Foolingsets und erweiterte Formulierungen

An der Fakultät für Mathematik
der Otto-von-Guericke-Universität Magdeburg
zur Erlangung des akademischen Grades
Bachelor of Science
angefertigte

Bachelorarbeit

vorgelegt von
Mirjam Friesen
geboren am 06.10.1988 in Hamburg,
Studiengang Mathematik,
mit Anwendungsfach Informatik.

3. Juli 2012

Betreut am Institut für Mathematische Optimierung von
Dr. rer. nat. Dirk Oliver Theis

Inhaltsverzeichnis

Kapitel 1

Einleitung

Die schönsten Lösungen der Mathematik sind die einfachen und schnellen, und oft findet man eine Lösung schneller, wenn man es schafft das Problem zu vereinfachen. In der linearen Optimierung geschieht dies zum Beispiel durch erweiterte Formulierungen. Vergleicht man das mit einer Autofahrt, so ist es, als würde man das Auto stärker beladen, dafür aber den Weg zum Ziel verkürzen. Letztendlich kommt man schneller an.
Ein lineares Optimierungsprogramm wird beschrieben durch eine lineare Zielfunktion f und linearen Nebenbedingungen, welche ein Polyeder beschreiben. Gesucht ist nun einen Vektor x aus jenem Polyeder, welcher $f(x)$ maximiert (alternativ auch minimiert).
In einer erweiterten Formulierung optimiert man über ein höherdimensionales Polyeder, das durch weniger Nebenbedingungen beschrieben wird. Das ursprüngliche Polyeder wird also erweitert und das neue Polyeder ist eine sogenannte Erweiterung des vorherigen Polyeders. Man hat also weniger Nebenbedingungen auf Kosten von mehr Variablen. Im Allgemeinen kann man über solch eine Erweiterung insgesamt schneller optimieren.
Für einige Probleme, wie zum Beispiel einen minimalen aufspannenden Baum in einem Graphen zu finden, sind bereits gute erweiterte Formulierungen bekannt. Für andere, wie zum Beispiel das Problem des Handlungsreisenden und das Matching-Problem, wurden noch keine polynomiellen Erweiterungen gefunden. Sowohl für das Problem des Handlungsreisenden als auch für das Matching-Problem, zeigte Yannakakis [8], dass unter bestimmten Symmetrieanforderungen an die erweiterte Formulierung keine mit polynomieller Größe existiert. Die Größe einer erweiterten Fomulierung ist in diesem Fall wenigstens exponentiell. Mittlerweile wurde für das Problem des Handlungsreisenden gezeigt, dass auch ohne Symmetrieanforderungen keine polynomiellen erweiterten Formulierungen existieren [4]. Es ist eine bekannte offene Frage, ob es polynomielle Erweiterungen für das Matching-Problem gibt.
Hier ist lediglich bekannt, dass die Größe einer erweiterten Formulierung in $\Omega(n^2)$ liegt. Es ist offen, wie genau diese Abschätzung ist.
Die minimale Größe einer erweiterten Formulierung wird Erweiterungskomplexität genannt. Es gibt einige untere Schranken, mit welchen man diese abschätzen kann. Um eine jener Schranken, die sogenannten Foolingsets, geht es in dieser Arbeit.
Foolingsets stammen aus dem Bereich der Kommunikationskomplexität, die 1979 von Yao [9] eingeführt wurde. Gegeben sind zwei Rechner Alice und Bob, sowie eine Funktion $f(x, y)$, welche beiden bekannt ist. Nun bekommt Alice ausschließlich x mitgeteilt und Bob ausschließlich y. Um $f(x, y)$ zu bestimmen und als Ergebnis zurückzugeben, müssen die Beiden also miteinander kommunizieren. Man ist nun daran interessiert, die Menge der Daten, welche dafür hin und her gesendet werden,

möglichst gering zu halten. Die minimale Anzahl auszutauschender Bits wird Kommunikationskomplexität von f genannt. Sie kann mithilfe von Foolingsets abgeschätzt werden.
Foolingsets sind quadratische Matrizen mit bestimmten Eigenschaften. Die Größe eines Foolingsets ist die Anzahl der Zeilen bzw. Spalten einer solchen Matrix. Foolingsets sucht man als Teilmatrizen von größeren Matrizen und bezeichnet mit $\mathrm{fool}(M)$ die Größe eines maximalen Foolingsets in M.
Dietzfelbinger, Hromkovič, Schnitger [2] verglichen die Größe von Foolingsets mit dem Rang einer 0,1-Matrix und konnten folgendes Theorem beweisen.

Theorem. *Es sei M eine Matrix mit Einträgen aus $\{0,1\}$ so gilt für alle Körper $\mathbb{K}$*

$$\mathrm{fool}(M) \leq \mathrm{rang}^2_{\mathbb{K}}(M),$$

wobei $\mathrm{rang}_{\mathbb{K}}$ den Rang über $\mathbb{K}$ bezeichnet.

