Elemente der Mathematik 79 (2024), 15–24
DOI 10.4171/EM/498

Ein chinesisches Orakel und zyklische Matrizen über dem Körper $\mathbb{F}_2$

Annegret Weng

Annegret Weng promovierte 2001 an der Universität Duisburg-Essen über ein zahlentheoretisches Thema mit Anwendung in der Kryptographie. Nach ihrer beruflichen Praxis bei verschiedenen Versicherungsunternehmen wurde sie 2012 auf eine Professur im Studiengang Mathematik an der Hochschule für Technik in Stuttgart berufen.

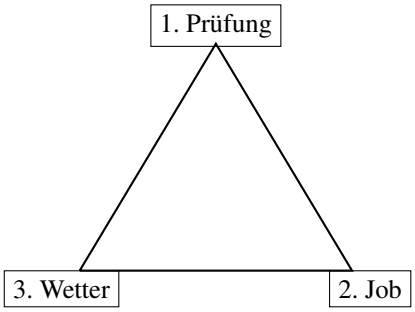
1 Einleitung

In ihrem Buch „Magical Mathematics“ [2, Kapitel 8] gehen die Autoren P. Diaconis und R. Graham auf chinesische Strichzeichen ein, die auf das Buch der Wandlungen (I Ging), einem der ältesten klassischen chinesischen Texte, zurückgehen. Nach einer Ausführung über die Konstruktion verschiedener Hexagramme bestehend aus durchgezogenen ——— oder gebrochenen Linien – – schlagen die Autoren auch drei Zauberroutinen vor.

Wir konzentrieren uns hier auf die dritte Routine, die die Überschrift „A performance piece“ trägt und sich dem Bereich der Mentalmagie zuordnen lässt. Wie wir sehen werden, kann diese mit Techniken der linearen Algebra über dem endlichen Körper $\mathbb{F}_2$ analysiert und verallgemeinert werden.

Zunächst aber beschreiben wir den Effekt: Der Mentalmagier gibt einem Zuschauer einen Umschlag mit einer Vorhersage, auf den er gut achten soll. Anschließend bittet er

Etliche Zaubertricks, vor allem aus dem Gebiet der Mentalmagie, verwenden mathematische Prinzipien. Manchmal wird sogar Mathematik benötigt, die über die herkömmliche Schulmathematik hinausgeht. Bei der in diesem Beitrag diskutierten Zauberroutine befragt der Magier ein Orakel. Dessen Antwort ergibt sich durch eine Reihe von Operationen, die mit einem Kartenstapel durchgeführt werden und die die Zuschauer selbst durch etliche freie Entscheidungen beeinflussen können. Aus der Anordnung der Karten ergibt sich am Ende ein Trigramm. Es zeigt sich, dass der Magier dieses schon zu Beginn korrekt vorhergesagt hatte. Bei der Analyse des Zaubertricks spielen Vektorräume über dem endlichen Körper $\mathbb{F}_2$ mit zwei Elementen, Faktorringe des univariaten Polynomrings $\mathbb{F}_2[x]$ und zyklische Matrizen eine wesentliche Rolle. Der Zaubertrick ist somit ein schönes Anwendungsbeispiel für Techniken der linearen und abstrakten Algebra.



Trigramm	Interpretation
⚊⚊⚊	Ja, Ja, Ja
⚋⚋⚋	Nein, Nein, Nein
⚊⚋⚊	Nein, Ja, Ja
⚋⚋⚊	Nein, Nein, Ja
⚋⚊⚋	Nein, Ja, Nein
⚊⚋⚋	Ja, Nein, Nein
⚊⚊⚋	Ja, Ja, Nein
⚊⚋⚊	Ja, Nein, Ja

Abbildung 1. Links ist das Dreieck für das Orakel abgebildet. Jeder Zuschauerfrage wird eine Ecke zugeordnet. Die rechte Tabelle gibt die möglichen Trigramme und ihre Interpretation im Zaubertrick an.

drei weitere Zuschauer, ihm eine für sie wichtige Frage zu stellen, wie z. B. „Werde ich meine nächste Prüfung bestehen?“, „Werde ich das erhoffte Jobangebot erhalten?“, „Wird das Wetter im Sommerurlaub gut?“ oder ähnliches.

