Punkte ($k = m, m-1, m-2, \ldots, 1, 0$) berechnet, wobei er folgende Strategie benutzt um gewisse Permutationen auszuschliessen:

Bemerkung. $\mathrm{Aut}(C)$ operiert auf

$$W := \{c \in C \mid wt(c) = d(C)\}$$

Diese Operation ist treu, falls $\langle W \rangle = C$.

Definition 4. Sei $I = (i_1, \ldots, i_s) \in \{1, \ldots, n\}^s$ und $v \in \mathbf{F}_2^s$. Definiere

$$A_W(I, v) := |\{c \in W \mid (c_{i_1}, \ldots, c_{i_s}) = v\}$$

als die Anzahl der Worte in W, die an den Spalten $(i_1, \ldots, i_s)$ genau das Wort v stehen haben.

Dann ist klar

Folgerung 5. Ist $\pi \in$Aut(C), so ist für jedes gegebene $v \in \mathbf{F}_2^s$ und jedes s-Tupel $I = (i_1, \ldots, i_s) \in \{1, \ldots, n\}^s$

$$A_W(I, v) = A_W(\pi(I), v).$$

Diese Strategie wird am Beispiel des Hammingcodes veranschaulicht.