Solche Zusammenhänge zwischen der Größe von Foolingsets in Matrizen und dem Rang können möglicherweise helfen Aussagen darüber zu treffen, inwieweit Foolingsets neue Erkenntnisse über die Erweiterungskomplexität bestimmter Probleme liefern können.
So kann man zu dem oben erwähnten Matching-Problem feststellen, dass der Rang der zugehörigen Matrix M in $\Theta(n^2)$ liegt. Es könnte also hilfreich sein nach Foolingsets zu suchen, denn möglicherweise existieren welche mit einer Größe zwischen $\Omega(n^2)$ und $O(n^4)$. In diesem Fall könnte die Abschätzung der Erweiterungskomplexität verbessert werden.
In dieser Arbeit möchte ich nun untersuchen, wie gut die Schranke $\mathrm{fool}(M) \leq \mathrm{rang}^2(M)$ ist. Es ist noch keine Matrix bekannt, welche die Ungleichung mit Gleichheit erfüllt. Die bisher besten Beispiele gab Theis [7]. Er fand eine Familie von Matrizen für welche gilt: $\mathrm{fool}(M) = \mathrm{rang}_{\mathbb{R}}^{\log_4(6)}(M)$, wobei $\log_4(6)$ ungefähr $1,29$ ist.
Ich habe intensiv nach weiteren Beispielen gesucht, um zu sehen, ob sich die obige Abschätzung verbessern lässt. Schließlich konnte ich eine Familie von Matrizen über $\mathbb{F}_2$ konstruieren, für welche ich vermute, dass sie Foolingsets sind. Dies würde dann eine Folge von Matrizen $(M_k)_{k\in\mathbb{N}}$ liefern, sodass gilt $\mathrm{fool}(M_k) \to \mathrm{rang}^2_{\mathbb{F}_2}(M_k)$ für $k \to \infty$. Die ersten 14 dieser Matrizen konnte ich mithilfe eines Computers auf die gewünschten Eigenschaften hin überprüfen und komme so zu dem Ergebnis $\mathrm{fool}(M_{14}) \geq \mathrm{rang}^{1,99999}(M_{14})$.

Kapitel 2

Erweiterungen von Polyedern

2.1 Einführung

Gegeben sei ein lineares Optimierungsproblem

$$\max\{\langle c,x\rangle \mid Ax \geq b,\ x \in \mathbb{R}^n\}.$$

Dieses ist lässt sich umformen zu

$$\max\left\{\langle c,x\rangle \mid Ax - x_{n+1}b \geq 0,\ x_{n+1} = 1,\ \begin{pmatrix} x \\ x_{n+1}\end{pmatrix} \in \mathbb{R}^{n+1}\right\}.$$

Ersetzt man die Gleichung $x_{n+1} = 1$ durch die Ungleichung $x_{n+1} \geq 0$, so erhält man einen Kegel K. Dieser Kegel ist die sogenannte *Homogenisierung* des Polyeders $P = \{x \in \mathbb{R}^n \mid Ax \geq b\}$.
Haben wir nun eine *Erweiterung* von K, das heißt ein Polyeder Q und eine lineare Abbildung π mit $\pi(Q) = K$, so erhalten wir folgende erweiterte Formulierung des obigen Programms

$$\min\left\{\langle c,x\rangle \;\middle|\; z \in Q\,,\ \begin{pmatrix} x \\ x_{n+1}\end{pmatrix} = \pi(z)\,,\ x_{n+1} = 1\right\}.$$

Ist P beschränkt, also ein Polytop, so kann man zeigen, dass die Ungleichung $x_{n+1} \geq 0$ redundant ist. Die Homogenisierung von P kann in diesem Fall also durch genauso viele Ungleichungen beschrieben werden wie P selber. Ist Q eine Erweiterung von P, so kann man annehmen das Q ebenfalls ein Polytop ist (vgl. [3] Seite 2). Die Homogenisierung von Q ist dann eine Erweiterung der Homogenisierung von P.
Wir werden später die Größe einer erweiterten Formulierung als die Anzahl der Ungleichungen, welche die Erweiterung Q beschreiben, definieren. In dem Fall das P ein Polytop ist, können wir uns auf Erweiterungen der Homogenisierung beschränken ohne die Größe zu verändern.

2.2 Kegel und erweiterte Formulierungen

Die Homogenisierung eines Polyeders ist offensichtlich ein polyedrischer Kegel. Da andere Kegel in dieser Arbeit nicht vorkommen ist im Folgenden mit Kegel stets ein polyedrischer Kegel gemeint.

Definition 2.2.1 (Erweiterung eines Kegels)**.** Eine *Erweiterung eines Kegels* $K \subseteq \mathbb{R}^n$ ist ein System von Gleichungen und Ungleichungen, welche einen Kegel $Q \subseteq \mathbb{R}^m$ beschreiben und eine lineare Abbildung $\pi : \mathbb{R}^m \to \mathbb{R}^n$ mit $\pi(Q) = K$.

Definition 2.2.2 (Größe einer Erweiterung)**.** Die *Größe einer Erweiterung* ist die Anzahl der Ungleichungen, welche Q beschreiben.

In dieser Definition werden die Gleichungen vernachlässigt, da man sie leicht loswerden kann. Es wurden für einige lineare Programme schon erstaunlich kleine erweiterte Formulierungen gefunden.