Jedem der drei Zuschauer bzw. jeder Frage wird die Ecke eines Dreiecks zugeordnet (Abbildung 1, links). Der Magier befragt nun das „chinesische Orakel“. Dazu führt er mit einem Kartenstapel ein gewisses, randomisiertes Ritual durch, bei dem die Zuschauer etliche Entscheidungen treffen dürfen. Am Ende erhält er dabei ein Trigramm bestehend aus drei Linien. Dabei steht jede Linie für eine Antwort auf eine der drei gestellten Fragen. Eine durchgezogene Linie bedeutet „Ja“. Eine gebrochene Linie steht für die Antwort „Nein“ (Abbildung 1, rechts). Wenn der erste Zuschauer den ihm anvertrauten Umschlag öffnet, enthält er eine Vorhersage, die mit dem ermittelten Trigramm übereinstimmt.

Die Tatsache, dass der Magier das Trigramm richtig vorhersieht, ist natürlich darauf zurückzuführen, wie es generiert wird. Für die Herleitung des Trigramms werden 14 Spielkarten verwendet. Diese Karten werden scheinbar zufällig durcheinandergebracht. Dazu werden beliebig viele sogenannte *G-Scam-Deals* durchgeführt. Unter einem *G-Scam-Deal* versteht man die folgende Operation: Man hält die Karten bildunten und zählt ebenfalls bildunten die erste und dann die zweite Karte auf den Tisch. Die dritte Karte wird bildoben abgelegt, die vierte Karte wieder bildunten. Dann werden die vier Karten umgedreht, so dass jetzt drei der vier Karten bildoben und eine bildunten liegen. Das Päckchen aus den vier Karten wird auf den restlichen Kartenstapel gelegt.

Anschließend kann ein Zuschauer noch an einer beliebigen Stelle abheben.

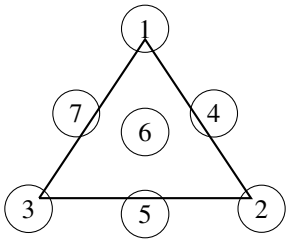


Abbildung 2. Das Orakel-Dreieck mit den verschiedenen Positionen, an denen die Karten abgelegt werden

Die Zuschauer können nun frei entscheiden, wie viele *G-Scam-Deals* durchgeführt werden und an welchen Stellen sie abheben wollen. Um aus den gemischten Karten das Trigramm zu bestimmen, werden die 14 Karten auf sieben Punkte des Dreiecks gelegt (Abbildung 2). Die erste Karte wird auf Position 1, die zweite auf die 2 usw. gelegt, die achte Karte wieder auf Position 1, die neunte auf 2 usw. Am Ende liegen auf jeder der sieben Positionen zwei Karten.

Um die erste Reihe des Trigramms zu bilden, werden die Karten der ersten Ecke und der benachbarten Positionen (d. h. die acht Karten in Position 1, 4, 6 und 7) betrachtet und die Parität aller bildoben liegenden Karten ermittelt. Eine gerade Anzahl entspricht einer durchgezogenen Linie, eine ungerade einer gebrochenen. Um die zweite Reihe zu erhalten, verfährt man analog mit der zweiten Ecke (Positionen 2, 4, 5 und 6) und schließlich sind für die dritte Reihe die Positionen 3, 5, 6, 7 relevant.

In Abschnitt 2 werden wir das Vorgehen mathematisch formalisieren und analysieren. Wir werden sehen, dass sich immer das Trigramm ☰ ergibt, unabhängig davon, an welchen Stellen die Zuschauer abheben und wie oft ein *G-Scam-Deal* durchgeführt wird. Die mathematische Abstraktion wird uns erlauben, das Vorgehen in Abschnitt 3 auf andere Kartenanzahlen und andere Mischverfahren zu verallgemeinern. Unter anderem finden wir ein Analogon des Dreieck-Orakels in der dritten Dimension.

Im letzten Abschnitt (Abschnitt 4) schließen wir mit einigen ergänzenden Bemerkungen.

