TECHNISCHE UNIVERSITÄT CHEMNITZ

Fakultät für Informatik

Professur Theoretische Informatik und Informationssicherheit

- Masterarbeit -

Ein Optimierungsproblem aus der Visuellen Kryptographie und seine Eigenschaften

vorgelegt von

Jakob Juhnke

Chemnitz, 15. Juli 2013

Gutachter: Prof. Dr. Hanno Lefmann
Dipl-math. Knut Odermann

Inhaltsverzeichnis

Danksagung

Ich möchte mich hiermit herzlich bei Herrn Prof. Dr. Lefmann der Professur für Theoretische Informatik und Informationssicherheit dafür bedanken, dass er mit seinen Anregungen, Anmerkungen, Hinweisen und kritischen Fragen während aller Phasen dieser Arbeit wesentlich zum Erfolg dieser Arbeit beigetragen hat.

Mein Dank gilt ebenfalls Herrn Prof. Dr. Volker Strehl der Universität Erlangen-Nürnberg für den Beweis der Lemmata 3.3 und 3.4, sowie für die Einführung in erzeugende und hypergeometrische Funktionen. Ohne diese Grundlagen wären viele Aussagen dieser Arbeit nicht möglich gewesen.

Desweiteren möchte ich mich bei Herrn Knut Odermann für seine Hinweise bei mathematischen Problemen und für seine Zweitgutachtertätigkeit bedanken.

Ich bedanke mich an dieser Stelle ebenfalls bei Silvana Freier und meiner Familie für die Unterstützung während des gesamten Masterstudiums. Insbesondere möchte ich Silvana Freier für die großartige organisatorische Hilfe, vor allem in den besonders stressigen Phasen dieser Arbeit, danken.

1 Einleitung

Die *Visuelle Kryptographie* ist ein *Secret-Sharing-Verfahren*, welches 1994 von Moni Naor und Adi Shamir in [8] auf der EUROCRYPT erstmals vorgestellt wurde. Im Allgemeinen werden Secret-Sharing-Verfahren verwendet, um ein zu schützendes Geheimnis in kleinere Teilgeheimnisse zu zerlegen und diese auf die verschiedenen Teilnehmer des Verfahrens zu verteilen. Dabei soll kein Geheimnisträger in der Lage sein, das Geheimnis allein zu rekonstruieren. Lediglich durch Kooperation mehrerer Teilnehmer soll sich das ursprüngliche Geheimnis wieder herstellen lassen.
Bei der Visuellen Kryptographie sind die geheim zu haltenden Informationen in einem (Schwarz-Weiß-)Bild enthalten. Jedes Pixel des Bildes wird, geeignet codiert, auf n (transparente) Folien gedruckt. Durch das Übereinanderlegen von k Folien wird das Bild wieder sichtbar. Bei der Verwendung von weniger als k Folien soll das Bild allerdings nicht erkennbar sein. Sind diese Bedingungen erfüllt, spricht man von einem (k, n)-*Schema der Visuellen Kryptographie*. Durch die Codierung der Pixel ist die Rekonstruktion des geheimen Bildes mit einem Kontrastverlust behaftet. Dieser soll möglichst klein sein, um das Bild gut erkennen zu können. Da das menschliche Auge zur Decodierung verwendet wird, kann hierbei auf Computer verzichtet werden. Nur zur Erstellung der einzelnen Folien wird ein Computer verwendet, da der manuelle Codieraufwand zu groß wäre.
Zur Codierung der einzelnen Pixel werden verschiedene Boolesche Matrizen genutzt. Diese Matrizen sind daher entscheidend für die Erkennbarkeit des rekonstruierten Bildes und haben somit direkten Einfluss auf den Kontrast. Daher müssen geeignete Matrizen gefunden werden, die einen möglichst großen Kontrast liefern.
Die Grundlagen zur Verwendung der Visuellen Kryptographie wurden bereits in [5] behandelt und konkrete Konstruktionen, die einen optimalen Kontrast liefern, wurden vorgestellt. Optimal heißt in diesem Zusammenhang, dass für das Paar (k, n) keine andere Auswahl an Matrizen einen besseren Kontrast liefern kann.
In [10] geben Hofmeister, Krause und Simon ein Lineares Programm $L(k, n)$ an, dessen optimaler Zielfunktionswert dem optimalen Kontrast eines (k, n)-Schemas entspricht. Auf dieser Grundlage werden in der vorliegenden Arbeit verschiedene Struktureigenschaften von zulässigen und optimalen Lösungen für das Lineare Programm $L(k, n)$ angeben. Um diese Aussagen beweisen zu können, werden in Kapitel 2 die nötigen mathematischen

Grundlagen erläutert. Diese beinhalten Kenntnisse zu Binomialkoeffizienten und deren Summen, erzeugende Funktionen sowie hypergeometrische Funktionen.
In Kapitel 3 wird zunächst das (k, n)-Schema nach Naor und Shamir definiert, wie es in [8] angegeben wird. Anschließend wird auf das Lineare Programm $L(k, n)$ von Hofmeister, Krause und Simon aus ihrer Arbeit [10] eingegangen. Dabei werden verschiedene Struktureigenschaften von zulässigen und optimalen Lösungen dargestellt.
Abschließend werden in Kapitel 4 die in Kapitel 3 gewonnenen Erkenntnisse angewandt, um optimale Lösungen für die Fälle $L(k, k)$ und $L(k-1, k)$ zu bestimmen, sowie eine untere Schranke für den optimalen Kontrast aller $(k-2, k)$-Schemata anzugeben.

2 Mathematische Grundlagen

In diesem Kapitel werden die verwendeten mathematischen Aspekte für diese Arbeit erklärt. Dabei wird mit $\mathbb{N} = \{0, 1, 2, \ldots\}$ die Menge der natürlichen Zahlen und mit $\mathbb{C}$ die Menge der komplexen Zahlen bezeichnet.

2.1 Binomialkoeffizienten

Viele kombinatorische Probleme lassen sich mit Hilfe von Binomialkoeffizienten bearbeiten. Je nach Anwendungsfall können dabei unterschiedliche Definitionen von Binomialkoeffizienten Verwendung finden.

Definition 2.1 - Fakultätsfunktion:
Sei $n \in \mathbb{N}$. Dann bezeichnet $n!$ die *Fakultät von* n mit

$$n! = \prod_{i=1}^{n} i.$$

Für $n = 0$ ist das Produkt leer und es gilt $0! = 1$.