Beispiel 2.2.3. Für das Problem des minimal aufspannenden Baums in einem Graphen, fand Martin Kipp [6] eine erweiterte Formulierung der Größe $O(n^3)$, während das ursprüngliche Polytop $O(2^n)$ Ungleichungen hatte.

Man möchte nun wissen, wie klein eine Erweiterung höchstens sein kann. Dieser Wert heißt Erweiterungskomplexität.

Definition 2.2.4 (Erweiterungskomplexität $\mathrm{xc}(K)$)**.** Die *Erweiterungskomplexität* eines linearen Programms (eines Kegels K), ist die Größe einer kleinsten Erweiterung von K.
Formal:

$$\mathrm{xc}(K) = \min\{ \text{ Anzahl der Ungleichungen von } Q \mid Q \text{ ist Erweiterung von } K \text{ } \}$$

Die Frage ist nun, wie man die Erweiterungskomplexität eines Problems bestimmen kann.

2.3 Nichtnegativer Rang und Erweiterungskomplexität

Yannakakis [8] zeigte 1991 einen Zusammenhang zwischen dem nichtnegativen Rang der Schlupfmatrix eines Kegels und seiner Erweiterungskomplexität. Es sei eine Matrix M *nichtnegativ* ($M \geq 0$), wenn jeder Eintrag von M nichtnegativ ist.

Definition 2.3.1 (Schlupfmatrix eines Kegels)**.** Zu gegebenem Kegel
$K = \{x \in \mathbb{R}^n \mid Ax \geq 0\} = \mathrm{ccone}(X)$ ist $S := AX$ die sogenannte *Schlupfmatrix* von K, wobei $\mathrm{ccone}(X)$ die konvexkonische Hülle der Elemente aus X ist.

Definition 2.3.2 (Nichtnegativer Rang)**.** Es sei $M \in \mathbb{R}^{n \times m}$ eine nichtnegative Matrix. Der *nichtnegative Rang* von M ist die kleinste Zahl $r \in \mathbb{N}$, sodass nichtnegative Matrizen $U \in \mathbb{R}^{n \times r}$ und $V \in \mathbb{R}^{r \times m}$ existieren mit $M = UV$. Er wird mit $\mathrm{rang}_+(M)$ bezeichnet.

Es ist offensichtlich, dass jede Schlupfmatrix nichtnegativ ist. Wir können nun also den nichtnegativen Rang der Schlupfmatrix eines Kegels betrachten. Der folgende Satz entspricht dem oben angekündigten Resultat von Yannakakis [8].

Satz 2.3.3. *Die Erweiterungskomplexität* $\mathrm{xc}(K)$ *eines Kegels* K *ist gleich dem nichtnegativen Rang seiner Schlupfmatrix.*

Beweis. Sei $K = \{x \in \mathbb{R}^n \mid Ax \geq 0\}$ und S die zugehörige Schlupfmatrix mit $\mathrm{rang}_+(S) = r$. Desweiteren sei $S = UV$, $U \in \mathbb{R}^{m \times r}$, $V \in \mathbb{R}^{r \times k}$ eine nichtnegative Zerlegung von S.
Wir definieren nun eine Erweiterung zu K:

$$Q := \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^{n+r} \;\middle|\; Ax = Uy, \; y \geq 0 \right\}, \qquad \pi\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) := x$$

Offensichtlich ist π linear. Da U nichtnegativ und somit $Uy \geq 0$ ist, folgt $\pi(Q) = K$.
Es hat nun Q genau r Ungleichungen und somit gilt

$$\mathrm{xc}(K) \leq r = \mathrm{rang}_+(S).$$

Für die Rückrichtung sei nun $Q = \{y \in \mathbb{R}^m \mid By \geq 0\}$ eine Erweiterung von K.
Es bezeichne a_i die i-te Zeile von A und π^{ad} die Adjungierte zu π.
Für $y \in Q$ gilt nun

$$a_i\pi(y) \geq 0 \text{ und somit auch } \pi^{ad}(a_i)y \geq 0,$$

das heißt $\pi^{ad}(a_i)y \geq 0$ sind zulässige Ungleichungen für Q mit $\pi^{ad}(a_i)\mathbb{0} = 0$. Nach Fakas Lemma (Variante III in [10]) existiert für alle i ein Vektor $\lambda_i \geq 0$ mit $\lambda_i^t B = \pi^{ad}(a_i)$.
Ist $K = \operatorname{ccone}\{x_1, \ldots, x_k\}$ und $y_1, \ldots, y_k$ aus Q mit $\pi(y_i) = x_i$ für $i = 1, \ldots, k$, so folgt für die Schlupfmatrix S von K

$$S_{i,j} = a_i x_j = a_i\pi(y_j) = \pi^{ad}(a_i)y_j = \lambda_i^t B y_j.$$

Da $\lambda_i \geq 0$ und $By_j \geq 0$, liefert dies eine nichtnegative Zerlegung von S und es folgt

$$\operatorname{rang}_+(S) \leq \operatorname{xc}(K).$$

□

2.4 Foolingsets als untere Schranke für die Erweiterungskomplexität

Foolingsets sind schon seit einiger Zeit als untere Schranke für den nichtnegativen Rank einer Matrix bekannt. So nutzten bereits Cohen und Rothblum [1] 1993 sogenannte „Mengen von unabhängigen Einträgen“ um den nichtnegativen Rang abzuschätzen. Diese lassen sich direkt in Foolingsets umformulieren.
Im Folgenden bezeichne ich mit $M_{i,j}$ den Eintrag von M in der i-ten Zeile und j-ten Spalte, desweiteren sind $M_{i,*}$ und $M_{*,j}$ die i-te Zeile bzw. j-te Spalte.

