Minimale Logarithmische Signaturen: Part II
-Sophiane Yahiatene-

Bezeichne den endlichen Körper mit q Elementen mit $\mathbb{F}_q$.

Lemma 18. *Sei G eine endliche Gruppe mit Untergruppen H und K, sodass $G = H.K$ und $H \cap K = 1$ gilt. Außerdem besitzen H und K eine Minimale Logarithmische Signature (kurz: MLS). So gelten folgende Aussagen:*

1. *G besitzt eine MLS.*
2. *Ist N ein Normalteiler von G, sodass $N \leq K$ und K/N eine MLS besitzt, so besitzt auch G/N eine MLS.*
3. *Analoge Aussage für $N \leq H$*

Beweis. Bezeichne mit $\alpha_H = [\alpha_1^H, ..., \alpha_s^H]$ (bzw. $\alpha_K = [\alpha_1^K, ..., \alpha_t^K]$) eine MLS von H (bzw. K). Genauer sei $\alpha_i^H = [\alpha_{i,0}^H, ..., \alpha_{i,r_i}^H]$ für alle $(1 \leq i \leq s)$.

1. $\alpha = [\alpha_1^H, ..., \alpha_s^H, \alpha_1^K, ..., \alpha_t^K]$ ist eine MLS von G.
2. Sei $\alpha^{K/N} = [\alpha_1^{K/N}, ..., \alpha_m^{K/N}]$ eine MLS von K/N und sei $\alpha^H N := [[\alpha_{1,0}^H N, ..., \alpha_{1,r_1}^H N], ..., [\alpha_{s,0}^H N, ..., \alpha_{s,r_s}^H N]]$ bestehend aus Elementen aus G/N.
   Nun ist $\alpha^{G/N} := [\alpha^H N, \alpha^{K/N}]$ eine MLS für G/N, denn für jedes $gN \in G/N$ gilt:
   $$\exists! h \in H \; \exists! k \in K : g = h \cdot k$$
   $$\Rightarrow gN = (hk)N = (hN) \cdot (kN),$$
   wobei sich kN eindeutig faktorisieren lässt und hN genau einen Repräsentanten aus H besitzt. Das α^G minimale Länge besitzt ist klar.
3. Dies lässt sich auf analoge Weise zeigen.

□

Satz 19. *Sei $n \in \mathbb{N}$ und q eine Primzahlpotenz. So besitzt $GL_n(\mathbb{F}_q)$ eine MLS. Allgemeiner, für alle Untergruppe $Z \leq Z(GL_n(q))$ besitzt die Gruppe $GL_n(q)/Z$ eine MLS.*
(ohne Beweis.)

Definition 20. *Die Projektive Lineare Gruppe ist durch*

$$PGL_n(q) := PGL_n(\mathbb{F}_q) := GL_n(\mathbb{F}_q)/Z(GL_n(\mathbb{F}_q))$$

definiert, wobei mit $Z(GL_n(\mathbb{F}_q))$ das Zentrum der Gruppe $GL_n(\mathbb{F}_q)$ bezeichnet wird.
Die Projektive Spezielle Lineare Gruppe ist durch

$$PSL_n(q) := PSL_n(\mathbb{F}_q) := SL_n(\mathbb{F}_q)/Z(SL_n(\mathbb{F}_q))$$

definiert, wobei mit $Z(SL_n(\mathbb{F}_q))$ das Zentrum der Gruppe $SL_n(\mathbb{F}_q)$ bezeichnet wird.

Im nächsten Abschnitt wird zur Hilfenahme der "Method of Double Coset Decomposition"(MDCD) und Lemma 6 nachgewiesen, dass die $PSL_n(q)$ und die $SL_n(q)$ eine MLS besitzen. Zuvor allerdings ein Lemma.

Lemma 21. *1. Es existiert eine zyklische Untergruppe $K \leq GL_n(q)$ der Ordnung $q^n - 1$, die scharf transitiv auf $\mathbb{F}_q^n$ operiert und für die $C_{GL_n(q)}(K) = K$ gilt. K nennt man auch den 'Singer-Zyklus'.*

2. *Definiere $Z := Z(GL_n(q))$ und $S := SL_n(q)$. So gilt $Z_0 := Z \cap S = Z(SL_n(q))$ ist eine zyklische Gruppe der Ordnung $d := ggt(n, q-1)$, d.h. es gibt d verschiedene n-te Einheitswurzeln in $\mathbb{F}_q^*$.*
3. *Die Gruppe $K_0 := K \cap S$ ist zyklisch der Ordnung $\frac{q^n-1}{q-1}$.*
4. *Es gilt $Z_0 = K_0 \cap Z$.*