Definition 2.2 - Binomialkoeffizient:
Seien $n, k \in \mathbb{N}$ und $0 \leq k \leq n$. Dann ist der Binomialkoeffizient $\binom{n}{k}$ definiert als

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

Durch diese Definition ist es nicht möglich, negative oder gebrochene Zahlen für n zu verwenden, da die Fakultätsfunktion nur für natürliche Zahlen definiert ist. Durch eine Verallgemeinerung wird dieses jedoch ermöglicht.

Definition 2.3 - allgemeiner Binomialkoeffizient:
Seien $a \in \mathbb{C}$ und $k \in \mathbb{N}$. Dann ist der allgemeine Binomialkoeffizient $\binom{a}{k}$ definiert als

$$\binom{a}{k} = \prod_{j=1}^{k} \frac{a+1-j}{j}.$$

Für eine natürliche Zahl $n = a$ ist diese Definition identisch zu Definition 2.2. Deshalb wird selten zwischen den verschiedenen Definitionen unterschieden.
Anstelle der Produktdarstellung des Binomialkoeffizienten kann auch das sogenannte *Pochhammer-Symbol* verwendet werden.

Definition 2.4 - Pochhammer-Symbol:
Seien $a \in \mathbb{C}$ und $n \in \mathbb{N}$. Dann ist das *Pochhammer-Symbol* $(a)_n$ definiert als

$$(a)_n = \prod_{j=1}^{n}(a+j-1) = \begin{cases} a \cdot (a+1) \cdot (a+2) \cdot \ldots \cdot (a+n-1) & n > 0 \\ 1 & n = 0. \end{cases}$$

Aus dieser Definition folgt, dass für jede natürliche Zahl n der Zusammenhang $n! = (1)_n$ gilt. Das Pochhammer-Symbol nach Definition 2.4 wird auch als *steigende Faktorielle* bezeichnet. Den Zusammenhang zwischen Binomialkoeffizienten und dem Pochhammer-Symbol stellt das folgende Lemma her.

Lemma 2.1:
Seien $a \in \mathbb{C}$ und $k \in \mathbb{N}$. Dann gilt

$$\binom{a}{k} = (-1)^k \cdot \frac{(-a)_k}{k!}.$$

Beweis:

$$\begin{aligned} \binom{a}{k} &= \prod_{j=1}^{k} \frac{a+1-j}{j} = \frac{1}{k!} \cdot \prod_{j=1}^{k}(a+1-j) = \frac{(-1)^k}{k!} \cdot \prod_{j=1}^{k}(j-a-1) \\ &= (-1)^k \cdot \frac{(-a)_k}{k!}. \end{aligned}$$

□

Für Binomialkoeffizienten, und damit ebenfalls für das Pochhammer-Symbol, sind viele Eigenschaften und Umformungsregeln bekannt. Die für diese Arbeit wichtigsten werden im Folgenden dargestellt.

Lemma 2.2:
Seien $a \in \mathbb{C}$ und $j, n \in \mathbb{N}$. Dann gilt

$$(a)_{n+j} = (a)_n \cdot (a+n)_j.$$

Beweis:

$$\begin{aligned}(a)_{n+j} &= \prod_{i=1}^{n+j}(a+i-1) = \prod_{i=1}^{n}(a+i-1) \cdot \prod_{i=n+1}^{n+j}(a+i-1) \\ &= \prod_{i=1}^{n}(a+i-1) \cdot \prod_{i=1}^{j}(a+n+i-1) \\ &= (a)_n \cdot (a+n)_j. \end{aligned}$$

□

Lemma 2.3:
Seien $a \in \mathbb{C}$ und $n \in \mathbb{N}$. Dann gilt

$$(a)_n = (-1)^n \cdot (1-a-n)_n.$$

Beweis:

$$\begin{aligned}(a)_n &= \prod_{i=1}^{n}(a+i-1) = (-1)^{2\cdot n} \cdot \prod_{i=1}^{n}(a+i-1) = (-1)^n \cdot \prod_{i=1}^{n}(-a-i+1) \\ &= (-1)^n \cdot \prod_{i=1}^{n}(-a-n+i) = (-1)^n \cdot (1-a-n)_n. \end{aligned}$$

□

Lemma 2.4:
Seien $n, k \in \mathbb{N}$ und $0 \leq k \leq n$. Dann gilt

$$\binom{n}{k} = \binom{n}{n-k}.$$

Beweis:

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} = \frac{n!}{(n-k)! \cdot k!} = \frac{n!}{(n-k)! \cdot (n-(n-k))!} = \binom{n}{n-k}.$$

□

Lemma 2.5:
Seien $n, k \in \mathbb{N}$ und $1 \leq k \leq n$. Dann gilt

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Beweis:

$$\begin{aligned}
\binom{n}{k} &= \frac{n!}{k! \cdot (n-k)!} = \frac{(n-1)! \cdot (n+k-k)}{k! \cdot (n-k)!} \\
&= \frac{(n-1)! \cdot k}{(k-1)! \cdot k \cdot (n-k)!} + \frac{(n-1)! \cdot (n-k)}{k! \cdot (n-k) \cdot (n-k-1)!} \\
&= \frac{(n-1)!}{(k-1)! \cdot (n-k)!} + \frac{(n-1)!}{k! \cdot (n-k-1)!} \\
&= \binom{n-1}{k-1} + \binom{n-1}{k}.
\end{aligned}$$

□

Lemma 2.6:
Sei $a \in \mathbb{C}$ und $k \in \mathbb{N}$. Dann gilt

$$\binom{a}{k} = (-1)^k \cdot \binom{k-a-1}{k}.$$

Beweis:

$$\begin{aligned}
\binom{a}{k} &= \prod_{j=1}^{k} \frac{a+1-j}{j} = \frac{1}{k!} \cdot \prod_{j=1}^{k} (a+1-j) = \frac{1}{k!} \cdot (-1)^k \cdot \prod_{j=1}^{k} (-a-1+j) \\
&= \frac{1}{k!} \cdot (-1)^k \cdot \prod_{j=1}^{k} (k-a-j) = (-1)^k \cdot \prod_{j=1}^{k} \frac{k-a-j}{j} \\
&= (-1)^k \cdot \binom{k-a-1}{k}.
\end{aligned}$$

□

Lemma 2.7:
Seien $r, m, k \in \mathbb{N}$ und $0 \leq k \leq m \leq r$. Dann gilt

$$\binom{r}{m} \cdot \binom{m}{k} = \binom{r}{k} \cdot \binom{r-k}{m-k}.$$

Beweis:

$$\begin{aligned}\binom{r}{m} \cdot \binom{m}{k} &= \frac{r!}{m! \cdot (r-m)!} \cdot \frac{m!}{k! \cdot (m-k)!} \\ &= \frac{r!}{m! \cdot (r-m)!} \cdot \frac{m!}{k! \cdot (m-k)!} \cdot \frac{(r-k)!}{(r-k)!} \\ &= \frac{r!}{k! \cdot (r-k)!} \cdot \frac{(r-k)!}{(m-k)! \cdot (r-m)!} \\ &= \binom{r}{k} \cdot \binom{r-k}{m-k}.\end{aligned}$$

