Lügner und die Gruppe $(\mathbb{Z}_2)^n$

Ehrhard Behrends

Bei manchen Zauberkunststücken sollen durch den Zuschauer ja-nein-Fragen beantwortet werden, um unauffällig an Informationen zu kommen („Liegt die gewählte Karte in dieser Reihe?“). Da braucht man n Fragen, um ein bestimmtes Objekt aus 2^n möglichen Kandidaten zu identifizieren. In einigen Varianten kann sich der Zuschauer vorher entscheiden, ob er immer die Wahrheit sagen wird oder immer lügen wird. Dann gilt die Faustregel: Braucht man n Fragen bei jemandem, der immer die Wahrheit sagt, so sind in der Variante „Wahrheit sagen oder lügen?“ $n+1$ Fragen erforderlich. Das ist plausibel, denn man kann ja durch die Antwort auf eine einzige Frage feststellen, ob man es mit einem Lügner zu tun hat oder nicht („Ist diese Wand weiß?“). Die Kunst besteht darin, das gleiche Ziel durch weniger offensichtliche Fragen zu erreichen.

Auf einen neuen Aspekt wurde ich durch ein Buch des Zauberers Werner Miller ([4]) aufmerksam. Diesmal werden Eigenschaften von Zahlen ausgenutzt. Um das Wesentliche herauszuarbeiten, beschreiben wir hier eine etwas vereinfachte Version von Millers Idee.

Der Zuschauer wählt in Gedanken eine der Zahlen $2, 3, \ldots, 10$, entscheidet sich, ob er immer lügen oder immer die Wahrheit sagen wird, und dann beantwortet er die folgenden fünf Fragen (immer richtig oder immer falsch):

Frage 1: Hast Du an eine der Zahlen $2, 6$ gedacht?
Frage 2: Hast Du an eine der Zahlen $3, 8, 10$ gedacht?
Frage 3: Hast Du an eine der Zahlen $4, 6, 9$ gedacht?
Frage 4: Hast Du an eine der Zahlen $5, 8, 9$ gedacht?
Frage 5: Hast Du an eine der Zahlen $7, 10$ gedacht?

Und dann kann die Zauberin sagen, welche Zahl gewählt wurde und ob sich der Zuschauer für das Lügen oder dagegen entschieden hatte.

Und wie geht das? Die Zauberin wichtet die Fragen 1, 2, 3, 4 bzw. 5 mit 2,3,4,5 bzw. 7 Punkten und addiert die Punkte zu den mit „ja“ beantworteten Fragen: Das Ergebnis sei z. (Gab es etwa ein „ja“ bei den Fragen 2, 4, und 5, so erhält sie $z = 3 + 5 + 7 = 15$ Punkte.) Und dann gilt:

- Ist die Punktezahl z kleiner als 11, so hat der Zuschauer an z gedacht und immer die Wahrheit gesagt.
- Andernfalls hat er sich für das Lügen entschieden, und er hatte sich die Zahl $21 - z$ ausgesucht.

Im vorstehenden Beispiel mit $z = 15$ hatte man es also mit einem Lügner zu tun, der zu Beginn die $21 - 15 = 6$ gewählt hatte.

Und warum gilt das? Wir nehmen zunächst an, dass immer die Wahrheit gesagt wird. Dann kommt die gedachte Zahl z genau bei den Fragen vor, für die die mit $2, 3, 4, 5, 7$ gewichtete Summe zu den „ja“-Antworten z ergibt. Da $2 + 3 + 4 + 5 +$

$7 = 21$ ist, gilt: Wurde an z gedacht und immer gelogen, so wird die gewichtete Summe gleich $21 - z$ sein. Wichtig ist noch, dass die Zahlen $2, 3, \ldots, 10$ durch die richtig beantworteten Fragen rekonstruiert werden können und dass folglich, wie eben begründet, im Lügner-Fall mit den Zahlen $21-2, 21-3, \ldots, 21-10$, also mit $19, 18, 17, \ldots, 11$ zu rechnen ist. Und da $\{2, 3, \ldots, 10\}$ und $\{11, 12, \ldots, 19\}$ disjunkt sind, sind stets Lügner und Nicht-Lügner zu unterscheiden, und man kann die Zahl z ermitteln.

Ziel der vorliegenden Arbeit ist das Studium einer Verallgemeinerung. Der Zuschauer wählt wieder in Gedanken ein Element aus einer vorgegebenen Menge, und dann werden ihm einige Fragen gestellt. Aber anders als „Immer lügen oder immer die Wahrheit sagen“ hat der Zuschauer viel mehr Möglichkeiten, etwa „Bei den 5 folgenden Fragen höchstens einmal lügen“. Trotzdem soll das gewählte Element von der Zauberin sicher identifiziert werden können.

Bemerkenswerter Weise führt das auf Eigenschaften der Gruppe $(\mathbb{Z}_2)^n$. Es ist wenig überraschend, dass mit größer werdender Anzahl der Zuschauermöglichkeiten die Menge der Zahlen, unter denen die Zauberin die gedachte ermittelt, kleiner wird. Wir werden das quantifizieren, und am Ende gibt es einige Anregungen für die Umsetzung der Ergebnisse in konkrete Zauberkunststücke.