5. $\overline{K} := K/Z$ *operiert scharf transitiv auf* $PG(\mathbb{F}_q^n)$ *und somit operiert* $\overline{K_0} := K_0/Z_0$ *regulär auf* $PG(\mathbb{F}_q^n)$*, wobei* $PG(\mathbb{F}_q^n)$ *der projektive Raum von* $\mathbb{F}_q^n$ *ist.*

Beweis. 1. Sei $\mathbb{F}_{q^n}^* =< \sigma >$, so ist folgende Abbildung ein $\mathbb{F}_q-$Vektorraumautomorphismus

$$\tilde{T}_\sigma : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n};\ a \longmapsto \sigma \cdot a.$$

Somit gibt es einen $\mathbb{F}_q-$Vektorraumautomorphismus

$$T_\sigma : \mathbb{F}_q^n \cong \mathbb{F}_{q^n} \xrightarrow{\cong} \mathbb{F}_{q^n} \cong \mathbb{F}_q^n.$$

Für die Ordnung von T_σ gilt nun

$$ord_{GL_n(q)}(T_\sigma) = \mathrm{ord}_{\mathbb{F}_{q^n}^*}(\sigma) = |\mathbb{F}_{q^n}^*| = q^n - 1.$$

Setze $K :=< T_\sigma >$.
Nun zum Zentralisator:
Da K zyklisch ist, gilt $K \subseteq C_G(K)$.
Sei $m := |\mathbb{F}_q^n \setminus \{0\}| = q^n - 1$ und bette $GL_n(q)$ in S_m ein, d.h. es gilt

$$K \subseteq GL_n(q) \subseteq S_m.$$

Sei $v_1 \in \mathbb{F}_q^n \setminus \{0\}$ und $C \in C_{S_m}(K)$ mit $C(v_1) = v_1$, so gilt

$$\begin{aligned} &\forall v \in \mathbb{F}_q^n \setminus \{0\}\ \exists A \in K :\ A(v_1) = v \\ &\Rightarrow C(v) = CA(v_1) = AC(v_1) = A(v_1) = v \\ &\Rightarrow C = 1 \end{aligned}$$

Also ist

$$|C_{GL_n(q)}(K)| \leq |C_{S_m}(K)| = [C_{S_m}(K) : stab_{C_{S_m}(K)}(v_1)] = |C_{S_m}(K) \bullet v_1| \leq |\mathbb{F}_q^n \setminus \{0\}| = q^n - 1 = |K|$$

Insegesamt gilt somit $C_{Gl_n(q)}(K) = K$.

2. Es gilt $Z_0 := Z \cap S \cong \{\lambda \in \mathbb{F}_q^* | \lambda^n = 1\} \leq \mathbb{F}_q^* =< \sigma >$. Somit ist Z_0 zyklisch mit $ord(Z_0)|n$ und $ord(Z_0)|q-1$.
Sei nun $d \cdot b = q - 1$, so erfüllt das Element σ^b die nötigen Voraussetzungen, d.h. $Z_0 =< \sigma^b >$.

3. $K_0 \leq K$ und ist somit zyklisch.
Die $\mathbb{F}_q-$lineare Abbildung $\tilde{T}_\sigma(x) = \sigma \cdot x\ \forall x \in \mathbb{F}_{q^n}$ hat den Eigenwert σ. So sind auch alle Konjugierten $\sigma, \sigma^q, ..., \sigma^{q(n-1)}$ von σ über $\mathbb{F}_q$ Eigenwerte von $\tilde{T}_\sigma$. Da sie paarweise verschieden sind, sind sie sämtliche Eigenwerte von $\tilde{T}_\sigma$.
Also ist $\det(T_\sigma) = \sigma^{\frac{q^n-1}{q-1}}$, woraus $K_0 =< T_\sigma^{q-1} >$ folgt.

4.

$$\begin{aligned} &C_{GL_n(q)}(K) = K \Rightarrow Z \cap S \subseteq K \\ \Rightarrow &K_0 \cap Z = K \cap S \cap Z = Z \cap S = Z_0 \end{aligned}$$

5. $\overline{K} = K/Z$ operiert scharf transitiv auf $PG(\mathbb{F}_q^n)$, somit ist

$$\overline{K_0} = K_0/Z_0 = (K \cap S)/(K \cap S \cap Z) \cong (K \cap S)Z/Z \leq KZ/Z = K/Z = \overline{K}$$

jeder Punktstabilisator trivial.