□

Aus Lemma 2.7 folgt direkt, dass auch gilt

$$\binom{m}{k} \cdot \binom{r}{k}^{-1} = \binom{r-k}{m-k} \cdot \binom{r}{m}^{-1}.$$

Lemma 2.8:
Seien $n, k \in \mathbb{N}$ und $0 \leq k \leq n$. Dann gilt

$$\binom{n}{k} = \frac{n}{k} \cdot \binom{n-1}{k-1}.$$

Beweis:

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} = \frac{n}{k} \cdot \frac{(n-1)!}{(k-1)! \cdot (n-k)!} = \frac{n}{k} \cdot \binom{n-1}{k-1}.$$

□

Summen von Binomialkoeffizienten

Mit den bisher vorgestellten Aussagen können viele Umformungen von Binomialkoeffizienten durchgeführt werden. Allerdings treten Binomialkoeffizienten häufig in Summen auf, für die explizite Formeln benötigt werden. Mit Hilfe von *hypergeometrischen Funktionen*, wie sie im Abschnitt 2.3 vorgestellt werden, können solche Summen meistens unkompliziert ausgewertet werden, wenn die entsprechenden Identitäten bekannt sind. Für einfache Summen von Binomialkoeffizienten, welche in dieser Arbeit benötigt werden, sind an dieser Stelle explizite Formeln angegeben.

Lemma 2.9:
Sei $n \in \mathbb{N}$. Dann gilt

$$\sum_{j=0}^{n} \binom{n}{j} = 2^n.$$

Beweis: Beweis per Induktion über n.
Induktionsanfang: $n = 0$:
Es gilt

$$\sum_{j=0}^{0} \binom{n}{j} = \binom{0}{0} = 1 = 2^0.$$

Induktionsvoraussetzung: Die Behauptung sei korrekt für alle $n \leq g$.
Induktionsschritt: $g \longrightarrow g + 1$:

$$\begin{aligned}\sum_{j=0}^{g+1} \binom{g+1}{j} &= 2 + \sum_{j=1}^{g} \left(\binom{g}{j} + \binom{g}{j-1} \right) = 1 + \sum_{j=0}^{g} \binom{g}{j} + \sum_{j=0}^{g-1} \binom{g}{j} \\ &= \sum_{j=0}^{g} \binom{g}{j} + \sum_{j=0}^{g} \binom{g}{j} = 2 \cdot 2^g = 2^{g+1}.\end{aligned}$$

□

Lemma 2.10:
Sei $n \in \mathbb{N}$ und $n > 0$. Dann gilt

$$\sum_{\substack{j=0 \\ j \text{ gerade}}}^{n} \binom{n}{j} = \sum_{\substack{j=0 \\ j \text{ ungerade}}}^{n} \binom{n}{j} = 2^{n-1}.$$

Beweis: Sei n ungerade. Dann gibt es genau $n + 1$, also eine gerade Anzahl, Binomialkoeffizienten $\binom{n}{j}$. Daher ist die Anzahl der Summanden der Summe über die geraden Binomialkoeffizienten identisch zu der Anzahl der Summanden der Summe über die ungeraden Binomialkoeffizienten. Für eine gerade Zahl j ist $n - j$ ungerade und umgekehrt. Durch die Symmetrie von Binomialkoeffizienten gilt daher

$$\sum_{\substack{j=0 \\ j \text{ gerade}}}^{n} \binom{n}{j} = \sum_{\substack{j=0 \\ j \text{ ungerade}}}^{n} \binom{n}{j}.$$

Daraus folgt

$$\sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{n}{j} + \sum_{\substack{j=0\\ j \text{ ungerade}}}^{n} \binom{n}{j} = \sum_{j=0}^{n} \binom{n}{j} = 2^n \qquad \text{nach Lemma 2.9}$$

$$\Longrightarrow \quad \sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{n}{j} = \sum_{\substack{j=0\\ j \text{ ungerade}}}^{n} \binom{n}{j} = 2^{n-1}.$$

Sei $n \geq 2$ gerade. Dann gilt für $n = 2$

$$\sum_{\substack{j=0\\ j \text{ gerade}}}^{2} \binom{2}{j} = \binom{2}{0} + \binom{2}{2} = 2 = 2^1$$

und

$$\sum_{\substack{j=0\\ j \text{ ungerade}}}^{2} \binom{2}{j} = \binom{2}{1} = 2 = 2^1.$$

Damit ist der Induktionsanfang gezeigt.

Induktionsvoraussetzung: Die Behauptung gelte für alle geraden $n \leq g$ mit g gerade.
Induktionsschritt: $g \longrightarrow g + 2$:

$$\begin{aligned}
\sum_{\substack{j=0\\ j \text{ gerade}}}^{g+2} \binom{g+2}{j} &= 2 + \sum_{\substack{j=2\\ j \text{ gerade}}}^{g} \binom{g+2}{j} = 2 + \sum_{\substack{j=2\\ j \text{ gerade}}}^{g} \left(\binom{g+1}{j} + \binom{g+1}{j-1} \right) \\
&= 2 + \sum_{\substack{j=2\\ j \text{ gerade}}}^{g} \binom{g+1}{j} + \sum_{\substack{j=1\\ j \text{ ungerade}}}^{g-1} \binom{g+1}{j} \\
&= 1 + \sum_{\substack{j=0\\ j \text{ gerade}}}^{g+1} \binom{g+1}{j} + \sum_{\substack{j=0\\ j \text{ ungerade}}}^{g+1} \binom{g+1}{j} - 1 \\
&= \sum_{j=0}^{g+1} \binom{g+1}{j} = 2^{g+1} \qquad \text{nach Lemma 2.9.}
\end{aligned}$$

Analog gilt

$$\sum_{\substack{j=0\\ j \text{ ungerade}}}^{g+2} \binom{g+2}{j} = \sum_{\substack{j=1\\ j \text{ ungerade}}}^{g+1} \binom{g+2}{j} = \sum_{\substack{j=1\\ j \text{ ungerade}}}^{g+1} \left(\binom{g+1}{j} + \binom{g+1}{j-1} \right)$$

$$= \sum_{\substack{j=1 \\ j \text{ ungerade}}}^{g+1} \binom{g+1}{j} + \sum_{\substack{j=0 \\ j \text{ gerade}}}^{g} \binom{g+1}{j} = \sum_{j=0}^{g+1} \binom{g+1}{j} = 2^{g+1}. \qquad \square$$