2 Korrektheit der Vorhersage

Zu Beginn liegen alle 14 Karten bildunten. Wir repräsentieren dies durch die binäre Sequenz

$$w_0 = 00000000000000 \in \{0,1\}^{14}.$$

Durch die wiederholte Ausführung eines *G-Scam-Deals* mit anschließendem Abheben erhalten wir eine andere binäre Sequenz $w \in \{0,1\}^{14}$. Dabei steht eine 0 für „bildunten“ und eine 1 für „bildoben“. Für die Analyse des Tricks klären wir, welche $w \in \{0,1\}^{14}$ im Laufe der Performance möglich sind.

Ein *G-Scam-Deal* ändert die Reihenfolge der Karten nicht, transformiert die Sequenz w_0 aber auf

$$w_1 := 11010000000000.$$

Durch anschließendes Abheben wird die Teilsequenz 1101 an eine beliebige Stelle verschoben. Wir nennen die Ausführung eines *G-Scam-Deals* mit anschließendem Abheben einen *Extended G-Scam-Deal*.

Satz 2.1. *Die Menge der Konfigurationen in* $\{0,1\}^{14}$*, die durch wiederholte* Extended G-Scam-Deals *erreichbar sind, bildet einen Untervektorraum des* $\mathbb{F}_2$*-Vektorraums* $\mathbb{F}_2^{14}$ *der Dimension* 11.

Beweis. Wir fassen die Elemente in $\{0,1\}^{14}$ als Vektoren des 14-dimensionalen Vektorraums $\mathbb{F}_2^{14}$ über dem Körper $\mathbb{F}_2$ mit zwei Elementen auf. Anwendung eines *Extended G-Scam-Deals* auf ein beliebiges Element $w \in \mathbb{F}_2^{14}$ entspricht der Addition einer der 14 möglichen zyklischen Shifts $w_1^{(k)}$, $k = 0, \ldots, 13$, von w_1. Somit entsprechen die vom Element w_0 erreichbaren Vektoren genau dem Untervektorraum, der von den 14 Elementen $w_1^{(k)}$, $k = 0, \ldots, 13$, aufgespannt wird.

Um die Dimension des Untervektorraums zu bestimmen, tragen wir die Vektoren in eine (14×14)-Matrix ein:

$$M_{14} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & \ldots & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & \ldots & 0 & 0 & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & 0 & 0 & 0 & 0 & \ldots & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & \ldots & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & \ldots & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{1}$$

Die ersten 11 Zeilen z_i der Matrix bilden eine obere Dreiecksmatrix und sind somit offensichtlich linear unabhängig. Auf der anderen Seite sieht man einfach, dass

$$\begin{aligned} z_{12} &= z_1 + z_2 + z_3 + z_5 + z_8 + z_9 + z_{10}, \\ z_{13} &= z_2 + z_3 + z_4 + z_6 + z_9 + z_{10} + z_{11}, \\ z_{14} &= z_1 + z_2 + z_4 + z_7 + z_8 + z_9 + z_{11}. \end{aligned}$$

Daraus folgt die Behauptung. ∎

Bisher haben wir die Zeilen der Matrix M_{14} betrachtet. Auch die Spalten erzeugen einen Untervektorraum der Dimension 11. Der Kern der Matrix hat also Dimension 3. Es seien s_i die Spalten der Matrix M_{14}. Dann gilt

$$\begin{aligned} s_1 + s_4 + s_6 + s_7 + s_8 + s_{11} + s_{13} + s_{14} &= 0, \\ s_2 + s_4 + s_5 + s_6 + s_9 + s_{11} + s_{12} + s_{13} &= 0, \\ s_3 + s_5 + s_6 + s_7 + s_{10} + s_{12} + s_{13} + s_{14} &= 0. \end{aligned} \tag{2}$$

Diese drei Gleichungen entsprechen gerade den drei Vorhersagen. Übersetzt auf die Karten bedeutet z. B. die erste Gleichung in (2), dass die Summe der bildoben liegenden Karten an Stelle 1, 4, 6, 7, 8, 11, 13 und 14 (das sind die acht Karten an den Positionen 1, 4, 6 und 7) immer gerade ist.