Definition 2.4.1 (Foolingset)**.** Es sei M eine Matrix mit Einträgen aus $\{0, 1\}$. Eine Menge $F \subset \mathbb{N}^2$ heißt *Foolingset*, wenn gilt

$$\begin{aligned} & M_{i,j} = 1 && \text{für alle } (i,j) \in F \\ \text{und} \quad & M_{i,j}M_{k,\ell} = 0 && \text{für alle } (i,j),(k,\ell) \in F \text{ mit } (i,j) \neq (k,\ell). \end{aligned}$$

Diese Definition lässt sich mit der Abwandlung $M_{i,j}M_{k,\ell} > 0$ auch allgemeiner auf nichtnegative Matrizen anwenden. Diese Form verwenden Cohen und Rothblum [1]. Ihre Mengen von unabhängigen Einträgen entsprechen Foolingsets in der Trägermatrix $\operatorname{supp}(M)$ von M, also in der Matrix, deren Einträge genau dann 1 sind, wenn der entsprechende Eintrag in M größer als 0 ist und 0 sonst.
Es sei nun $\operatorname{fool}(M)$ die größte Zahl z, so dass ein Foolingset der Größe z in M existiert. Aufgrund des oben beschriebenen Zusammenhangs bezeichne ich mit $\operatorname{fool}(M)$ auch die Foolingsetzahl der Trägermatrix, also $\operatorname{fool}(M) = \operatorname{fool}(\operatorname{supp}(M))$.

Satz 2.4.2. *Für eine nichtnegative Matrix M gilt:* $\operatorname{fool}(M) \leq \operatorname{rang}_+(M)$. *[1]*

Cohen und Rothblum erwähnen diesen Zusammenhang, geben aber keinen Beweis an. In [3] wird ein Beweis gegeben, welcher einige Umwege geht, die hier nicht benötigt werden. Ich stelle hier nun einen direkten Beweis vor.

Beweis. Sei $M \in \mathbb{R}^{n\times m}$ eine nichtnegative Matrix und F ein Foolingset von M. Weiterhin sei $M = UV$ eine nichtnegative Zerlegung von M mit $U \in \mathbb{R}^{n\times r}, V \in \mathbb{R}^{r\times m}$ mit $r = \operatorname{rang}_+(M)$.
Das Permutieren der Zeilen in M entspricht dem Permutieren der Zeilen in U und das Permutieren

der Spalten in M denen in V. Der nichtnegative Rang von M wird dadurch also nicht verändert und wir können o.B.d.A annehmen, dass $F = \{(1,1),(2,2),\dots,(|F|,|F|)\}$ ist. Der Übersicht halber schreiben wir $k \in F$, wenn gilt $(k,k) \in F$. Es gilt also:

$$M_{k,k} > 0 \text{ und } M_{k,i}M_{i,k} = 0 \qquad \text{für alle } k,i \in F \text{ mit } k \neq i \tag{2.1}$$

Angenommen $|F| > \operatorname{rang}_+(M)$, dann folgt aus

$$M_{k,k} = U_{k,*}V_{*,k} > 0,$$

dass für alle $k \in F$ ein $i = i(k) \in \{1,\dots,\operatorname{rang}_+(M)\}$ existiert mit

$$U_{k,i}V_{i,k} > 0.$$

Da aber $|F| > \operatorname{rang}_+(M)$ ist, existieren k,ℓ mit $k \neq \ell, i(k) = i(\ell) = i$, sodass gilt

$$U_{k,i}V_{i,k} > 0 \text{ und } U_{\ell,i}V_{i,\ell} > 0.$$

Es folgt

$$M_{k,\ell} \geq U_{k,i}V_{i,\ell} > 0 \text{ und } M_{\ell,k} \geq U_{\ell,i}V_{i,k} > 0$$

und damit gilt $M_{\ell,k}M_{k,\ell} > 0$ im Widerspruch zu (2.1). Dementsprechend ist $|F| \leq \operatorname{rang}_+(M)$ für alle Foolingsets F und insbesondere $\operatorname{fool}(M) \leq \operatorname{rang}_+(M)$. $\square$

Kapitel 3

Foolingsets versus Rang

3.1 Bereits bekannte Zusammenhänge

Für Matrizen aus Nullen und Einsen kann man die Foolingsetzahl durch den Rang abschätzen. Dietzfelbinger et al. [2] bewiesen hierzu 1996 folgendes Theorem.