Lemma 2.11:
Sei $n \in \mathbb{N}$. Dann gilt

$$\sum_{j=0}^{n} \binom{2n}{j} = 2^{2n-1} + \frac{1}{2}\binom{2n}{n} \qquad \text{und} \qquad \sum_{j=0}^{n} \binom{2n+1}{j} = 2^{2n}.$$

Beweis: Durch Lemma 2.9 ist bekannt, dass gilt

$$\sum_{j=0}^{2n} \binom{2n}{j} = 2^{2n}.$$

Da $2n$ eine gerade Zahl ist und Binomialkoeffizienten symmetrisch sind, gilt ebenfalls

$$\sum_{j=0}^{n-1} \binom{2n}{j} = \sum_{j=n+1}^{2n} \binom{2n}{j} \qquad \text{und} \qquad \sum_{j=0}^{n-1} \binom{2n}{j} + \sum_{j=n+1}^{2n} \binom{2n}{j} = 2^{2n} - \binom{2n}{n}.$$

Daraus folgt

$$\sum_{j=0}^{n} \binom{2n}{j} = 2^{2n-1} + \frac{1}{2}\binom{2n}{n}.$$

Da $2n+1$ ungerade ist, gilt analog

$$\sum_{j=0}^{n} \binom{2n+1}{j} = \sum_{j=n+1}^{2n+1} \binom{2n+1}{j} \qquad \text{und} \qquad \sum_{j=0}^{n} \binom{2n+1}{j} + \sum_{j=n+1}^{2n+1} \binom{2n+1}{j} = 2^{2n+1}.$$

Daraus folgt

$$\sum_{j=0}^{n} \binom{2n+1}{j} = 2^{2n}. \qquad \square$$

Lemma 2.12:
Sei $n \in \mathbb{N}$. Dann gilt

$$\sum_{j=0}^{n} \binom{2n}{j} \cdot j = \frac{4^n \cdot n}{2}.$$

Beweis: Beweis per Induktion über n.
Induktionsanfang: $n = 0$:
Es gilt

$$\sum_{j=0}^{0} \binom{0}{j} \cdot j = 0 = \frac{4^0 \cdot 0}{2}.$$

Induktionsvoraussetzung: Die Behauptung sei korrekt für alle $n \leq g$.

Induktionsschritt: $g \longrightarrow g+1$:

$$\begin{aligned}
\sum_{j=0}^{g+1} \binom{2g+2}{j} \cdot j &= \sum_{j=1}^{g+1} \binom{2g+2}{j} \cdot j = \sum_{j=1}^{g+1} \binom{2g+1}{j-1} \cdot (2g+2) && \text{nach Lemma 2.8} \\
&= (2g+2) \sum_{j=0}^{g} \binom{2g+1}{j} = (2g+2) \cdot 2^{2g} && \text{nach Lemma 2.11} \\
&= 4^g \cdot 2g + 2 \cdot 4^g = \frac{4^{g+1}(g+1)}{2}. && \square
\end{aligned}$$

Lemma 2.13:
Sei $n \in \mathbb{N}$. Dann gilt

$$\sum_{\substack{j=0 \\ j \text{ gerade}}}^{n} \binom{2n}{j} = 4^{n-1} + \frac{1+(-1)^n}{4} \binom{2n}{n}.$$

Beweis: Durch Lemma 2.10 ist bekannt, dass gilt

$$\sum_{\substack{j=0 \\ j \text{ gerade}}}^{2n} \binom{2n}{j} = 2^{2n-1}.$$

Für ein ungerades n folgt durch die Symmetrie von Binomialkoeffizienten ebenfalls

$$\sum_{\substack{j=0 \\ j \text{ gerade}}}^{n-1} \binom{2n}{j} = \sum_{\substack{j=n+1 \\ j \text{ gerade}}}^{2n} \binom{2n}{j} \qquad \text{und} \qquad \sum_{\substack{j=0 \\ j \text{ gerade}}}^{n-1} \binom{2n}{j} + \sum_{\substack{j=n+1 \\ j \text{ gerade}}}^{2n} \binom{2n}{j} = 2^{2n-1}.$$

Daraus folgt

$$\sum_{\substack{j=0 \\ j \text{ gerade}}}^{n} \binom{2n}{j} = \frac{2^{2n-1}}{2} = 4^{n-1}.$$

Für ein gerades n gilt analog

$$\sum_{\substack{j=0\\ j \text{ gerade}}}^{n-2} \binom{2n}{j} = \sum_{\substack{j=n+2\\ j \text{ gerade}}}^{2n} \binom{2n}{j} \qquad \text{und} \qquad \sum_{\substack{j=0\\ j \text{ gerade}}}^{n-2} \binom{2n}{j} + \sum_{\substack{j=n+2\\ j \text{ gerade}}}^{2n} \binom{2n}{j} = 2^{2n-1} - \binom{2n}{n}.$$

Daraus folgt

$$\sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{2n}{j} = \frac{1}{2}\left(2^{2n-1} - \binom{2n}{n}\right) + \binom{2n}{n} = 4^{n-1} + \frac{1}{2}\binom{2n}{n}. \qquad \square$$

Lemma 2.14:
Sei $n \in \mathbb{N}$. Dann gilt

$$\sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{2n+1}{j} = 2^{2n-1} + \frac{(-1)^n}{2}\binom{2n}{n}.$$

Beweis: Es gilt

$$\begin{aligned}\sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{2n+1}{j} &= 1 + \sum_{\substack{j=2\\ j \text{ gerade}}}^{n} \binom{2n+1}{j} = 1 + \sum_{\substack{j=2\\ j \text{ gerade}}}^{n} \binom{2n}{j} + \sum_{\substack{j=2\\ j \text{ gerade}}}^{n} \binom{2n}{j-1} \\ &= \sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{2n}{j} + \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-1} \binom{2n}{j}.\end{aligned}$$

Mit n gerade folgt

$$\sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{2n}{j} + \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-1} \binom{2n}{j} = \sum_{j=0}^{n} \binom{2n}{j} = 2^{2n-1} + \frac{1}{2}\binom{2n}{n} \qquad \text{nach Lemma 2.11.}$$

Für n ungerade hingegen folgt

$$\sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{2n}{j} + \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-1} \binom{2n}{j} = \sum_{j=0}^{n-1} \binom{2n}{j} = 2^{2n-1} - \frac{1}{2}\binom{2n}{n} \qquad \text{nach Lemma 2.11.}$$

$\square$

Lemma 2.15:
Sei $n \in \mathbb{N}$. Dann gilt

$$\sum_{\substack{j=0 \\ j \text{ gerade}}}^{n} \binom{n}{j} j = \sum_{\substack{j=0 \\ j \text{ ungerade}}}^{n} \binom{n}{j} j = n \cdot 2^{n-2}.$$