1. Vorbereitungen

Wir beginnen mit einigen Bezeichnungen. Zunächst fixieren wir ein $n \in \mathbb{N}$, das wird die Anzahl der Fragen sein, die die Zauberin stellen wird. (Für die spätere Umsetzung in ein Zauberkunststück sollte n nicht allzu groß sein.)

Wir bezeichnen noch mit G_n die Gruppe $(\mathbb{Z}_2)^n$, die Elemente werden wir als $\varepsilon_1 \cdots \varepsilon_n$ mit $\varepsilon_i \in \{0, 1\}$ schreiben.

Nun beschreiben wir die Rohfassung unseres Zauberkunststücks. Die wird, zugegeben, noch recht technisch aussehen, aber später werden wir unsere Idee so verkleiden, dass der mathematische Hintergrund nicht zu erkennen ist.

Schritt 1: Wir betrachten eine nicht leere Teilmenge $\mathbb{A} \subset G_n$, die *Auswahlmenge*. Zur Illustration wählen wir $n = 4$ und $\mathbb{A} := \{0011, 0100, 1010, 1011, 1111\}$.
Die Idee: Der Zuschauer wählt in Gedanken ein Element $x \in \mathbb{A}$

Schritt 2: $\mathbb{A}$ induziert die n Teilmengen $F_1, \ldots, F_n \subset \mathbb{A}$, die *Fragemengen*. Für $i = 1, \ldots, n$ ist F_i durch

$$F_i := \{\varepsilon_1 \cdots \varepsilon_n \in \mathbb{A} \mid \varepsilon_i = 1\}$$

definiert. In unserem Beispiel ergibt sich:

$$F_1 = \{1010, 1011, 1111\}, F_2 = \{0100, 1111\},$$

$$F_3 = \{0011, 1010, 1011, 1111\}, F_4 = \{0011, 1011, 1111\}.$$

Die Idee: Es werden n Fragen gestellt, und die i-te Frage lautet „Liegt das gewählte Element in F_i ?“

Schritt 3: Bei den Antworten hat der Zuschauer die Möglichkeit zu lügen. Genauer: Eine nicht leere Teilmenge $\mathbb{L} \subset G_n$, die *Lügnermenge*, ist vorgegeben, und der Zuschauer wählt heimlich irgendein $\lambda = \lambda_1 \cdots \lambda_n \in \mathbb{L}$. Die Zauberin kennt $\mathbb{L}$, aber sie weiß nicht, welches $\lambda \in \mathbb{L}$ gewählt wurde[1]. Der Zuschauer muss sich an die folgende Regel halten: Ist, für $i = 1, \ldots, n$, das $\lambda_i = 0$, so muss die Frage „$x \in F_i$?“ wahrheitsgemäß beantwortet werden, und im Fall $\lambda_i = 1$ muss gelogen werden.

Zur Illustration nehmen wir in unserem Beispiel einmal an, dass sich der Zuschauer in $\mathbb{A}$ für das Element $x = 1010$ und unter den Lügnerszenarien $\mathbb{L} = \{0110, 1001\}$ für $\lambda_1\lambda_2\lambda_3\lambda_4 = 0110 \in \mathbb{L}$ entschieden hat: Lügen bei der zweiten und der dritten Frage. Dann passiert doch folgendes:

- Es ist $x \in F_1$ und $\lambda_1 = 0$. Der Zuschauer muss „ja“ sagen.
- Es ist $x \notin F_2$ und $\lambda_2 = 1$. Der Zuschauer antwortet wieder „ja“.
- Es ist $x \in F_3$ und $\lambda_3 = 1$. Die Antwort ist diesmal „nein“.
- Es ist $x \notin F_4$ und $\lambda_4 = 0$. Noch einmal ist die Antwort „nein“.

Die Zauberin hat sich Notizen gemacht, sie hat für „ja“ bzw. „nein“ jeweils 1 bzw. 0 aufgeschrieben: Ihr Ergebnis ist also 1100. Bemerkenswerter Weise ist $1010 + 0110 = 1100$ in der Gruppe G_4, und eine entsprechende Formel gilt – wie wir gleich sehen werden – bei beliebiger Wahl von $\mathbb{A}$, x und λ. Es ist überraschend, dass man „Auswahl“ und „Lüge“ miteinander sinnvoll verknüpfen kann.

Diese Tatsache wird die Grundlage dafür sein, dass gruppentheoretische Eigenschaften von G_n hier eine wichtige Rolle spielen werden:

1.1 Satz: *Wir nehmen an, dass sich der Zuschauer aus $\mathbb{A}$ das Element $x = \varepsilon_1 \cdots \varepsilon_n$ gemerkt und sich unter den Elementen aus $\mathbb{L}$ für $\lambda_1 \cdots \lambda_n$ entschieden hat. Er beantwortet für $i = 1, \ldots, n$ die Frage F_i so, wie in den Spielregeln vorgesehen, und die Zauberin notiert die Antwort als ν_i (mit $\nu_i = 0$ für ein „nein“ und $\nu_i = 1$ für ein „ja“).*

Dann ist $\nu_1 \cdots \nu_n = \varepsilon_1 \cdots \varepsilon_n + \lambda_1 \cdots \lambda_n$ in G_n.