3 Verallgemeinerung

3.1 Zyklische Matrizen

Ein *G-Scam-Deal* verändert vier aufeinanderfolgende Karten gemäß dem Muster

$$[1, 1, 0, 1].$$

Wir betrachten nun allgemeine Kartenoperationen, denen ein Muster $m \in \{0, 1\}^k$ zugrunde liegt. Wir nehmen an, dass das Muster m mit einer 1 beginnt und endet, denn sonst würde es sich bei m eigentlich um ein Muster kleinerer Länge handeln. Die entsprechende Matrix M_n^m ist wie die Matrix in (1) eine zyklische Matrix, bei der sich alle restlichen Zeilen aus einer zyklischen Verschiebung der ersten Zeile ergeben. Wir sind im Besonderen am Rang einer solchen Matrix und an der Form des Kerns interessiert.

Dazu identifizieren wir den Vektorraum $V_n = \mathbb{F}_2^n$ mit der additiven Gruppe des Faktorrings $R_n = \mathbb{F}_2[x]/(x^n - 1)$. Dabei wird dem Vektor $(1, 0, \ldots, 0)$ das konstante Polynom 1, dem Vektor $(0, 1, \ldots, 0)$ das Polynom x, dem Vektor $(0, 0, 1, \ldots, 0)$ das Polynom x^2 usw. zugeordnet. Dann entspricht die Anwendung von M_n^m mit $m = [m_1, \ldots, m_k]$, $k \leq n$, auf ein Element in V_n der Multiplikation mit dem Polynom

$$f(x) = m_1 + \sum_{i=2}^{k} m_i x^{n-i+1} \quad \text{in } R_n.$$

Dieses Polynom wird auch als das zur zyklischen Matrix M_n^m assoziierte Polynom bezeichnet.

Satz 3.1. *Sei $f_{M_n^m}(x) \in \mathbb{F}_2[x]$ das zu M_n^m assoziierte Polynom. Dann ist die Dimension des Kerns von M_n^m gleich dem Grad d des Polynoms*

$$g(x) = \mathrm{ggT}(f_{M_n^m}(x), x^n - 1).$$

Beweis. Wir betrachten die Multiplikation mit $f_{M_n^m}(x)$ in R_n. Der Kern der Matrix M_n^m ist trivial, wenn $f_{M_n^m}(x)$ in R_n invertierbar ist, d. h., falls $g(x)$ konstant ist.

Nehmen wir nun an, dass $g(x)$ nicht konstant ist und somit $d \geq 1$. Dann gilt $x^n - 1 = g(x) \cdot h(x)$ für ein Polynom $h(x) \in \mathbb{F}_2[x]$ vom Grad kleiner n. In diesem Fall ist der Kern nicht trivial und besteht aus den Vielfachen von $h(x)$ in R_n. Die Vielfachen von $h(x)$ bilden einen Untervektorraum von R_n, der von den Polynomen $h(x), h(x) \cdot x, \ldots, h(x) \cdot x^{d-1}$ erzeugt wird. Somit entspricht die Dimension des Kerns dem Grad von $g(x)$. ∎

Der Beweis liefert uns auch eine Methode, die Basis des Kerns zu bestimmen. Wenn wir $g(x) = \mathrm{ggT}(f_{M_n^m}(x), x^n - 1)$ ermittelt haben, müssen wir nur $h(x) = \frac{x^n-1}{g(x)}$ berechnen.

Beispiel 3.2. Betrachten wir unser Eingangsbeispiel mit $n = 14$ und $m = [1, 1, 0, 1]$. Das assoziierte Polynom ist $f(x) = x^{13} + x^{11} + 1$ und es gilt $\mathrm{ggT}(f(x), x^n - 1) = x^3 + x^2 + 1$. Weiter erhalten wir

$$h(x) = \frac{x^{14} - 1}{f(x)} = x^{11} + x^{10} + x^9 + x^7 + x^4 + x^3 + x^2 + 1.$$

Die Dimension des Kerns ist somit 3 (der Grad des Polynoms $x^3 + x^2 + 1$). Eine Basis des Kerns ist gegeben durch die aus $h(x)$, $h(x) \cdot x$, $h(x) \cdot x^2$ abgeleiteten Vektoren

$$\begin{aligned} v_1 &= (1,0,1,1,1,0,0,1,0,1,1,1,0,0), \\ v_2 &= (0,1,0,1,1,1,0,0,1,0,1,1,1,0), \\ v_3 &= (0,0,1,0,1,1,1,0,0,1,0,1,1,1). \end{aligned} \tag{3}$$

Ersetzen von v_1 durch $v_1 + v_3$ führt auf die Gleichungen in (2).