Beweis: Sei n gerade. Dann gilt

$$\begin{aligned}
\sum_{\substack{j=0 \\ j \text{ gerade}}}^{n} \binom{n}{j} j &= n + \sum_{\substack{j=2 \\ j \text{ gerade}}}^{n-2} \binom{n}{j} j = n + n \sum_{\substack{j=2 \\ j \text{ gerade}}}^{n-2} \binom{n-1}{j-1} && \text{nach Lemma 2.8} \\
&= n \left[1 + \sum_{\substack{j=1 \\ j \text{ ungerade}}}^{n-3} \binom{n-1}{j} \right] = n \sum_{\substack{j=1 \\ j \text{ ungerade}}}^{n-1} \binom{n-1}{j} \\
&= n \cdot 2^{n-2} && \text{nach Lemma 2.10}
\end{aligned}$$

und

$$\begin{aligned}
\sum_{\substack{j=0 \\ j \text{ ungerade}}}^{n} \binom{n}{j} j &= \sum_{\substack{j=1 \\ j \text{ ungerade}}}^{n-1} \binom{n}{j} j = n \sum_{\substack{j=1 \\ j \text{ ungerade}}}^{n-1} \binom{n-1}{j-1} = n \sum_{\substack{j=0 \\ j \text{ gerade}}}^{n-2} \binom{n-1}{j} \\
&= n \sum_{\substack{j=0 \\ j \text{ gerade}}}^{n-1} \binom{n-1}{j} = n \cdot 2^{n-2} && \text{nach Lemma 2.10.}
\end{aligned}$$

Sei n ungerade. Dann gilt

$$\begin{aligned}
\sum_{\substack{j=0 \\ j \text{ gerade}}}^{n} \binom{n}{j} j &= \sum_{\substack{j=2 \\ j \text{ gerade}}}^{n-1} \binom{n}{j} j = n \sum_{\substack{j=2 \\ j \text{ gerade}}}^{n-1} \binom{n-1}{j-1} && \text{nach Lemma 2.8} \\
&= n \sum_{\substack{j=1 \\ j \text{ ungerade}}}^{n-2} \binom{n-1}{j} = n \sum_{\substack{j=0 \\ j \text{ ungerade}}}^{n-1} \binom{n-1}{j} \\
&= n \cdot 2^{n-2} && \text{nach Lemma 2.10}
\end{aligned}$$

und

$$\sum_{\substack{j=0 \\ j \text{ ungerade}}}^{n} \binom{n}{j} j = n + \sum_{\substack{j=1 \\ j \text{ ungerade}}}^{n-2} \binom{n}{j} j = n + n \sum_{\substack{j=1 \\ j \text{ ungerade}}}^{n-2} \binom{n-1}{j-1} = n \left[1 + \sum_{\substack{j=0 \\ j \text{ gerade}}}^{n-3} \binom{n-1}{j} \right]$$

$$= n \sum_{\substack{j=0 \\ j \text{ gerade}}}^{n-1} \binom{n-1}{j} = n \cdot 2^{n-2} \qquad \text{nach Lemma 2.10,}$$

wie behauptet. □

Lemma 2.16:
Sei $n \in \mathbb{N}$. Dann gilt

$$\sum_{\substack{j=0 \\ j \text{ gerade}}}^{n} \binom{2n+1}{j} j = (2n+1) \cdot \left[2^{2n-2} - \frac{1-(-1)^n}{4} \binom{2n}{n} \right].$$

Beweis: Es gilt

$$\sum_{\substack{j=0 \\ j \text{ gerade}}}^{n} \binom{2n+1}{j} j = \sum_{\substack{j=2 \\ j \text{ gerade}}}^{n} \binom{2n+1}{j} j = (2n+1) \sum_{\substack{j=2 \\ j \text{ gerade}}}^{n} \binom{2n}{j-1} \qquad \text{nach Lemma 2.8}$$

$$= (2n+1) \sum_{\substack{j=1 \\ j \text{ ungerade}}}^{n-1} \binom{2n}{j}.$$

Da $2n$ gerade ist, folgt aus der Symmetrie von Binomialkoeffizienten und Lemma 2.10 für gerades n

$$\sum_{\substack{j=0 \\ j \text{ ungerade}}}^{n-1} \binom{2n}{j} = \sum_{\substack{j=n+1 \\ j \text{ ungerade}}}^{2n} \binom{2n}{j} \qquad \text{und} \qquad \sum_{\substack{j=0 \\ j \text{ ungerade}}}^{n-1} \binom{2n}{j} + \sum_{\substack{j=n+1 \\ j \text{ ungerade}}}^{2n} \binom{2n}{j} = 2^{2n-1}.$$

Demnach gilt

$$\sum_{\substack{j=0 \\ j \text{ ungerade}}}^{n-1} \binom{2n}{j} = \frac{1}{2} \cdot 2^{2n-1} = 2^{2n-2}$$

$$\Longrightarrow \quad \sum_{\substack{j=0 \\ j \text{ gerade}}}^{n} \binom{2n+1}{j} j = (2n+1) \cdot 2^{2n-2}.$$

Analog gilt für ungerades n

$$\sum_{\substack{j=0 \\ j \text{ ungerade}}}^{n-2} \binom{2n}{j} = \sum_{\substack{j=n+2 \\ j \text{ ungerade}}}^{2n} \binom{2n}{j}$$

und

$$\sum_{\substack{j=0\\ j \text{ ungerade}}}^{n-2} \binom{2n}{j} + \sum_{\substack{j=n+2\\ j \text{ ungerade}}}^{2n} \binom{2n}{j} = 2^{2n-1} - \binom{2n}{n}.$$

Daraus folgt für ungerades n

$$\sum_{\substack{j=0\\ j \text{ ungerade}}}^{n-1} \binom{2n}{j} = \frac{1}{2} \cdot \left(2^{2n-1} - \binom{2n}{n}\right) = 2^{2n-2} - \frac{1}{2}\binom{2n}{n}$$

$$\Longrightarrow \quad \sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{2n+1}{j} j = (2n+1) \cdot \left(2^{2n-2} - \frac{1}{2}\binom{2n}{n}\right).$$

Zusammengefasst gilt damit

$$\sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{2n+1}{j} j = (2n+1) \cdot \left[2^{2n-2} - \frac{1-(-1)^n}{4}\binom{2n}{n}\right]. \qquad \square$$

Lemma 2.17:
Sei $n \in \mathbb{N}$. Dann gilt

$$\sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{n}{j} j^2 = \sum_{\substack{j=0\\ j \text{ ungerade}}}^{n} \binom{n}{j} j^2 = n(n+1) \cdot 2^{n-3}.$$