Beweis: Es gibt für jedes i die 4 Möglichkeiten $\varepsilon_i = 0, 1$ und $\lambda_i = 0, 1$. Mal angenommen, es ist zum Beispiel $\varepsilon_i = 0$ und $\lambda_i = 1$. Dann gehört x *nicht* zu F_i und es wird gelogen. Die Zauberin notiert also $\nu_i = 1$. Und wirklich ist $0 + 1 = 1$ in $\mathbb{Z}_2$. Die anderen drei Möglichkeiten können genauso analysiert werden. □

Die Zauberin hat nun eine Tabelle vorbereitet, in der alle $\varepsilon_1 \cdots \varepsilon_4 + \lambda_1 \cdots \lambda_4$ für $\varepsilon_1 \cdots \varepsilon_4 \in \mathbb{A}$ und $\lambda_1 \cdots \lambda_4 \in \mathbb{L}$ enthalten sind. Links stehen die Elemente $x \in \mathbb{A}$, oben die $\lambda \in \mathbb{L}$, und die zu x gehörige Zeile enthält die $x + \lambda$ für alle λ:

[1] Jedenfalls, wenn $\mathbb{L}$ mehr als ein Element enthält.

	0110	1001
0011	0101	1010
0100	0010	1101
1010	1100	0011
1011	1101	0010
1111	1001	0110

Sie hat Glück gehabt: 1100 taucht nur einmal auf! Und deswegen weiß sie sicher, dass 1010 gewählt und gemäß 0110 geantwortet wurde. Das hätte bei „Wahl 0100 und Szenario 0110“ anders ausgesehen, diese Situation ist von „1011 gewählt, gemäß 1001 geantwortet“ nicht zu unterscheiden, denn beide führen zu 0010[2].

Das motiviert die folgende Definition. *So* sollen Situationen aussehen, in denen der Zauberin nichts passieren kann:

1.2 Definition: *Sei $(G,+)$ eine abelsche Gruppe, und $\mathbb{A},\mathbb{L}\subset G$. Das Paar $(\mathbb{A},\mathbb{L})$ heißt* zulässig, *wenn die Elemente in $\mathbb{A}+\mathbb{L}:=\{x+y\mid x\in\mathbb{A},y\in\mathbb{L}\}$ paarweise verschieden sind.*

Uns wird diese Definition praktisch nur im Fall $G=G_n$ interessieren. Um illustrieren zu können, dass einige Ergebnisse im Zusammenhang mit diesem Begriff nur dort gelten, haben wir aber auch allgemeinere Gruppen zugelassen.

Ohne Beweis stellen wir einige offensichtliche Ergebnisse zusammen:

1.3 Lemma: *Es seien $\mathbb{A},\mathbb{L}$ Teilmengen der kommutativen Gruppe G.*

(i) Ist $(\mathbb{A},\mathbb{L})$ zulässig, so auch $(\mathbb{L},\mathbb{A})$.

(ii) Ist $\mathbb{A}$ oder $\mathbb{L}$ einelementig, so ist $(\mathbb{A},\mathbb{L})$ zulässig.

(iii) Ist $(\mathbb{A},\mathbb{L})$ zulässig, so auch $(\mathbb{A}',\mathbb{L}')$ für $\mathbb{A}'\subset\mathbb{A}$ und $\mathbb{L}'\subset\mathbb{L}$.

(iv) Wenn $(\mathbb{A},\mathbb{L})$ zulässig ist, so gilt $\sharp\mathbb{A}\sharp\mathbb{L}\leq\sharp G$. (Dabei bezeichnet $\sharp M$ die Anzahl der Elemente einer Menge M.)

Wir wollen nun analysieren, welche optimale Strategie man der Zauberin empfehlen kann. Es gibt zwei naheliegende Fragestellungen:

- Man könnte $\mathbb{L}$ vorgeben und sich fragen, welche $\mathbb{A}$ möglich sind, so dass $(\mathbb{A},\mathbb{L})$ zulässig ist. Natürlich wäre es wünschenswert, dass $\mathbb{A}$ dann „möglichst groß“ ist.
- Man könnte auch $\mathbb{A}$ vorgeben und möglichst große $\mathbb{L}$ zu suchen.

Dabei reicht es wegen Lemma 1.3(i), sich auf eine der Fragen zu konzentrieren.

2. Zulässige Paare

2.1 Definition: *Sei G eine endliche kommutative Gruppe und $\mathbb{L}\subset G$. Dann bezeichnen wir mit $\alpha(\mathbb{L})$ das Maximum der Zahlen k, für die es eine k-elementige Menge $\mathbb{A}\subset G$ so gibt, dass $(\mathbb{A},\mathbb{L})$ zulässig ist.*

[2] Übrigens kommt auch 1101 zweimal vor.

Die Zauberin sucht sich also $\mathbb{L}$ aus und möchte die Auswahl $\mathbb{A}$ für den Zuschauer möglichst reichhaltig gestalten: Mit $\alpha(\mathbb{L})$ Elementen kann sie bei geschickter Wahl von $\mathbb{A}$ rechnen.

Hier sind zunächst einige erste Ergebnisse für beliebige $(G,+)$.

2.2 Satz: *Sei $\mathbb{L} \subset G$.*

(i) $\alpha(\mathbb{L}) = \alpha(x+\mathbb{L})$ für jedes $x \in G$.

