Schachbrett-Codes

Lange Nacht der Mathematik 2025

TECHNISCHE UNIVERSITÄT DARMSTADT

Das Rätsel um die Schachbrett-Codes

Du bist gemeinsam mit einem Freund in einem Verlies gefangen, dessen Wärter euch nur rauslässt, wenn ihr sein Rätsel lösen könnt. Er zeigt euch ein Schachbrett, 64 handelsübliche Münzen und den Schlüssel zur Verliestür.

Er sagt: „Einen von euch werde ich in ein anderes Verlies sperren, von dem aus die Person nichts mehr mitbekommt. Der anderen Person werde ich zeigen, wie ich den Schlüssel unter einem der 64 Felder verstecke und auf jedes der Felder eine Münze mit wahlweise Kopf oder Zahl oben lege. Dann muss diese Person genau eine Münze umdrehen. Schließlich tauscht ihr die Positionen und der von euch, der zuerst weggesperrt war, muss anhand der Münzen erkennen unter welchem Feld der Schlüssel versteckt ist. Nur dann kommt ihr hier raus. “

Die Person, die hinterher rät, sieht also nur die Anordnung nach dem Umdrehen der Münze, weiß aber nicht, welche Münze umgedreht wurde. Es gibt während des Rätsels keine Möglichkeit der Kommunikation, aber ihr dürft vorher miteinander reden, um eine Strategie auszumachen. Seid aber gewarnt, denn der Wärter hört eure Strategie und kann die Münzen so fies wie möglich auslegen, um eure Strategie zunichte zu machen. Wie könnt ihr trotzdem garantieren, den Schlüssel zu finden, um aus dem Verlies herauszukommen?

Erste Lösungsgedanken

Da der ratenden Person nicht bewusst ist, welche Münze umgedreht wurde, muss sie allein anhand der ausliegenden Münzen erkennen, wo der Schlüssel ist. Wir müssen also jeder der 2^{64} möglichen Auslegungen der Münzen genau ein Zielfeld zuordnen, unter dem dann der Schlüssel versteckt sein soll. Es gibt 64 mögliche Felder für den Schlüssel und wir dürfen genau eine von 64 Münzen umdrehen. Damit unsere Zuordnung gewinnbringend ist, müssen wir aus jeder Position mit nur einem Umdrehen einer Münze in eine Position kommen, die das richtige Zielfeld hat - egal, wo der Schlüssel ist.

Der Einfachheit halber wollen wir das Rätsel erstmal auf einem 2×2-Feld lösen. Die Ideen bleiben aber gleich.

Rechnen mit zwei Elementen

In der Schule wird hauptsächlich in den reellen Zahlen gerechnet, aber es gibt auch weitere Zahlenbereiche mit eigenen Rechenoperationen, die ähnlichen Gesetzmäßigkeiten folgen, sogenannte *Körper*. Hier wollen wir den Körper mit zwei Elementen betrachten, den $\mathbb{F}_2$. Dieser besteht aus den Zahlen 0 und 1, die man wie folgt miteinander „addiert “: Wenn ich etwas mit 0 addiere, dann bleibt es wie gewohnt gleich, wenn ich aber 1 und 1 addiere, dann soll 0 herauskommen. Da wir keine anderen Zahlen haben, ist das alles, was wir wissen müssen.

Vergewissere dich, dass bei dieser Rechenoperation Addition und Subtraktion das gleiche sind.

Geordnete Paare

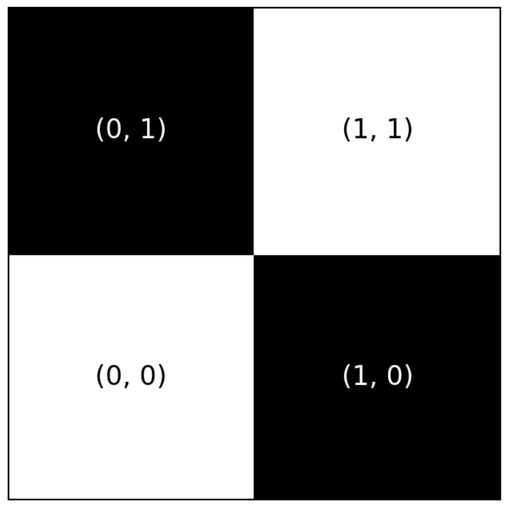
Statt mit nur einer Zahl zu rechnen, kann man auch mehrere Zahlen hintereinander in sogenannten *Tupeln* schreiben. Bei zwei Zahlen nennt man das dann einen *2-Tupel* oder ein *geordnetes Paar*. Wenn man mehrerer solcher Tupel addieren will, geht man *komponentenweise* vor. Das heißt, die erste Zahl wird mit der ersten addiert, die zweite mit der zweiten, etc.

Vielleicht hast Du etwas Ähnliches bereits als Vektoren in der Schule kennengelernt.

Die Lösung

Nutzen wir die Begriffe, die wir soeben eingeführt haben. Wir ordnen auf unserem 2×2-Brett jedem Feld ein geordnetes Paar aus Elementen im $\mathbb{F}_2$ zu - von denen gibt es auch genau 4. Jeder möglichen Auslegung ordnen wir wie folgt ein Zielfeld zu: Wir addieren die Paare aller Felder, auf denen die Münze auf Kopf liegt und nehmen das Feld, das zur Summe gehört. Wenn der Wärter uns jetzt eine beliebige Auslegung gibt und den Schlüssel unter einem Feld versteckt, dann müssen wir nur ausrechnen, was das aktuelle Zielfeld ist und die Differenz mit dem Paar bilden, das zum Feld mit dem Schlüssel gehört. Wenn wir die Münze auf dem Feld umdrehen, das zur Differenz gehört, dann ist das neue Zielfeld genau das Feld mit dem Schlüssel! Man beachte, dass dabei egal ist, ob wir die Münze von Kopf auf Zahl oder von Zahl auf Kopf drehen, weil Plus und Minus im $\mathbb{F}_2$ dasselbe sind.

Wenn wir das Rätsel auf einem richtigen Schachbrett lösen wollen, dann müssen wir nur jedem Feld ein 6-Tupel im $\mathbb{F}_2$ zuordnen, wovon es genau $2^6 = 64$ gibt.



Ausblick

Da die Anordnung der Felder für das Rätsel eigentlich egal ist, können wir uns das gleiche Rätsel auch für beliebige Felderanzahlen stellen. Unsere Lösung hier lässt sich so variieren, dass sie das Rätsel löst, solange die Felderanzahl eine Zweierpotenz ist, indem wir die Länge des Tupels anpassen. Tatsächlich kann man beweisen, dass das Rätsel unlösbar ist, wenn die Felderanzahl keine Zweierpotenz ist! Das benötigt aber andere Mathematik, nämlich die Fragestellung nach der Färbbarkeit von Graphen.

Die Mathematik dieses Rätsels findet Anwendung in der digitalen Signalverarbeitung in der Form fehlerkorrigierender Codes. Das Stichwort hier für die weitere Suche sind Hamming-Codes.

Fachbereich Mathematik der Technischen Universität Darmstadt, AG Algebra

Die lange Nacht der Mathematik

Link zu diesem Poster