Theorem 3.1.1. *Für eine 0,1-Matrix M und für jeden Körper $\mathbb{K}$ gilt:* $\mathrm{fool}(M) \leq \mathrm{rang}_{\mathbb{K}}^2(M)$, *wobei* $\mathrm{rang}_{\mathbb{K}}(M)$ *den Rang über $\mathbb{K}$ bezeichnet.*

Beweis. Der Beweis ist übernommen von Theis [7].
Sei F ein Foolingset in M. Es gelte o.B.d.A. wieder $F = \{(1,1),(2,2),\ldots,(|F|,|F|)\}$. Sei nun $M = XY$ eine zum Rang gehörige Zerlegung von M, das heißt für $\mathrm{rang}(M) = r$ gilt $X \in \mathbb{K}^{n\times r}$ und $Y \in \mathbb{K}^{r\times m}$.
Seien $x_1,\ldots,x_n$ die Zeilen von X und $y_1,\ldots,y_m$ die Spalten von Y, so gilt $M_{i,j} = x_i y_j$.
Wir definieren nun auf dem Tensorprodukt $\mathbb{K}^r \otimes \mathbb{K}^r$ das Skalarprodukt

$$\langle x_1 \otimes y_1, x_2 \otimes y_2\rangle = x_1y_2 \cdot x_2y_1$$

Damit haben wir

$$\begin{array}{lll} & \langle x_i \otimes y_i, x_i \otimes y_i\rangle = M_{i,i}^2 = 1 & \text{für } i = 1,\ldots,|F| \\ \text{und} & \langle x_i \otimes y_i, x_j \otimes y_j\rangle = M_{i,j}M_{j,i} = 0 & \text{für } i,j = 1,\ldots|F| \text{ und } i \neq j \end{array}$$

Das heißt $\{x_1 \otimes y_1, x_2 \otimes y_2, \ldots, x_{|F|} \otimes y_{|F|}\}$ bilden ein orthogonales System in $\mathbb{K}^r \otimes \mathbb{K}^r$, sind also linear unabhängig. Die Dimension von $\mathbb{K}^r \otimes \mathbb{K}^r$ ist r^2 und somit gilt $|F| \leq r^2 = \mathrm{rang}^2(M)$. □

Die Frage ist nun, wie genau diese Abschätzung ist. Dietzfelbinger et al. [2] zeigten eine Familie von Beispielen in $\mathbb{R}$, für welche gilt $\mathrm{fool}(M) = \mathrm{rang}^{\log_3(4)}(M)$ und Theis [7] fand ähnliche Beispiele, sodass $\mathrm{fool}(M) = \mathrm{rang}^{\log_4(6)}(M)$. Beide benutzen dafür das Kroneckerprodukt und konstruieren so aus einer Matrix eine Familie von Matrizen, ohne dass sich der Exponent ändert.

Die beiden Ausgangsmatizen sind:

$$M_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \qquad \text{mit } \operatorname{rang}(M_1) = 3 \text{ und } \operatorname{fool}(M) = 4$$

$$\text{und} \qquad M_2 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad \text{mit } \operatorname{rang}(M_2) = 4 \text{ und } \operatorname{fool}(M) = 6$$

Es liegt nun nahe die 8×8-Matrix

$$M_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

zu betrachten, M_3 hat allerdings Rang 5 und es gilt $\log_5(8) \approx 1,2920 \leq 1,2925 \approx \log_4(6)$, das heißt M_3 ist kein besseres Beispiel.

3.2 Der Rang in $\mathbb{F}_2$

Da wir mit Matrizen aus Einsen und Nullen rechnen, liegt es nahe, den Rang im Körper mit zwei Elementen ($\mathbb{F}_2$) zu betrachten.

Bemerkung 3.2.1. Für eine Matrix M aus Einsen und Nullen gilt:

$$\operatorname{rang}_{\mathbb{F}_2}(M) \leq \operatorname{rang}_{\mathbb{K}}(M) \text{ für alle Körper } \mathbb{K}$$

Es liegt also Nahe nach Matrizen über $\mathbb{F}_2$ zu suchen, welche möglichst dicht an der Abschätzung $\operatorname{fool}(M) \leq \operatorname{rang}^2_{\mathbb{F}_2}(M)$ aus Theorem 3.1.1 liegen. Man findet zum Beispiel leicht die Matrix

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

Hier gilt $\operatorname{rang}_{\mathbb{F}_2}(M) = 2$ und $\operatorname{fool}(M) = 3$, also $\operatorname{fool}(M) = \operatorname{rang}_{\mathbb{F}_2}^{\log_2(3)}(M)$. Dies liegt schon näher an der Abschätzung in 3.1.1 als die vorherigen Beispiele in $\mathbb{R}$ ($\log_2(3) \approx 1,58 > 1,29$).

3.3 Konstruktion einer Familie von Matrizen in $\mathbb{F}_2$

Ich werde nun eine Familie von Matrizen in $\mathbb{F}_2$ vorstellen, anhand welcher man sieht, dass die Abschätzung aus Theorem 3.1.1 sehr gut ist. Es sei mit $\operatorname{rang}(M)$ im Folgenden stets der Rang über $\mathbb{F}_2$ gemeint. Desweiteren bezeichne ich mit $\mathbb{N}$ die natürlichen Zahlen ohne Null und schreibe $\mathbb{N}_0$ für $\mathbb{N} \cup \{0\}$. Für die Konstruktion betrachten wir nun zunächst eine Folge in $\mathbb{F}_2$.