(ii) Ist $\mathbb{L}$ einelementig, so ist $\alpha(\mathbb{L}) = \sharp G$.

(iii) Bezeichne mit $<\mathbb{L}>$ die von $\mathbb{L}$ erzeugte Untergruppe Dann ist $\alpha(\mathbb{L})$ mindestens so groß wie die Anzahl der Elemente in der Quotientengruppe $G/<\mathbb{L}>$.

(iv) Es kann vorkommen, dass $\alpha(\mathbb{L})$ echt größer als $\sharp(G/<\mathbb{L}>)$ ist.

(v) Sei $\mathbb{L}^* := \{x-y \mid x,y \in \mathbb{L}\}$. Es ist genau dann $\alpha(\mathbb{L}) > 1$, wenn $\mathbb{L}^*$ eine echte Teilmenge von G ist.

(vi) Wir nehmen an, dass $\mathbb{L}^*$ eine echte Teilmenge von G ist, und wir setzen $\mathbb{L}^{**} := G \setminus \mathbb{L}^*$. Definiert man dann $\kappa(\mathbb{L})$ als das Maximum der Zahlen l, so dass es verschiedene $z_1,\ldots,z_l$ in $\mathbb{L}^{**}$ so gibt, dass alle $z_i - z_j$ für $i \neq j$ zu $\mathbb{L}^{**}$ gehören, so ist $\alpha(\mathbb{L}) = 1+\kappa(\mathbb{L})$.

Beweis: (i), (ii) Das ist klar.

(iii) Sei zunächst $\mathbb{L}$ eine Untergruppe und $k := \sharp(G/\mathbb{L})$. Wir wählen ein Repräsentantensystem $x_1,\ldots,x_k$ zu den zu $\mathbb{L}$ gehörigen Nebenklassen. Es ist dann G die disjunkte Vereinigung der $x_i+\mathbb{L}$, und das beweist $\alpha(\mathbb{L}) = k$. Falls $\mathbb{L}$ eine echte Teilmenge von $<\mathbb{L}>$ ist, suche $x_1,\ldots,x_k$ zu $<\mathbb{L}>$. Es ist dann $(\{x_1,\ldots,x_k\},\mathbb{L})$ zulässig.

(iv) Betrachte in $\mathbb{Z}_4$ die Menge $\mathbb{L} = \{0,1\}$. Es ist $<\mathbb{L}> = \mathbb{Z}_4$, aber $(\{0,2\},\mathbb{L})$ ist zulässig, so dass $\alpha(\mathbb{L}) = 2$.

(v) Wenn $\alpha(\mathbb{L}) > 1$ gilt, gibt es y_1,y_2, so dass $y_1+\mathbb{L}$ und $y_2+\mathbb{L}$ disjunkt sind. Mit $y := y_1-y_2$ sind dann auch $y+\mathbb{L}$ und $\mathbb{L}$ disjunkt. Für $x,x' \in \mathbb{L}$ ist also $y+x \neq x'$, und das bedeutet $y \notin \mathbb{L}^*$. Ist umgekehrt $y \notin \mathbb{L}^*$, so sind $y+\mathbb{L}$ und $\mathbb{L}$ disjunkt, d.h. $\alpha(\mathbb{L}) > 1$.

(vi) Mal angenommen, das Paar $(\{y_1,\ldots,y_r\},\mathbb{L})$ ist zulässig, dann ist auch das Paar $(\{0,z_1,\ldots,z_{r-1}\},\mathbb{L})$ zulässig, wo $z_i := y_{i+1}-y_1$. Die Mengen $\mathbb{L}, z_1+\mathbb{L},\ldots,z_{r-1}+\mathbb{L}$ sind also paarweise disjunkt. Insbesondere ist jedes $z_i+\mathbb{L}$ zu $\mathbb{L}$ disjunkt, d.h. $z_i \in \mathbb{L}^{**}$. Und $(z_i+\mathbb{L})\cap(z_j+\mathbb{L}) = \emptyset$ impliziert $z_i-z_j \notin \mathbb{L}^*$. Das zeigt $\kappa(\mathbb{L}) \geq \alpha(\mathbb{L})-1$. Die Ungleichung „$\leq$“ wird analog bewiesen. □

Es ist etwas überraschend, dass man für den Spezialfall $G = G_n$ wesentlich detailliertere Aussagen beweisen kann. Dabei wird mehrfach eine Rolle spielen, dass $x+x = 0$ für alle $x \in G_n$ gilt.

2.3 Satz: *Sei $n \in \mathbb{N}$ und $\mathbb{L} \subset G_n$.*

(i) Ist $\mathbb{L}$ zweielementig, so ist $\alpha(\mathbb{L}) = 2^{n-1}$.

(ii) Ist $\mathbb{L}$ dreielementig, so ist $\alpha(\mathbb{L}) = 2^{n-2}$.

(iii) Ist $\mathbb{L}$ vierelementig, so ist $\alpha(\mathbb{L}) = 2^{n-2}$.

(iv) Für jedes $k < n$ gibt es 2^k-elementige $\mathbb{L}$ mit $\alpha(\mathbb{L}) = 2^{n-k}$.