Der in Abschnitt 1 beschriebene Trick lässt sich mit jeder durch 7 teilbaren Kartenanzahl durchführen, also auch mit 21, 28 usw. Karten.

Satz 3.3. *Die Matrix M_n^m mit $m = [1,1,0,1]$ hat Rang $n-3$, falls n durch 7 teilbar ist, und n sonst.*

Beweis. Das Polynom $x^3 + x^2 + 1$ ist irreduzibel über $\mathbb{F}_2$. Seine Nullstellen liegen also in einer Körpererweiterung vom Grad 3 über $\mathbb{F}_2$, dem Körper mit 8 Elementen. Dessen multiplikative Gruppe hat Ordnung 7. Somit sind alle Nullstellen von $x^3 + x^2 + 1$ siebte Einheitswurzeln im algebraischen Abschluss des Körpers $\mathbb{F}_2$. Die Polynome $x^n - 1$ und $x^3 + x^2 + 1$ haben deshalb genau dann einen gemeinsamen Teiler, wenn n durch 7 teilbar ist. Dieser Teiler muss dann aufgrund der Irreduzibilität gleich $x^3 + x^2 + 1$ sein. ∎

Mithilfe des folgenden Satzes können wir uns leicht davon überzeugen, dass sich auch bei einer anderen durch 7 teilbaren Kartenzahl ein Trigramm mit ausschließlich durchgezogenen Linien ergibt.

Satz 3.4. *Es sei $g(x) = \mathrm{ggT}(f_{M_q^m}(x), x^q - 1)$ nicht konstant und $x^q - 1 = g(x) \cdot h(x)$. Für $r \in \mathbb{N}$ folgt dann*

$$x^{q \cdot r} - 1 = g(x) \cdot \sum_{i=0}^{r-1} h(x) \cdot x^{i \cdot q}.$$

Beweis. Unter Verwendung der Summenformel für die geometrische Reihe erhalten wir

$$g(x) \cdot \sum_{i=0}^{r-1} h(x) \cdot x^{i \cdot q} = g(x) \cdot h(x) \cdot \sum_{i=0}^{r-1} (x^q)^i = (x^q - 1) \cdot \frac{x^{q \cdot r} - 1}{x^q - 1} = x^{q \cdot r} - 1. \quad ∎$$

Nach Satz 3.4 reicht es, im Fall $m = [1,1,0,1]$ die Basis des Kerns für $n = q = 7$ zu kennen. Eine Basis des Kerns von M_n^m für eine durch 7 teilbare Zahl $7 \cdot r$ ergibt sich dann, wenn die Einträge der einzelnen Vektoren r-mal wiederholt werden (vergleiche auch (3) für den Fall $q = 7$, $r = 2$).

3.2 Die Muster [1, 1, 0, 0, 1]

Das Muster $[1,1,0,0,1]$ bietet eine interessante Übertragung des ursprünglichen Zaubertricks in die dritte Dimension.