□

Satz 22. *Sei* $n \geq 2$ *und* q *eine Primzahlpotenz, sodass* $ggt(n, q-1) \in \{1, 4\}$ *oder* $ggt(n, q-1) = p$ *gilt, wobei* p *eine Primzahl ist. So besitzt die* $PSL_n(q)$ *eine MLS.*

Beweis. Sei $v \in \mathbb{F}_q^n \setminus \{0\}$ und $H_v := stab_{GL_n(q)}(v)$. So haben die Elemente von H_v bei einer geeigneten Wahl einer Basis die Form $\begin{pmatrix} 1 & 0 & \dots & 0 \\ \alpha_2 & & & \\ \vdots & & A_1 & \\ \alpha_n & & & \end{pmatrix}$, wobei $A_1 \in GL_n(q)$ und $\alpha_i \in \mathbb{F}_q$ $(2 \leq i \leq n)$ sind.
Somit ist

$$H := stab_{GL_n(q)}(< v >) = \{ \begin{pmatrix} \alpha_1 & 0 & \dots & 0 \\ \alpha_2 & & & \\ \vdots & & A_1 & \\ \alpha_n & & & \end{pmatrix} | A_1 \in GL_n(q),\ \alpha_i \in \mathbb{F}_q\ (1 \leq i \leq n),\ \alpha_1 \neq 0\}$$

der Stabilisator des 1-dimensionalen Unterraums $< v >$.
Betrachte die folgende Abbildung

$$\phi : H_v \longrightarrow GL_{n-1}(q); \begin{pmatrix} 1 & 0 & \dots & 0 \\ \alpha_2 & & & \\ \vdots & & A_1 & \\ \alpha_n & & & \end{pmatrix} \longmapsto A_1.$$

ϕ ist ein Epimorphismus mit

$$Q := Ker(\phi) \cong \mathbb{F}_q^{n-1},$$

also ist Q eine abelsche Gruppe der Ordnung q^{n-1}, die eine MLS besitzt.
Sei

$$L := \{ \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{pmatrix} | A_1 \in GL_n(q)\} \leq H_v \leq H$$

und somit gilt $L \cong GL_{n-1}(q)$ und $H_v = Q \rtimes L$, also auch $H = Z \times (Q \rtimes L)$, denn

$$Z \cap (Q \rtimes L) = Z \cap H_v = 1 \text{ und } |H| = |Z| \cdot |Q \rtimes L| = |\mathbb{F}_q^*| \cdot |H_v|.$$

Außerdem gilt

$$H_0 := H \cap S = Q \rtimes L_0$$

mit $L_0 := (Z \times L) \cap S \cong GL_{n-1}(q)$ und $\overline{H_0} = H_0/Z_0 \cong Q' \rtimes L_0/Z_0$, wobei $Q' \cong Q$ gilt.
Q und L_0 besitzen eine MLS, somit auch L_0/Z_0 und schließlich auch $\overline{H_0} \cong Q \rtimes L_0/Z_0$.
Da $\overline{K_0}$ zyklisch ist, besitzt es eine MLS.
Aufgrund des Lemmas 21(5) gilt nun $\overline{H_0} \cap \overline{K_0}^g = 1\ \forall g \in PSL_n(q)$.
Nun lässt sich die MDCD-Methode anwenden, vorausgesetzt $\tilde{n}$ ist 1,4 oder eine Primzahl, wobei $|PSL_n(q)| = \tilde{n}|H||K|$. Diese Voraussetzung ist erfüllt, denn:

$$|\overline{H_0K_0}| = |\overline{H_0}| \cdot |\overline{K_0}| = \frac{q^{n-1}|GL_{n-1}(q)|}{d} \cdot \frac{q^n - 1}{d(q-1)} = \frac{|GL_n(q)|}{(q-1)d^2} = \frac{|PSL_n(q)|}{d}.$$

□

Korollar 23. *Die $SL_n(q)$ besitzt eine MLS.*

Beweis. Da die Gruppe $Z_0 := Z(SL_n(q))$ zyklisch ist, besitzt sie eine MLS. So folgt aus dem obigen Satz zusammen mit Lemma 18 die Behauptung. □

Korollar 24. *Für $n \in \{4, p\}$, wobei p eine Primzahl ist, besitzen die $PSL_n(q)$ und die $SL_n(q)$ eine MLS.*

Bei näherer Untersuchung einfacher Gruppen stellt man fest, dass die MDCD-Methode für einige wenige Gruppen mit Ordnung $\leq 10^{10}$ nicht anwendbar ist, da sie die Voraussetzungen nicht erfüllen. Betrachte dazu folgendes Beispiel:

Dritte Janko Gruppe

Sei $G = J_3$ die dritte Janko Gruppe und es gilt $|G| = 50232960 = 2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$. Gesucht sind nun zwei Untergruppen H und K, die die Voraussetzungen der MDCD-Methode erfüllen, d.h. für die gilt

$$H \cap gKg^{-1} = 1 \ \forall g \in G \tag{1}$$

$$G = \bigcup_{i=1}^{n} Hg_iK, \tag{2}$$

wobei $n \in \{1, 4, p\}$ mit p eine Primzahl ist.
Nehme man nun an, dass solche H und K existieren, so gilt aufgrund der Eigenschaften (1) und (2), dass $|H|$ oder $|K|$ gerade ist. O.B.d.A. sei $|H|$ gerade. Aus den Sylowsätzen kann man nun folgen, dass in H mindestens ein Element der Ordnung 2 existieren muss. Da die J_3 lediglich eine Konjugationsklasse von Involutionen besitzt und die Eigenschaft (1) gilt, muss $|K|$ ungerade sein, denn angenommen K sei gerade, so gilt

$$\begin{aligned} &\exists k \in K : \mathrm{ord}(k) = 2 \\ \Rightarrow &\exists g \in G, h \in H : g^{-1}kg = h, \end{aligned}$$

was ein Widerspruch zu Eigenschaft (1) wäre.
Somit gilt $2^5 \mid |H|$.
Bezeichne mit M die maximale Untergruppe von G, die H enthält und betrachte folgende Fälle:

1. $\underline{|H|_2 = 2^5}$

   $$|H|_2 = 2^5 \quad \Rightarrow \quad n = 4 \quad \Rightarrow \quad |K| \mid 3^5 \cdot 5 \cdot 17 \cdot 19$$

   Somit ergeben sich folgende mögliche Isomorphien

   $$\Rightarrow H \leq M \cong 2^4 : (3 \times A_5), 2^{1+4} : A_5, 2^{2+4} : (3 \times S_3), L_2(16) : 2.$$

   Die Gruppenordnungen lauten

   $$\begin{aligned} |2^4 : (3 \times A_5)| &= 2^4 \cdot 3 \cdot 5 \cdot 2^2 \cdot 3, \\ |2^{1+4} : A_5| &= 2^5 \cdot 5 \cdot 2^2 \cdot 3, \\ |2^{2+4} : (3 \times S_3)| &= 2^6 \cdot 3 \cdot 3 \cdot 2, \\ |L_2(16) : 2| &= 15 \cdot 16 \cdot 17 \cdot 2. \end{aligned}$$

   Also gilt $19, 3^3 \mid |K|$, was ein Widerspruch ist, da es keine maximale Untergruppe mit dieser Eigenschaft gibt.

2. $\underline{|H|_2 = 2^6}$
   In diesem Fall ist $n = 2$. Dies läuft analog zum Fall $|H|_2 = 2^5$.

3. $\underline{|H|_2 = 2^7}$ Sei $p > 2$ eine Primzahl.

   $$\Rightarrow n \in \{1, p\} \quad \Rightarrow \quad |K| \mid 3^5 \cdot 5 \cdot 17 \cdot 19$$

   Somit ergeben sich folgende mögliche Isomorphien

   $$\Rightarrow H \leq M \cong 2^{1+4} : A_5, 2^{2+4} : (3 \times S_3),$$

   woraus $17, 19, 3^2 \mid |K|$ folgt, was ein Widerspruch ist, denn es eistiert keine maximale Untergruppe mit dieser Eigenschaft.

Folglich existieren keine Gruppen H und K, die die Bedingungen (1) und (2) erfüllen.

"Glueing-method"

Wie bereits erwähnt greift die MDCD-Methode nicht für alle einfachen Gruppen der Ordnung $\leq 10^{10}$. Diese Fälle kann man mit der sogenannten "glueing-method"behandeln. Dazu betrachte konkret folgendes Beispiel:

$\underline{G := A_6}$

$$H :=< (12345), (123) > \cong A_5 \text{ maximale Untergruppe in G}$$
$$K :=< (12345), (14)(56) > \cong A_5 \text{ maximale Untergruppe in G}$$
$$\Rightarrow G = H.K \text{ und } W := H \cap K \cong D_{10} \neq 1$$

Nun existieren $X \leq H$ und $Y \leq K$ mit jeweils Ordnung 3, so besitzen sie eine MLS, die mit α_X bzw. α_Y bezeichnet wird. Auch W besitzt eine MLS, da D_{10} auflösbar ist.
Also bekommen wir mit Hilfe der MDCD-Methode mit dem Paar (W,X) eine MLS für H der Form

$$\alpha_H := \alpha_X \cup \{1, h\} \cup \alpha_W$$

und mit dem Paar (W,Y) erhält man eine MLS für K der Form

$$\alpha_K := \alpha_W \cup \{1, k\} \cup \alpha_Y.$$

Nun "verklebt"('*glueing*') man die MLS und erhält schließlich

$$\alpha_G = \alpha_X \cup \{1, h\} \cup \alpha_W \cup \{1, k\} \cup \alpha_Y$$

eine MLS für G.