(v) Sei $2^{n-2} < \sharp\mathbb{L}$. Dann ist $\alpha(\mathbb{L}) \leq 2$.

Beweis: (i) $\mathbb{L}$ sei zweielementig. Wegen Satz 2.2(i) dürfen wir annehmen, dass $0 \in \mathbb{L}$. Damit hat $\mathbb{L}$ die Form $\{0, x\}$ mit einem $x \neq 0$, es handelt sich (wegen $x + x = 0$) also um eine zweielementige Untergruppe. Nun ist noch Satz 2.2(iii) anzuwenden.

(ii) O.B.d.A. ist $\mathbb{L} = \{0, x, x'\}$ mit $x \neq 0 \neq x' \neq x$. Es ist dann $<\mathbb{L}> = \{0, x, x', x + x'\}$, und das zeigt wegen Satz 2.2.(ii) schon $\alpha(\mathbb{L}) \geq \sharp(G_n/<\mathbb{L}>) = 2^{n-2}$.

Nun sei y vorgelegt, so dass $(y+\mathbb{L})\cap\mathbb{L} = \emptyset$. Dann ist auch $(y+<\mathbb{L}>)\cap<\mathbb{L}> = \emptyset$. Angenommen nämlich, das wäre nicht der Fall, etwa $y + x = x + x'$. Es würde der Widerspruch $y = x'$ folgen. Was wäre, wenn $x = y + (x + x')$? Dann folgt $y = x'$, diesmal wird die Gleichung $x' + x' = 0$ wichtig. Ganz analog kann man die anderen Möglichkeiten ausschließen, und so haben wir $\alpha(\mathbb{L}) = \alpha(<\mathbb{L}>)$ gezeigt.

(iii) Das ist klar, man kann $\mathbb{L}$ einfach als 2^k-elementige Untergruppe wählen.

(iv) O.B.d.A. ist $\mathbb{L} = \{0, x, x', x''\}$ mit paarweise verschiedenen und von 0 verschiedenen x, x', x''. Wir betrachten $<\mathbb{L}>$, also die Menge

$$\{0, x, x', x'', x + x', x + x'', x + x'', x + x' + x''\}.$$

Die Ordnung einer Untergruppe teilt die Gruppenordnung, und deswegen hat $<\mathbb{L}>$ 4 oder 8 Elemente.
Fall 1: $\sharp<\mathbb{L}> = 4$. Dann folgt die Aussage aus Satz 2.2(iii).
Fall 2: $\sharp<\mathbb{L}> = 8$. Wähle 2^{n-3} disjunkte Translationen von $<\mathbb{L}>$ In jeder dieser Translationen gibt es zwei disjunkte Translationen von $\mathbb{L}$, denn wegen $\sharp<\mathbb{L}> = 8$ sind $\mathbb{L}$ und $x + x' + x'' + \mathbb{L}$ disjunkt. Insgesamt erhalten wir so 2^{n-2} disjunkte Translationen.

(v) Angenommen, es wäre $\alpha(\mathbb{L}) \geq 3$. Dann gäbe es eine dreielementige Menge $\mathbb{A}$, so dass $(\mathbb{A}, \mathbb{L})$ zulässig sind. Wegen (ii) könnte $\mathbb{L}$ höchstens 2^{n-2} Elemente haben, hier nutzen wir die Symmetrie des Begriffs „zulässig“ aus. Das widerspricht der Voraussetzung. □

Die Aussage (v) ist aus Sicht der Zauberin etwas enttäuschend. Mal angenommen, sie hat sich im Fall $n = 4$ für ein 5-elementiges $\mathbb{L}$ entschieden. Wegen $3\cdot5 \leq 2^4$ und Lemma 1.3(iv) könnte sie hoffen, ein dreielementiges $\mathbb{A}$ so zu finden, dass $(\mathbb{A}, \mathbb{L})$ zulässig ist. So etwas gibt es aber im Fall der Gruppe G_4 nicht, denn $5 > 2^2$. (In anderen Gruppen geht es: Auch $\mathbb{Z}_{16}$ hat 16 Elemente, und offensichtlich ist $\alpha(\{0, 1, 2\}) = 5$.)

Wir diskutieren noch kurz Empfehlungen für die Zauberin, wenn sie bereit ist, auf Risiko zu spielen. Genauer soll das folgendes bedeuten. Sie möchte unbedingt mit einer festen Menge $\mathbb{L}$ arbeiten, aber es gibt keine „großen“ $\mathbb{A}$, so dass $(\mathbb{A}, \mathbb{L})$ zulässig ist. Vielleicht gibt es aber ein „großes“ $\mathbb{A}$, so dass die Anzahl der Elemente in $\mathbb{A} + \mathbb{L}$ nicht weit von $\sharp\mathbb{A} \cdot \sharp\mathbb{L}$ entfernt ist. Dann wird es in den meisten Fällen möglich sein, aus den Antworten des Zuschauers auf des gewählte $x \in \mathbb{A}$ und das verwendete Lügenszenario $\lambda \in \mathbb{L}$ zu schließen. Wir definieren:

2.4 Definition: *Sei $\mathbb{L} \subset G$ und $k \in \mathbb{N}$. Dann soll $\beta(\mathbb{L}, k)$ die Maximalzahl der $\sharp(\mathbb{A} + \mathbb{L})$ sein, wenn $\mathbb{A}$ alle k-elementigen Teilmengen von G durchläuft.*