Satz 3.5. *Die Matrix M_n^m mit $m = [1,1,0,0,1]$ hat Rang $n-4$, falls $n \equiv 0 \bmod 15$, und Rang n sonst.*

Beweis. Das assoziierte Polynom zur Matrix M_n^m ist $f_{M_n^m}(x) = x^{n-1} + x^{n-4} + 1$. Es gilt

$$\begin{aligned}\mathrm{ggT}(f_{M_n^m}(x), x^n - 1) &= \mathrm{ggT}(x^4 \cdot f_{M_n^m}(x), x^n - 1)\\ &= \mathrm{ggT}(x^4 \cdot f_{M_n^m}(x) \bmod x^n - 1, x^n - 1)\\ &= \mathrm{ggT}(x^4 + x^3 + 1, x^n - 1).\end{aligned}$$

Das Polynom $x^4 + x^3 + 1$ ist irreduzibel über $\mathbb{F}_2$. Seine Nullstellen im algebraischen Abschluss von $\mathbb{F}_2$ erzeugen den Körper mit 16 Elementen, dessen multiplikative Gruppe aus den 15. Einheitswurzeln besteht. Daraus folgt die Behauptung. ∎

Mit Satz 3.4 erhalten wir

$$x^{15q} - 1 = (x^4 + x^3 + 1) \cdot \sum_{i=0}^{q-1} h(x) \cdot x^{15 \cdot i}$$

mit

$$h(x) = (x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1).$$

Der Kern der Matrix M_n^m für $n = 15$ wird durch

$$\begin{aligned}v_1 &= (1,0,0,1,1,0,1,0,1,1,1,1,0,0,0),\\ v_2 &= (0,1,0,0,1,1,0,1,0,1,1,1,1,0,0),\\ v_3 &= (0,0,1,0,0,1,1,0,1,0,1,1,1,1,0),\\ v_4 &= (0,0,0,1,0,0,1,1,0,1,0,1,1,1,1)\end{aligned}$$

erzeugt. Für jedes Vielfache $15 \cdot q$ erhalten wir eine Basis des Kerns, in dem wir die Einträge der Vektoren v_i q-mal hintereinander schreiben.

Für den Zaubertrick betrachten wir allerdings die transformierte Basis

$$v_1 + v_4 = (1,0,0,0,1,0,0,1,1,0,1,0,1,1,1), v_2, v_3, v_4.$$

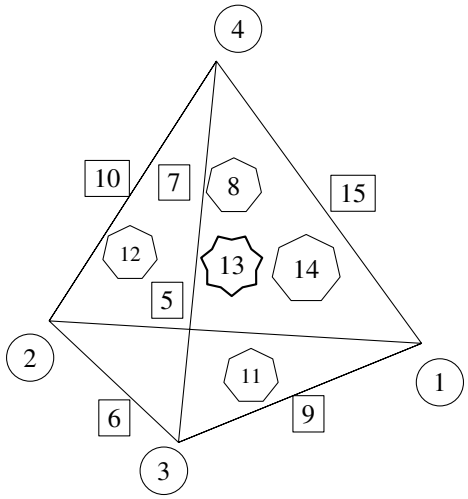
Sei n eine durch 15 teilbare Kartenzahl. Dann werden die Karten beliebig häufig einem *Extended G-Scam-Deal* mit $m = [1,1,0,0,1]$ unterzogen und schließlich auf die in Abbildung 3 angegebene Weise auf die speziellen 15 Punkte eines Tetraeders verteilt. Wir erhalten ein Quadrigramm, in dem wir für jede der vier Ecken die Parität der bildoben liegenden Karten in der Ecke selbst, den angrenzenden Seiten und Flächen und des Mittelpunkts des Dreiecks ermitteln.

3.3 Das Muster [1, 1, . . . , 1]

In diesem Abschnitt betrachten wir das Muster $[1, 1, \ldots, 1]$ bestehend aus k aufeinanderfolgenden Einsen.

Satz 3.6. *Sei $m = [1, 1, \ldots, 1]$ der Länge k gegeben. Dann hat M_n^m für $n \equiv 0 \bmod k$ den Rang $n - k + 1$. Für $n = k$ wird der Kern der Matrix M_m^n durch folgende Vektoren erzeugt:*

$$v_1 = (1,0,0,\ldots,0,1),\ v_2 = (0,1,0,\ldots,0,1),\ \ldots,\ v_{k-1} = (0,0,0,\ldots,1,1).$$