Definition 3.3.1. Zu gegebenem $r \in \mathbb{N}$ sei die Folge $(a_i)_{i \in \mathbb{N}_0}$ in $\mathbb{F}_2$ definiert durch:

$$\begin{aligned} a_i &= 1 && \text{für } 0 \leq i \leq r-1 \\ a_i &= a_{i-r} + a_{i-1} && \text{für } i \geq r \end{aligned}$$

Offensichtlich ist solch eine Folge periodisch in dem Sinn, dass ein $n \in \mathbb{N}$ existiert mit

$$a_{i+n} = a_i \text{ für alle } i \in \mathbb{N}_0.$$

Sei nun n die kleinste Periode von $(a_i)_{i \in \mathbb{N}_0}$, so lässt sich zu jedem r eine $n \times n$-Matrix wie folgt konstruieren.

Definition 3.3.2. Zu einer Folge $(a_i)_{i \in \mathbb{N}_0}$ aus 3.3.1 mit minimaler Periode n sei eine $n \times n$-Matrix M definiert durch

$$\begin{aligned} M_{0,*} &= (a_0, a_1, \cdots, a_{n-1}) \\ M_{i,j} &= M_{i-1,j-1} && \text{für } i, j \in \mathbb{Z}_n,\ i \neq 0 \end{aligned}$$

Wobei hier $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ der Restklassenring modulo n ist und die Elemente aus $\mathbb{Z}_n$ mit $0, 1, \ldots, n-1$ bezeichnet werden.

Beispiel 3.3.3. Für $r = 2$ und $r = 3$ erhält man nach obiger Konstruktion folgende Matrizen.

$$M_0 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \quad \text{und} \quad M_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Ich bezeichne eine $n \times n$-Matrix M als Foolingset, wenn $\{(i,i) \mid i = 0, \ldots, n-1\}$ ein Foolingset in M ist. Dies trifft auf die obigen beiden Matrizen zu und es lässt sich leicht überprüfen, dass sie in $\mathbb{F}_2$ den Rang r haben.

Da $\operatorname{fool}(M) \leq \operatorname{rang}^2(M)$ gilt, interessieren uns nur Folgen mit einer Periode n kleiner oder gleich r^2. Folgendes Bespiel zeigt, dass diese Bedingung noch nicht hinreichend dafür ist, dass eine wie oben konstruierte Matrix ein Foolingset ist.

Beispiel 3.3.4. Für $r = 4$ ist $n = 15$ und wir erhalten nach 3.3.2

$$M = \begin{pmatrix}
\mathbf{1} & 1 & 1 & 1 & 0 & 1 & 0 & \mathbf{1} & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & \mathbf{1} & 1 & 1 & 1 & 0 & 1 & 0 & \mathbf{1} & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & \mathbf{1} & 1 & 1 & 1 & 0 & 1 & 0 & \mathbf{1} & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 & 0 & 1 & 0 & \mathbf{1} & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 & 0 & 1 & 0 & \mathbf{1} & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 & 0 & 1 & 0 & \mathbf{1} & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 & 0 & 1 & 0 & \mathbf{1} & 1 \\
\mathbf{1} & 0 & 0 & 1 & 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 & 0 & 1 & 0 & \mathbf{1} \\
1 & \mathbf{1} & 0 & 0 & 1 & 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & \mathbf{1} & 0 & 0 & 1 & 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & \mathbf{1} & 0 & 0 & 1 & 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & \mathbf{1} & 0 & 0 & 1 & 0 & 0 & 0 & \mathbf{1} & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & \mathbf{1} & 0 & 0 & 1 & 0 & 0 & 0 & \mathbf{1} & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & \mathbf{1} & 0 & 0 & 1 & 0 & 0 & 0 & \mathbf{1} & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 1 & \mathbf{1} & 0 & 0 & 1 & 0 & 0 & 0 & \mathbf{1}
\end{pmatrix}$$

Diese Matrix ist kein Foolingset, da $M_{0,7} = M_{7,0} = 1$ gilt.

Die Eigenschaft Foolingset zu sein bedarf anscheinend noch einiger Untersuchungen, der Rang dieser Matrizen jedoch ist leicht bestimmt.

Lemma 3.3.5. *Für eine Matrix M aus 3.3.2 gilt* $\operatorname{rang}(M) = r$.

Beweis. Nach Konstruktion gilt

$$M_{i,j} = M_{i-r,j} + M_{i-1,j} \qquad \text{für alle } i, j \in \mathbb{Z}_n.$$

Es folgt $\operatorname{rang}(M) \leq r$. Da die erste Zeile von M periodisch mit Periode n ist, sind die letzten $r - 1$ Einträge 0 und die $r \times r$-Teilmatrix oben links ist eine obere Dreiecksmatrix, damit folgt die Gleichheit. □

Weitere Konstruktionen mit verschiedenen Werten für r veranlassten mich nun folgende Vermutungen zu formulieren.