Einige Aussagen sind offensichtlich, etwa „Ist $k \leq \alpha(\mathbb{L})$, so ist $\beta(\mathbb{L}, k) = k \cdot \sharp\mathbb{L}$ “. Wir wollen das nicht systematisch studieren, sondern nur auf ein Ergebnis hinweisen, dass für die Zauberin vielleicht interessant sein könnte:

2.5 Satz: *Es sei $\mathbb{L}$ eine 8-elementige Teilmenge von G_4. Dann ist $\beta(\mathbb{L}, 2) \in \{14, 16\}$. Anders ausgedrückt: Ist $\mathbb{L} \subset G_4$ mit $\sharp\mathbb{L} = 8$ beliebig, so gibt es ein zweielementiges $\mathbb{A}$, so dass $(\mathbb{A}, \mathbb{L})$ zulässig ist oder doch mindestens ein zweielementiges $\mathbb{A}$, für das $\mathbb{A}+\mathbb{L}$ 14 Elemente hat. Das Risiko, dass der Zaubertrick bei Verwendung von diesem $\mathbb{A}$ nicht klappt, ist also sehr gering.*

Beweis: Wir betrachten die Menge $\mathbb{L}^* := \{x + x' \mid x, x' \in \mathbb{L}\}$.

Fall 1: $\mathbb{L}^*$ ist eine echte Teilmenge von G_4. Dann ist (wegen Satz 2.2(v)) $\alpha(\mathbb{L}) > 1$, d.h., man findet sogar ein $\mathbb{A}$, für das $\mathbb{A} + \mathbb{L}$ 16 Elemente hat.

Fall 2: $\mathbb{L}^* = G_4$. Dann ist $\sharp(\mathbb{A} + \mathbb{L}) = 16$ nicht erreichbar. Die $x + x'$ mit $x \neq x'$ stellen also alle Elemente aus G_4 außer der Null dar. Nun gibt es $8 \cdot 7 = 56$ Paare in $\mathbb{L}$ mit $x \neq x'$. Sortiere sie in disjunkte Klassen: $K_y := \{(x, x') \mid x, x' \in \mathbb{L}, x \neq x', x + x' = y\}$, wobei y alle Elemente in $G_4 \setminus \{0\}$ durchläuft. Jedes K_y ist nicht leer und enthält eine gerade Anzahl von Elementen. Es kann aber nicht jedes K_y mindestens 4-elementig sein, denn dann gäbe es mindestens $4 \cdot 15 = 60$ Paare, ein Widerspruch. Wähle also ein y so, dass $K_y = \{(x, x'), (x', x)\}$ zweielementig ist. Dann ist $(y + \mathbb{L}) \cap \mathbb{L} = \{x, x'\}$, es ist also $\sharp(\{0, y\} + \mathbb{L}) = 2 \cdot 8 - 2 = 14$. □

Zum Abschluss dieses Abschnitts gibt es noch einige Bemerkungen zum hier relevanten mathematischen Hintergrund. Die Zahl $\alpha(\mathbb{L})$ für Teilmengen $\mathbb{L}$ einer endlichen Gruppe scheint bisher noch nicht untersucht worden zu sein. Im Fall $G = (\mathbb{Z}_2)^n$ gibt es für einen Spezialfall allerdings einen Zusammenhang. Angenommen nämlich, $\mathbb{L}$ ist eine d-Kugel um den Nullpunkt in Bezug auf den Hammingabstand, d.h. $\mathbb{L}$ ist die Menge aller $\varepsilon_1 \cdots \varepsilon_n$, für die höchstens d der ε_i gleich 1 sind. Wenn dann $x + \mathbb{L}$ und $x' + \mathbb{L}$ disjunkt sind, so heißt das: Ein an höchstens d Stellen verändertes x kann von einem an höchstens d Stellen veränderten x' unterschieden werden. Die Maximalzahl der $x_1, \ldots, x_k$ mit disjunkten $x_1 + \mathbb{L}, \ldots, x_k + \mathbb{L}$ ist folglich interessant für die *Codierungstheorie*. Vergleiche das Kapitel Codes und Kugelpackungen in [5].

Die Frage nach der konkreten Berechnung von $\alpha(\mathbb{L})$ kann übrigens im Fall $G = G_n$ mit Hilfe von Satz 2.2(vi) auf ein Problem der *Graphentheorie* zurückgeführt werden. Wir nehmen an, dass $\mathbb{L}^{**}$ nicht leer ist. Unser Graph hat als Eckenmenge die Elemente aus $\mathbb{L}^{**}$, und eine Kante zwischen $z, z' \in \mathbb{L}^{**}$ mit $z \neq z'$ gibt es genau dann, wenn $z + z'$ zu $\mathbb{L}^{**}$ gehört. $\kappa(\mathbb{L}) = \alpha(\mathbb{L}) - 1$ ist dann wegen Satz 2.2(vi) das maximale l, für das es einen vollständigen Teilgraphen mit l Elementen gibt.

Das ist ein bekanntes Problem der Graphentheorie: das *Cliquenproblem*. Es gehört zu den den klassischen 21 NP-vollständigen Problemen der Komplexitätstheorie, vgl. [2][3].