Beweis: Sei n gerade. Dann gilt

$$\begin{aligned}
\sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{n}{j} j^2 &= n^2 + \sum_{\substack{j=2\\ j \text{ gerade}}}^{n-2} \binom{n}{j} j^2 = n^2 + n \sum_{\substack{j=2\\ j \text{ gerade}}}^{n-2} \binom{n-1}{j-1} j \qquad \text{nach Lemma 2.8} \\
&= n^2 + n \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-3} \binom{n-1}{j} (j+1) \\
&= n^2 + n \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-3} \binom{n-1}{j} j + n \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-3} \binom{n-1}{j} \\
&= n^2 + n \left[\sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-1} \binom{n-1}{j} j - (n-1) + \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-1} \binom{n-1}{j} - 1 \right]
\end{aligned}$$

$$= n^2 + n\left[\sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-1} \binom{n-1}{j} j - n + 2^{n-2}\right] \qquad \text{nach Lemma 2.10}$$

$$= n^2 + n\left[(n-1)\cdot 2^{n-3} - n + 2^{n-2}\right] \qquad \text{nach Lemma 2.15}$$

$$= n(n+1)\cdot 2^{n-3}$$

und

$$\sum_{\substack{j=0\\ j \text{ ungerade}}}^{n} \binom{n}{j} j^2 = \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-1} \binom{n}{j} j^2 = n \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-1} \binom{n-1}{j-1} j \qquad \text{nach Lemma 2.8}$$

$$= n \sum_{\substack{j=0\\ j \text{ gerade}}}^{n-2} \binom{n-1}{j}(j+1) = n \sum_{\substack{j=0\\ j \text{ gerade}}}^{n-2} \binom{n-1}{j} j + n \sum_{\substack{j=0\\ j \text{ gerade}}}^{n-2} \binom{n-1}{j}$$

$$= n\left[\sum_{\substack{j=0\\ j \text{ gerade}}}^{n-1} \binom{n-1}{j} j + \sum_{\substack{j=0\\ j \text{ gerade}}}^{n-1} \binom{n-1}{j}\right]$$

$$= n\left[\sum_{\substack{j=0\\ j \text{ gerade}}}^{n-1} \binom{n-1}{j} j + 2^{n-2}\right] \qquad \text{nach Lemma 2.10}$$

$$= n\left[(n-1)\cdot 2^{n-3} + 2^{n-2}\right] = n(n+1)\cdot 2^{n-3} \qquad \text{nach Lemma 2.15.}$$

Sei n ungerade. Dann gilt

$$\sum_{\substack{j=0\\ j \text{ gerade}}}^{n} \binom{n}{j} j^2 = \sum_{\substack{j=2\\ j \text{ gerade}}}^{n-1} \binom{n}{j} j^2 = n \sum_{\substack{j=2\\ j \text{ gerade}}}^{n-1} \binom{n-1}{j-1} j \qquad \text{nach Lemma 2.8}$$

$$= n \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-2} \binom{n-1}{j}(j+1) = n \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-2} \binom{n-1}{j} j + n \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-2} \binom{n-1}{j}$$

$$= n\left[\sum_{\substack{j=0\\ j \text{ ungerade}}}^{n-1} \binom{n-1}{j} j + \sum_{\substack{j=0\\ j \text{ ungerade}}}^{n-1} \binom{n-1}{j}\right]$$

$$= n\left[\sum_{\substack{j=0\\ j \text{ ungerade}}}^{n-1} \binom{n-1}{j} j + 2^{n-2}\right] \qquad \text{nach Lemma 2.10}$$

$$= n\left[(n-1)\cdot 2^{n-3} + 2^{n-2}\right] = n(n+1)\cdot 2^{n-3} \qquad \text{nach Lemma 2.15}$$

und

$$\begin{aligned}
\sum_{\substack{j=0\\ j \text{ ungerade}}}^{n} \binom{n}{j} j^2 &= n^2 + \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-2} \binom{n}{j} j^2 = n^2 + n \sum_{\substack{j=1\\ j \text{ ungerade}}}^{n-2} \binom{n-1}{j-1} j \quad \text{nach Lemma 2.8} \\
&= n^2 + n \sum_{\substack{j=0\\ j \text{ gerade}}}^{n-3} \binom{n-1}{j} (j+1) \\
&= n^2 + n \sum_{\substack{j=0\\ j \text{ gerade}}}^{n-3} \binom{n-1}{j} j + n \sum_{\substack{j=0\\ j \text{ gerade}}}^{n-3} \binom{n-1}{j} \\
&= n^2 + n \left[\sum_{\substack{j=0\\ j \text{ gerade}}}^{n-1} \binom{n-1}{j} j - (n-1) + \sum_{\substack{j=0\\ j \text{ gerade}}}^{n-1} \binom{n-1}{j} - 1 \right] \\
&= n^2 + n \left[\sum_{\substack{j=0\\ j \text{ gerade}}}^{n-1} \binom{n-1}{j} j - n + 2^{n-2} \right] \quad \text{nach Lemma 2.10} \\
&= n^2 + n \left[(n-1) \cdot 2^{n-3} - n + 2^{n-2} \right] \quad \text{nach Lemma 2.15} \\
&= n(n+1) \cdot 2^{n-3}. \qquad \square
\end{aligned}$$

Lemma 2.18:
Seien $n, a \in \mathbb{N}$. Dann gilt für alle $a \geq 1$

$$\sum_{j=0}^{n} \binom{n}{j} \cdot (-1)^j \cdot \frac{1}{j+a} = \frac{1}{a \cdot \binom{n+a}{a}}. \tag{2.1}$$

Beweis: Beweis per Induktion über n.
Induktionsanfang: $n = 0$:
Es gilt für alle $a \geq 1$

$$\sum_{j=0}^{0} \binom{0}{j} \cdot (-1)^j \cdot \frac{1}{j+a} = 1 \cdot (-1)^0 \cdot \frac{1}{a} = \frac{1}{a} = \frac{1}{a \cdot \binom{0+a}{a}}.$$

Induktionsvoraussetzung: Die Formel (2.1) sei korrekt für alle $n \leq g$ und für alle $a \geq 1$.