Erläuterung
1, 2, 3, 4: die vier Ecken des Tetraeders
5: Kante zwischen Ecken 1 und 2
6: Kante zwischen Ecken 2 und 3
7: Kante zwischen Ecken 3 und 4
8: Fläche zwischen Ecken 1, 2 und 4
9: Kante zwischen Ecken 1 und 3
10: Kante zwischen Ecken 2 und 4
11: Fläche zwischen Ecken 1, 2 und 3
12: Fläche zwischen Ecken 2, 3 und 4
13: Mittelpunkt des Tetraeders
14: Fläche zwischen Ecken 1, 3 und 4
15: Kante zwischen Ecken 1 und 4

Abbildung 3. Ein Orakel-Tetraeder analog zu Abbildung 2 zur Generierung eines Quadrigramms

Beweis. Mit dem Polynom $f_{M_n^m}(x) = x^{n-1} + \cdots + x^{n-k+1} + 1$ erhalten wir

$$\begin{aligned} \mathrm{ggT}(f_{M_n^m}(x), x^n - 1) &= \mathrm{ggT}(x^k \cdot f_{M_n^m}(x), x^n - 1) \\ &= \mathrm{ggT}(x^k \cdot f_{M_n^m}(x) \bmod x^n - 1, x^n - 1) \\ &= \mathrm{ggT}(x^{k-1} + \cdots + x + 1, x^n - 1). \end{aligned}$$

Da $(x^{k-1} + \cdots + x + 1) \cdot (x - 1) = x^k - 1$, sind die Nullstellen von $x^{k-1} + \cdots + x + 1$ k-te Einheitswurzeln und für $n \equiv 0 \bmod k$ auch Nullstellen von $x^n - 1$. Somit ist die Dimension des Kerns von M_n^m für $n \equiv 0 \bmod k$ gleich $k - 1$, und M_n^m hat Rang $n - k + 1$.

Aus $x^n - 1 = (x + 1) \cdot (x^{n-1} + \cdots + x + 1)$ in $\mathbb{F}_2[x]$ erhalten wir mit $h(x) = x + 1$ die Basis

$$w_1 = (1, 1, 0, \ldots, 0, 0),\ w_2 = (0, 1, 1, 0, \ldots, 0, 0),\ \ldots,\ w_{k-1} = (0, 0, \ldots, 1, 1).$$

Die transformierte Basis $w_1 + \cdots + w_{k-1}$, $w_2 + \cdots + w_{k-1}$, $\ldots$, w_{k-1} hat die gewünschte Form. ∎

Sei n eine durch k teilbare Zahl. In diesem Fall werden immer k Karten bildunten auf den Tisch gezählt, dann umgedreht und auf den restlichen Kartenstapel gelegt. Nach beliebig vielen *Extended G-Scam-Deals* mit $m = [1, 1, \ldots, 1]$ werden die Karten auf einem regelmäßigen $(k - 1)$-Eck ausgeteilt (siehe Abbildung 4 für den Fall $k = 5$), und zwar erst eine Karte auf jede der $k - 1$ Ecken, dann eine Karte in die Mitte, dann wieder auf die $k - 1$ Ecken, in die Mitte usw. Das Orakel beantwortet hier $k - 1$ Fragen der Zuschauer, denen wieder die einzelnen Ecken zugeordnet werden. Zur Beantwortung einer Frage wird hier die Parität der bildoben liegenden Karten der jeweiligen Ecke und der Mitte betrachtet. Da der dazugehörige Vektor im Kern der Matrix M_n^m liegt, ist die Anzahl immer gerade.

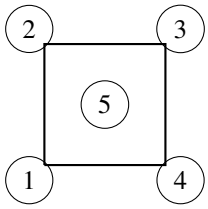


Abbildung 4. Abbildung für den Fall $k = 5$

4 Ergänzungen und Ausblick

Über zyklische Matrizen gibt es bereits mathematische Literatur. So findet sich das Resultat von Satz 3.1 auch in [3], allerdings mit einem abweichenden Beweisansatz.

Der Umweg über die Trigramme ist natürlich nicht nötig. Stattdessen wäre auch die direkte Vorhersage der Antworten möglich. Der Bezug auf die chinesischen Strichzeichen wertet die Vorführung auf und kann das Trickgeheimnis zusätzlich verschleiern.