Für große n ist die Berechnung fast aussichtslos, in den uns hier interessierenden Fällen mäßig großer n kann $\kappa(\mathbb{L})$ aber leicht mit Computerhilfe ermittelt werden.

[3] Das heißt noch nicht, dass die Bestimmung von $\kappa(\mathbb{L})$ NP-vollständig ist, da hier nur sehr spezielle Graphen auftreten.

Und schließlich ist noch auf den Zusammenhang zu *Differenzmengen* hinzuweisen, die in der *Kombinatorik* eine Rolle spielen. Vgl. Abschnitt X in [3]. Sie entsprechen optimal großen $\mathbb{L}$ mit $\alpha(\mathbb{L}) = 2$.

3. Zaubern!

Es ist nun an der Zeit, die Spuren zu verwischen und unsere Erkenntnisse für ein Zauberkunststück nutzbar zu machen. Betrachten wir als Beispiel den Fall $n = 5$ und nehmen wir an, dass wir das zulässige Paar $\mathbb{A} = \{00100, 11110, 10001, 10101, 11101, 01011, 00111, 01111\}$ und $\mathbb{L} = \{01000, 01110, 10011, 01111\}$ gefunden haben. Nach unserem bisherigen Kenntnisstand sähe es dann so aus: Die Fragemengen sind
$F_1 = \{11110, 10001, 10101, 11101\}$,
$F_2 = \{11110, 11101, 01011, 01111\}$,
$F_3 = \{00100, 11110, 11101, 00111, 01111\}$,
$F_4 = \{11110, 01011, 00111, 01111\}$,
$F_5 = \{10001, 10101, 11101, 01011, 00111, 01111\}$,
und die Matrix der Zauberin hätte die folgende Form:

	01000	01110	10011	01111
00100	01100	01010	10111	01011
11110	10110	10000	01101	10001
10001	11001	11111	00100	11110
10101	11101	11011	00110	11010
11101	10101	10011	01110	10010
01011	00011	00101	11000	00100
00111	00111	01001	10100	01000
01111	00111	00001	11100	00000

Das ist recht unübersichtlich und sieht verdächtig nach Mathematik aus. Zwei Änderungen beheben diese Probleme:

- Für die Elemente aus $\mathbb{A}$ wählen wir irgendwelche Symbole: Buchstaben, Zahlen, Tiernamen, Musikinstrumente, ... Hier wählen wir einfach die ersten Buchstaben des Alphabets: $A, B, C, \ldots$.
- Die Zauberin notiert nicht eine 0-1-Folge, sondern sie berechnet eine Zahl: eine 1 (d.h. ein „ja“) im ersten bzw. zweiten bzw. dritten bzw. vierten bzw. fünften Schritt zählt 1 bzw. 2 bzw. 4 bzw. 8 bzw. 16, und Nullen werden nicht berücksichtigt; diese Punkte werden dann addiert[4]. So führt etwa 11001 zu $1+2+0+0+16 = 19$. (Man beachte: 11001 ist die verkehrt herum gelesene Dualzahlentwicklung von 19.)

[4]Statt mit $1, 2, 4, 8, \ldots$ zu wichten, kann man auch a_i mit $0 < a_1 < \cdots < a_n$ verwenden, falls die Zahlen $\sum_{i\in\Delta} a_i$ für jede Teilmenge $\Delta \subset \{1, \ldots, n\}$ zu einem anderen Ergebnis führen. Die a_i können oft so gewählt werden, dass $a_n < 2^{n-1}$. Wie klein genau, ist schon für mäßig große n noch offen, es ist ein altes Problem von Erdös. Einige neuere Ergebnisse zu diesem Fragenkreis findet man in [1]. Wir werden hier bei der vertrauten Dualzahlentwicklung bleiben.

Das beseitigt für die Zuschauer jeden Verdacht von Mathematik, und es wird für die Zauberin viel übersichtlicher! Konkret: Die Auswahlmenge ist nun die Menge $\{A, B, C, D, E, F, G, H\}$, die Fragemengen sind
$F_1 = \{B, C, D, E\}$, $F_2 = \{B, E, F, H\}$, $F_3 = \{A, B, D, E, G, H\}$
$F_4 = \{B, F, G, H\}$ und $F_5 = \{C, D, E, F, G, H\}$.
Und hier ist die Matrix:

	01000	01110	10011	01111
A	6	10	29	26
B	13	1	22	17
C	19	31	8	15
D	23	27	12	11
E	21	25	14	9
F	24	20	3	4
G	30	18	5	2
H	28	16	7	0

Ergab ihre Rechnung etwa eine 19, so ist sie sicher: Der Zuschauer hat sich das „C“ ausgesucht und gemäß Lügenszenario 01000 geantwortet.