Vermutung 1. *Für $r = 2^k + 1$ mit $k \in \mathbb{N}$ gilt: Die kleinste Periode einer Folge wie in 3.3.1 ist $n = r^2 - r + 1$.*

Vermutung 2. *Eine Matrix M, konstruiert wie in 3.3.2 mit r wie in Vermutung 1, ist ein Foolingset.*

Beide Vermutungen konnte ich für $k = 1, \ldots, 14$ bestätigen. Wenn sie für alle $k \in \mathbb{N}$ gelten würden, so würde folgen, dass $\operatorname{fool}(M) \geq (\operatorname{rang}(M))^{\log_r(r^2-r+1)}$ gilt.
Da $\lim_{r\to\infty} \log_r(r^2 - r + 1) = 2$ gilt, wäre damit gezeigt, dass die Abschätzung von Dietzfelbinger et al. in Theorem 3.1.1 schon bestmöglich ist.
Um die Vermutung für $k = 1, \ldots, 14$ zu bestätigen, brauchte ich folgende Aussage.

Lemma 3.3.6. *Eine wie oben konstruierte Matrix ist ein Foolingset genau dann, wenn gilt*

$$a_j a_{n-j} = 0 \textit{ für } j = 1, \ldots, \frac{n-1}{2}$$

Beweis. Nach Konstruktion gilt für $j > 0$

$$M_{j,0} = M_{j-1,n-1} = M_{j-1-(j-1),n-1-(j-1)} = M_{0,n-j} = a_{n-j}$$

Nun ist M ein Foolingset genau dann wenn,

$$M_{i,j}M_{j,i} = 0 \qquad \text{für alle } i, j \in \mathbb{Z}_n \text{ mit } i \neq j$$

($M_{i,i} = 1$ für alle i aus $\mathbb{Z}_n$ gilt bereits nach Konstruktion). Da nun

$$M_{i,j}M_{j,i} = M_{i-i,j-i}M_{j-i,i-i} = M_{0,j-i}M_{j-i,0} = a_{j-i}a_{n-(j-i)}$$

folgt die Behauptung. □

Es genügt also die ersten Zeilen der Matrizen zu konstruieren, um die vermuteten Eigenschaften zu überprüfen. Dies habe ich in Matlab/Octave implementiert und für $k = 1, \ldots, 14$ getestet. Für $r = 2^k + 1$, war die kleinste Periode der Folge aus 3.3.1 stets $n = r^2 - r + 1$ und die nach 3.3.2 konstruierten Matrizen waren alle Foolingsets. Für $k = 14$ erhält man $\operatorname{rang}(M) = 16\,385$ und $\operatorname{fool}(M) = 268\,451\,841$. Daraus ergibt sich $\operatorname{fool}(M) \geq \operatorname{rang}^{1{,}99999}(M)$.

3.4 Eine weitere Charakterisierung der Konstruktion

Im Folgenden werde ich eine weitere Eigenschaft der Matrizen aus 3.3 vorstellen. Jene gibt zum einen eine weitere Konstruktionsmöglichkeit und zum anderen ein Kriterium, um zu überprüfen, ob n eine Periode einer Folge nach 3.3.1 ist.

Satz 3.4.1. *Zu einer Folge $(a_i)_{i\in\mathbb{N}_0}$ nach 3.3.1 ist n eine Periode, genau dann wenn $x^n + 1$ durch $x^r + x + 1$ in $\mathbb{F}_2[x]$ teilbar ist. Für den Quotienten*

$$p = \frac{x^n + 1}{x^r + x + 1}$$

gilt in diesem Fall

$$p = \sum_{i=0}^{n} a_i x^i$$

(vgl. Theorem 6.25 in [5]).

Beweis. Es seien $(a_0, a_1, \ldots, a_{n-1})$ die ersten Glieder einer Folge nach 3.3.1 und $p = \sum_{i=0}^{n} a_i x^i$ so gilt:

$$\begin{aligned}
(x^r + x + 1)p &= \sum_{i=0}^{n-1} a_i x^{i+r} + \sum_{i=0}^{n-1} a_i x^{i+1} + \sum_{i=0}^{n-1} a_i x^i \\
&= a_0 \\
&\quad + (a_0 + a_1)x + \cdots + (a_{r-2} + a_{r-1})x^{r-1} \\
&\quad + (a_0 + a_{r-1} + a_r)x^r + \cdots + (a_{n-1-r} + a_{n-2} + a_{n-1})x^{n-1} \\
&\quad + (a_{n-r} + a_{n-1})x^n \\
&\quad + a_{n-r+1}x^{n+1} + \cdots + a_{n-1}x^{n+r-1}
\end{aligned}$$