In [2] erhöhen die Autoren den Effekt des Tricks. Dafür werden den drei Zuschauern am Ende die zwei Spielkarten ihrer jeweiligen Ecke gegeben. Der Umschlag mit der Vorhersage des Trigramms enthält zusätzlich noch Hinweise auf die Karten der drei Zuschauer. Für diese Steigerung ist es notwendig, dass die 14 Karten zu Beginn in einer vorgegebenen Reihenfolge liegen und dass vor dem Austeilen an einer vorgegebenen Stelle abgehoben wird. Dieser Teil ist jedoch mathematisch uninteressant und wird hier nur der Vollständigkeit halber erwähnt.

Tabelle 1 zeigt Auswertungen zum Rang der Matrix M_n^m, die wir mit SageMath [1] für eine Kartenanzahl $n \leq 52$ und sämtliche Muster m der Länge 3, 4 und 5 gemacht haben. Mit dem eigens für diesen Beitrag erstellten SageMath Notebook[1] kann der interessierte Leser weitere Muster m anderer Längen (beispielsweise der Länge 6) untersuchen oder seinen eigenen Zaubertrick kreieren.

Literatur

[1] SageMath, The Sage Mathematics Software System (Version 8.8), The Sage Developers, 2022, https://www.sagemath.org (Stand: 4. 10. 2022)

[2] P. Diaconis und R. Graham, *Magical mathematics*. Princeton University Press, Princeton, 2012

[3] A. W. Ingleton, The rank of circulant matrices. *J. Lond. Math. Soc.* **31** (1956), 445–460

Annegret Weng
Hochschule für Technik
Schellingstr. 24, 70174 Stuttgart, Germany
annegret.weng@hft-stuttgart.de

[1] https://transfer.hft-stuttgart.de/gitlab/annegret.weng/chinesisches-orakel-und-zyklische-matrizen

Länge des Musters	Muster m	n: Rang der Matrix M_n^m
3	[1, 0, 1]	$n \equiv 0 \bmod 2$: $n-2$ $n \equiv 1 \bmod 2$: $n-1$
	[1, 1, 1]	$n \equiv 0 \bmod 3$: $n-2$ $n \not\equiv 0 \bmod 3$: n
4	[1, 0, 0, 1]	$n \equiv 0 \bmod 3$: $n-3$ $n \not\equiv 0 \bmod 3$: $n-1$
	[1, 0, 1, 1] [1, 1, 0, 1]	$n \equiv 0 \bmod 7$: $n-3$ $n \not\equiv 0 \bmod 7$: n
	[1, 1, 1, 1]	$n \equiv 0 \bmod 4$: $n-3$ $n \equiv 2 \bmod 4$: $n-2$ $n \not\equiv 0 \bmod 2$: $n-1$
5	[1, 0, 0, 0, 1]	$n \equiv 0 \bmod 4$: $n-4$ $n \equiv 2 \bmod 4$: $n-2$ $n \equiv 1 \bmod 2$: $n-1$
	[1, 0, 0, 1, 1] [1, 1, 0, 0, 1]	$n \equiv 0 \bmod 15$: $n-4$ $n \not\equiv 0 \bmod 15$: n
	[1, 0, 1, 0, 1]	$n \equiv 0 \bmod 6$: $n-4$ $n \equiv 3 \bmod 6$: $n-2$ $n \not\equiv 0 \bmod 3$: n
	[1, 0, 1, 1, 1] [1, 1, 1, 0, 1]	$n \equiv 0 \bmod 7$: $n-4$ $n \not\equiv 0 \bmod 7$: $n-1$
	[1, 1, 0, 1, 1]	$n \equiv 0 \bmod 6$: $n-4$ $n \equiv 3 \bmod 6$: $n-3$ $n \equiv 2, 4 \bmod 6$: $n-2$ $n \equiv 1, 5 \bmod 6$: $n-1$
	[1, 1, 1, 1, 1]	$n \equiv 0 \bmod 5$: $n-4$ $n \not\equiv 0 \bmod 5$: n

Tabelle 1. Rang der Matrix M_n^m für m, $3 \leq |m| \leq 5$ und $|m|+1 \leq n \leq 52$