Hier ein zweites Beispiel, da betrachten wir das zulässige Paar $\mathbb{A} = \{11000, 11100, 01010, 10110, 01001, 10101, 00011, 00111\}$ und $\mathbb{L} = \{00000, 10000, 01000, 00111\}$. Man beachte: Diesmal kann die Menge der Lügnerszenarien auch mit Worten leicht beschrieben werden: „Immer ehrlich. Oder beim ersten oder zweiten Mal lügen. Oder bei den letzten drei Fragen lügen.“ Nach der vorstehend beschriebenen Verkleidung sieht es dann so aus. Die Fragemengen sind
$F_1 = \{A, B, D, F\}$, $F_2 = \{A, B, E\}$, $F_3 = \{B, D, F, H\}$
$F_4 = \{C, D, G, H\}$ und $F_5 = \{E, F, G, H\}$.
Und als Matrix ergibt sich

	00000	10000	01000	00111
A	3	2	1	31
B	7	6	5	27
C	10	11	8	22
D	13	12	15	17
E	18	19	16	14
F	21	20	23	9
G	24	25	26	4
H	28	29	30	0

Es folgen noch weitere Beispiele in Kurzfassung. Es sollte klar sein, wie die Tabelle zu erstellen ist. Wir erwähnen noch, dass der Fall einelementiger $\mathbb{L}$ im Wesentlichen zu der bekannten Vorgehensweise führt, ein Element aus einer 2^n-elementigen Menge durch n Fragen zu identifizieren. (Hier kann man immer $\mathbb{A} = G_n$ wählen.)

Beispiel „Fünf Fragen: Einmal lügen, aber nicht bei der dritten Frage!“.

Hier ist $\mathbb{L} = \{10000, 01000, 00010, 00001\}$, und unter den vielen möglichen Auswahlmengen wählen wir $\mathbb{A} = \{10000, 11100, 01010, 00110, 10001, 11101, 01011, 00111\}$. Dann ist $(\mathbb{A}, \mathbb{L})$ zulässig, und die Fragemengen sind
$F_1 = \{A, B, E, F\}$, $F_2 = \{B, C, F, G\}$, $F_3 = \{B, D, F, H\}$
$F_4 = \{C, D, G, H\}$ und $F_5 = \{E, F, G, H\}$.

Beispiel „Vier Fragen: Genau einmal lügen!“

Es ist $\mathbb{L} = \{1000, 0100, 0010, 0001\}$, und es wird $\mathbb{A} = \{0010, 1010, 0101, 1101\}$ vorgeschlagen. Das führt zu den Fragemengen $F_1 = \{B, D\}$, $F_2 = \{C, D\}$, $F_3 = \{A, B\}$, $F_4 = \{C, D\}$.

Beispiel „Vier Fragen: Immer lügen, oder lügen nur bei den Fragen 1, 2, oder 3“.

Die Bedingung führt auf $\mathbb{L} = \{1000, 0100, 0010, 1111\}$, und Computerhilfe liefert als mögliches $\mathbb{A}$ die Menge $\{0100, 1010, 0101, 1011\}$. Hier sind die zugehörigen Fragemengen: $F_1 = \{B, D\}$, $F_2 = \{A, C\}$, $F_3 = \{B, D\}$, $F_4 = \{C, D\}$.

Zum Abschluss des Abschnitts gibt es für diejenigen noch einen „psychologischen“ Ratschlag, die ein derartiges Kunststück selbst entwickeln wollen: Mathematisch ist es völlig in Ordnung, aber für die Vorführung wäre es sehr ungünstig, wenn eine der Fragemengen leer bzw. gleich der Auswahlmenge $\mathbb{A}$ wäre. Denn dann wäre auf die Frage „Liegt das Element in dieser Menge?“ jede Antwort trivial oder würde zur Entlarvung des Lügners (an dieser Stelle) führen. Auch wäre es wünschenswert, dass jedes Element der Auswahlmenge in mindestens einer Fragemenge auftaucht.

Zusammenfassung

Es ist unter Zauberern ein bewährtes Verfahren, durch n richtig beantwortete Fragen ein Element einer 2^n-elementigen Menge sicher zu identifizieren. Es gibt auch Ansätze, durch $n + 1$ Fragen das gleiche unter der Bedingung zu leisten, dass der Zuschauer immer die Wahrheit sagt oder immer lügt. Hier haben wir studiert, welche Auswahlen bei beliebigen vorgegebenen Lügnerszenarien zugelassen werden. Die Kombination von Auswahlmöglichkeiten und Lügnerszenarien gab Anlass zu konkreten Fragen in endlichen abelschen Gruppen.

Danksagung: Ich bin den Kollegen Martin Aigner und Ralph-Hardo Schulz für interessante Hintergrundinformationen aus der Komplexitätstheorie und der Graphentheorie dankbar.

Literatur

[1] E. Behrends. *Tupel aus n natürlichen Zahlen, für die alle Summen verschieden sind, und ein Maßkonzentrations-Phänomen*. Elemente der Mathematik 74, 2019, 114 – 130.

[2] https://de.wikipedia.org/wiki/Karps_21_NP-vollst%C3%A4ndige_Probleme.

[3] D. Jungnickel. *Einführung in die Kombinatorik*. De Gruyter, 2004.

[4] W. Miller. *ad rem 6*. Verlag Magic Center Harri, 2018, 98 Seiten.

[5] R.-H. Schulz. *Codierungstheorie, eine Einführung*. Springer Verlag, 2003.

Ehrhard Behrends
Mathematisches Institut, Freie Universität Berlin
Arnimallee 6
D-14 195 Berlin
Germany
e-mail: behrends@math.fu-berlin.de