Induktionsschritt: $g \longrightarrow g+1$:

$$\sum_{j=0}^{g+1} \binom{g+1}{j} \cdot (-1)^j \cdot \frac{1}{j+a}$$

$$= \sum_{j=1}^{g} \binom{g}{j} \cdot (-1)^j \cdot \frac{1}{j+a} + \sum_{j=1}^{g} \binom{g}{j-1} \cdot (-1)^j \cdot \frac{1}{j+a} + \frac{1}{a} + (-1)^{g+1} \cdot \frac{1}{g+1+a}$$

nach Lemma 2.5

$$= \sum_{j=0}^{g} \binom{g}{j} \cdot (-1)^j \cdot \frac{1}{j+a} + \sum_{j=0}^{g} \binom{g}{j} \cdot (-1)^{j+1} \cdot \frac{1}{j+a+1}$$

$$= \sum_{j=0}^{g} \binom{g}{j} \cdot (-1)^j \cdot \frac{1}{j+a} - \sum_{j=0}^{g} \binom{g}{j} \cdot (-1)^j \cdot \frac{1}{j+(a+1)}$$

$$= \frac{1}{a \cdot \binom{g+a}{a}} - \frac{1}{(a+1) \cdot \binom{g+a+1}{a+1}}$$ nach Induktionsvoraussetzung

$$= \binom{g+a}{g}^{-1} \cdot \left(\frac{1}{a} - \frac{1}{(g+a+1)} \right) = \binom{g+a}{g}^{-1} \cdot \frac{g+1}{a \cdot (a+g+1)}$$

$$= \frac{1}{a} \cdot \binom{a+g+1}{g+1}^{-1}$$ nach Lemma 2.8.

□

2.2 Erzeugende Funktionen

Wenn sich eine Funktion $F(x,t)$ durch eine Potenzreihenentwicklung in t darstellen lässt als

$$F(x,t) = \sum_{j \geq 0} f_j(x) \cdot t^j, \tag{2.2}$$

wobei diese nicht notwendiger Weise konvergieren muss, dann sind die $f_j(x)$ als Koeffizienten von t^j, im Allgemeinen, Funktionen von x. Man sagt, die Menge der Funktionen $f_j(x)$ wurde durch die Reihenentwicklung von $F(x,t)$ *erzeugt* und $F(x,t)$ ist eine *erzeugende Funktion* der $f_j(x)$. Sind die Funktionen $f_j(x), j \geq 0$, bekannt und lässt sich die Summe in (2.2) bestimmen, dann ist auch die erzeugende Funktion $F(x,t)$ bekannt.
Die Summe (2.2) läuft über alle ganzen Zahlen $j \geq 0$. Diese Einschränkung ist nicht notwendig, wenn aus dem Summanden deutlich wird, welche Werte für j zulässig sind. Dazu definiert man $f_j(x) := 0$ für $j < 0$. Dadurch treten keine Probleme auf, wenn durch Umformungen der erzeugenden Funktionen negative Indizes entstehen.
Durch Untersuchungen der erzeugenden Funktionen $F(x,t)$ können Aussagen über die er-

zeugten Funktionen $f_j(x)$ abgeleitet werden. Besonders im Kontext von Funktionen, die Binomialkoeffizienten enthalten, stellen erzeugende Funktionen ein mächtiges Hilfsmittel dar, um Umformungen zu ermöglichen. Oft benötigt man einzelne Funktionen $f_j(x)$, die jedoch in der erzeugenden Funktion $F(x,t)$ verborgen sind. Um diese dennoch direkt angeben zu können, wird die Notation

$$[t^j]F(x,t) := f_j(x)$$

verwendet. Mit $[t^j]F(x,t)$ wird also der Koeffizient von t^j in $F(x,t)$ bezeichnet.
Da die Funktionen $f_j(x)$ für $j = 0, 1, 2, \ldots$ aufgezählt werden, kann man die $f_j(x)$ auch als Folge (f_j) betrachten. Erzeugende Funktionen stellen somit eine Möglichkeit dar, Folgen anzugeben. Für die Folge $(a_n) = (a_0, a_1, a_2, \ldots)$ ist nach (2.2) die erzeugende Funktion gegeben durch

$$A(t) = \sum_j a_j \cdot t^j.$$

Eine wichtige Eigenschaft erzeugender Funktionen ist, dass die Faltung zweier Folgen der Multiplikation der entsprechenden erzeugenden Funktionen entspricht. Um dieses zu zeigen, sei $A(t)$ die erzeugende Funktion der Folge $(a_0, a_1, \ldots)$ und $B(t)$ die erzeugende Funktion der Folge $(b_0, b_1, \ldots)$. Das Produkt von $A(t)$ und $B(t)$ ist dann

$$\begin{aligned} A(t) \cdot B(t) &= (a_0 + a_1 \cdot t + a_2 \cdot t^2 + \ldots) \cdot (b_0 + b_1 \cdot t + b_2 \cdot t^2 + \ldots) \\ &= a_0 \cdot b_0 + (a_0 \cdot b_1 + a_1 \cdot b_0) \cdot t + (a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0) \cdot t^2 + \ldots. \end{aligned}$$

Der Koeffizient von t^n in diesem Produkt ist also

$$\begin{aligned} [t^n](A(t) \cdot B(t)) &= a_0 \cdot b_n + a_1 \cdot b_{n-1} + a_2 \cdot b_{n-2} + \ldots + a_{n-1} \cdot b_1 + a_n \cdot b_0 \\ &= \sum_j a_j \cdot b_{n-j}. \end{aligned}$$

Dieses entspricht der Definition der Faltung zweier Folgen. Ist dabei eine Folge endlich, besteht also aus den $k+1$ Folgengliedern $c_0, c_1, \ldots, c_k$, dann wird diese unendlich fortgesetzt durch die Definition $c_j := 0$ für $j > k$ und der Summationsbereich umfasst die Werte $j = 0, \ldots, k$. Betrachtet man also Folgen durch ihre entsprechenden erzeugenden Funktionen, wird immer angenommen, dass die Folgen für alle $j \in \mathbb{Z}$ definiert sind.

Beispiel

Um zu verdeutlichen, wie erzeugende Funktionen für Beweise über Binomialkoeffizienten genutzt werden können, soll an dieser Stelle die bekannte Identität von Vandermonde

$$\sum_k \binom{r}{k} \cdot \binom{s}{n-k} = \sum_{k=0}^{n} \binom{r}{k} \cdot \binom{s}{n-k} = \binom{r+s}{n}$$

gezeigt werden.
Für die Folge $\left(\binom{r}{0}, \binom{r}{1}, \binom{r}{2}, \ldots\right)$ ist $(1+t)^r$ die erzeugende Funktion. Es gilt also

$$(1+t)^r = \sum_k \binom{r}{k} \cdot t^k$$

und

$$(1+t)^s = \sum_k \binom{s}{k} \cdot t^k.$$

Multipliziert man nun beide erzeugenden Funktionen, erhält man

$$\begin{aligned} (1+t)^r \cdot (1+t)^s &= (1+t)^{r+s} \\ \Longrightarrow [t^n]((1+t)^r \cdot (1+t)^s) = \sum_k \binom{r}{k} \cdot \binom{s}{n-k} &= [t^n]((1+t)^{r+s}) = \binom{r+s}{n}. \end{aligned}$$

Damit ist die Identität von Vandermonde gezeigt.
Für weitere Informationen zu erzeugenden Funktionen sei auf [2], [4] und [9] verwiesen.