Das heißt $(x^r + x + 1)p = x^n + 1$ ist genau dann erfüllt, wenn folgende Bedingungen gelten:

$$a_0 = 1 \tag{3.1}$$

$$a_{i-1} + a_i = 0 \qquad \text{für } i = 1, \cdots, r-1 \tag{3.2}$$

$$a_{i-r} + a_{i-1} + a_i = 0 \qquad \text{für } i = r, \cdots, n-1 \tag{3.3}$$

$$a_{n-r} + a_{n-1} = 1 \tag{3.4}$$

$$a_i = 0 \qquad \text{für } i = n-r+1, \cdots, n-1 \tag{3.5}$$

Nun sind (3.1) und (3.2) äquivalent zu

$$a_0 = a_1 = \cdots = a_{r-1} = 1 \tag{3.6}$$

und entsprechen also zusammen mit (3.3) der Konstruktionsvorschrift 3.3.1 der Folge.
Desweiteren ist (3.4) mit (3.1) äquivalent zu

$$a_0 = a_{n-r} + a_{n-1}$$

und (3.5) ist mit (3.6) äquivalent zu

$$a_i = a_{n-r+i} + a_{n-1+i} \text{ für } i = 1, \cdots, r-1,$$

das heißt n ist eine Periode der Folge. □

Wenn man nun Aussagen über die Teilbarkeit von $x^n + 1$ durch $x^r + x + 1$ in $\mathbb{F}_2[x]$ treffen kann, hilft das wahrscheinlich, Vermutung 1 zu zeigen. Ich könnte mir außerdem vorstellen, dass diese Charakterisierung auch beim Beweis von Vermutung 2 hilfreich ist.

Kapitel 4

Fazit

Der Schwerpunkt meiner Arbeit lag in der Untersuchung des Zusammenhangs zwischen der maximalen Größe von Foolingsets in Matrizen und dem Rang. Grundlage war der von Diezfelbinger et al. gezeigte Zusammenhang $\mathrm{fool}(M) \leq \mathrm{rang}^2(M)$. Das Rechnen im Körper mit nur zwei Elementen half mir Beispiele zu finden, welche wesentlich näher an dieser Abschätzung sind als die vorher bekannten in $\mathbb{R}$.
Würde man nun allgemeine Beweise der Vermutungen 1 und 2 auf Seite 10 finden, so wäre die Abschätzung von Dietzfelbinger et al. sogar als bestmöglich bewiesen.
Bei einem allgemeinen Beweis dieser Vermutungen könnte möglicherweise die Charakterisierung der Konstruktion durch Polynome helfen.
Da die Beispiele in $\mathbb{F}_2$ so gute Ergebnisse liefern, ist es möglicherweise hilfreich, für Polyeder der Optimierung den Rang über $\mathbb{F}_2$ zu bestimmen. Auf diese Weise kann man Aussagen darüber treffen, ob mithilfe von Foolingsets die Abschätzung der Erweiterungskomplexität verbessert werden könnte oder nicht.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt habe.

Magdeburg, 3. Juli 2012 ______________________________

Mirjam Friesen

Anhang

Matlab/Octave Funktion

```
%Erzeugt die erste Zeile x einer Matrix M
%und überprüft ob M ein Foolingset ist und Rang r hat.


function [ ret ] = check (k)
   r = 2^k + 1;
   n = r^2 - r + 1;

   x = zeros(1 , n + r);
   %r weitere Stellen zum leichten Überprüfen,
   % ob x periodisch mit Periode n ist

   x(1 : r)= 1;
   for i = r + 1 : n + r
      x(i) = xor(x(i - r),x(i - 1));
   end

   %Vektor periodisch? => rang(M) = r
   ret = sum(x(1 : r) == x(n + 1 : n + r)) == r;

   %erzeugte Matrix Foolingset?
   k = (n - 1) / 2 + 1;
   for i = 2 : k
      ret = ret & (x(i) * x(n - i + 2) == 0);
   end
end
```

Literaturverzeichnis

[1] Joel E. Cohen and Uriel G. Rothblum. Nonnegative ranks, decompositions, and factorizations of nonnegative matrices. *Linear Algebra and its Applications*, 190(0):149 – 168, 1993.

[2] Martin Dietzfelbinger, Juraj Hromkovic, and Georg Schnitger. A comparison of two lower-bound methods for communication complexity. *Theoretical Computer Science*, 168(1):39 – 51, 1996.

[3] S. Fiorini, V. Kaibel, K. Pashkovich, and D. O. Theis. Combinatorial Bounds on Nonnegative Rank and Extended Formulations. *ArXiv:1111:0444*, November 2011.

[4] Samuel Fiorini, Serge Massar, Sebastian Pokutta, Hans Raj Tiwary, and Ronald de Wolf. Linear vs. semidefinite extended formulations: Exponential separation and strong lower bounds. In *STOC*, 2012.

[5] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge University Press, 1994.

[6] R.Kipp Martin. Using separation algorithms to generate mixed integer model reformulations. *Operations Research Letters*, 10(3):119 – 128, 1991.

[7] D. O. Theis. On some lower bounds on the number of bicliques needed to cover a bipartite graph. *ArXiv:1203:3961*, August 2007.

[8] Mihalis Yannakakis. Expressing combinatorial optimization problems by linear programs. *Journal of Computer and System Sciences*, 43(3):441 – 466, 1991.

[9] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing(preliminary report). In *Proceedings of the eleventh annual ACM symposium on Theory of computing*, STOC '79, pages 209–213, New York, NY, USA, 1979. ACM.

[10] Günter M. Ziegler. *Lectures on Polytopes*. Graduate Texts in Mathematics; 152 Springer-Verlag New York, 1995.