2.3 Hypergeometrische Funktionen

Hypergeometrische Funktionen sind ein mächtiges Werkzeug, um Summen von Binomialkoeffizienten zu untersuchen. Jedoch finden sie auch in vielen anderen Bereichen Anwendung, da sich eine Vielzahl an Funktionen als hypergeometrische Funktionen darstellen lassen. An dieser Stelle soll nur eine kurze Einführung zu dieser Thematik gegeben werden. Für weitere Informationen sei auf [2], [3] und [9] verwiesen.

Definition 2.5 - Hypergeometrische Funktion:
Seien $a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q, z \in \mathbb{C}$ mit $b_i \notin \{0, -1-2, \ldots\}$ für alle $i = 1, \ldots, q$. Dann ist die *hypergeometrische Funktion* ${}_pF_q$ definiert als

$$ {}_pF_q\left(\begin{matrix} a_1, \ldots, a_p \\ b_1, \ldots, b_q \end{matrix} ; z \right) := \sum_{n=0}^{\infty} \frac{(a_1)_n \cdot \ldots \cdot (a_p)_n}{(b_1)_n \cdot \ldots \cdot (b_q)_n} \cdot \frac{z^n}{n!}, $$

wobei $(c)_n$ das Pochhammer-Symbol nach Definition 2.4 ist.

Im Allgemeinen wird die Frage nach der Konvergenz einer hypergeometrischen Funktion ignoriert, da das Argument z lediglich als ein Symbol fungiert. Sobald jedoch ein konkreter Wert für z eingesetzt wird, muss verifiziert werden, dass die Funktion wohldefiniert ist.
Viele elementare Funktionen lassen sich als hypergeometrische Funktion darstellen, wie die folgende Übersicht zeigt:

$$ \sin x = x \cdot {}_0F_1\left(\begin{matrix} \\ \frac{3}{2} \end{matrix} ; -\frac{x^2}{4} \right) \qquad \cos x = {}_0F_1\left(\begin{matrix} \\ \frac{1}{2} \end{matrix} ; -\frac{x^2}{4} \right) $$

$$ e^x = {}_0F_0\left(\begin{matrix} \\ \end{matrix} ; x \right) \qquad (1+x)^a = {}_1F_0\left(\begin{matrix} -a \\ \end{matrix} ; -z \right) \quad \text{für } a \in \mathbb{Z}. $$

Im Laufe der Zeit wurden viele hypergeometrische Funktionen untersucht, sodass eine Vielzahl an Identitäten bekannt ist, mit denen solche Funktionen umgeformt werden können. Die einzigen, für diese Arbeit relevanten Aussagen, sind die Identität von Chu und Vandermonde, die Formel von Pfaff und Saalschütz, sowie eine Transformation für ${}_3F_2$-Reihen.

Satz 2.1 (Chu-Vandermonde):
Seien $b, c \in \mathbb{C}$ und $m \in \mathbb{N}$. Dann gilt

$$ {}_2F_1\left(\begin{matrix} -m, b \\ c \end{matrix} ; 1 \right) = \frac{(c-b)_m}{(c)_m}. $$

Satz 2.2 (Pfaff-Saalschütz):
Seien $a, b, c, d \in \mathbb{C}, m \in \mathbb{N}$ und es gelte $d = 1 + a + b - c - m$. Dann gilt

$$ {}_3F_2\left(\begin{matrix} a, b, -m \\ c, d \end{matrix} ; 1 \right) = \frac{(c-a)_m \cdot (c-b)_m}{(c)_m \cdot (c-a-b)_m}. $$

Beweise zu diesen Sätzen sind unter anderem in [3] zu finden.

Für ${}_3F_2$-Reihen ist der Satz 2.2 nur anwendbar, wenn für den Parameter $d = 1 + a + b - c - m$ gilt. Da dieses nicht immer der Fall ist, werden Transformationen benötigt, um die betreffenden Reihen umformen zu können. Eine dieser Transformationen ist in Lemma 2.19 angegeben.

Lemma 2.19:
Seien $a_1, a_2, a_3, b_1, b_2, z \in \mathbb{C}$. Dann gilt

$$(a_2 - a_3) \cdot {}_3F_2\left(\begin{matrix} a_1, a_2, a_3 \\ b_1, b_2 \end{matrix} ; z \right) = a_2 \cdot {}_3F_2\left(\begin{matrix} a_1, a_2 + 1, a_3 \\ b_1, b_2 \end{matrix} ; z \right) - a_3 \cdot {}_3F_2\left(\begin{matrix} a_1, a_2, a_3 + 1 \\ b_1, b_2 \end{matrix} ; z \right).$$

Beweis:

$$\begin{aligned}
&(a_2 - a_3) \cdot {}_3F_2\left(\begin{matrix} a_1, a_2, a_3 \\ b_1, b_2 \end{matrix} ; z \right) = (a_2 - a_3) \cdot \sum_{j=0}^{\infty} \frac{(a_1)_j \cdot (a_2)_j \cdot (a_3)_j}{(b_1)_j \cdot (b_2)_j} \cdot \frac{z^j}{j!} \\
&= \sum_{j=0}^{\infty} \frac{(a_1)_j \cdot (a_2)_j \cdot (a_3)_j}{(b_1)_j \cdot (b_2)_j} \cdot (a_2 + j - a_3 - j) \cdot \frac{z^j}{j!} \\
&= \sum_{j=0}^{\infty} \frac{(a_1)_j \cdot (a_2 + j) \cdot (a_2)_j \cdot (a_3)_j}{(b_1)_j \cdot (b_2)_j} \cdot \frac{z^j}{j!} - \sum_{j=0}^{\infty} \frac{(a_1)_j \cdot (a_2)_j \cdot (a_3 + j) \cdot (a_3)_j}{(b_1)_j \cdot (b_2)_j} \cdot \frac{z^j}{j!} \\
&= \sum_{j=0}^{\infty} \frac{(a_1)_j \cdot a_2 \cdot (a_2 + 1)_j \cdot (a_3)_j}{(b_1)_j \cdot (b_2)_j} \cdot \frac{z^j}{j!} - \sum_{j=0}^{\infty} \frac{(a_1)_j \cdot (a_2)_j \cdot a_3 \cdot (a_3 + 1)_j}{(b_1)_j \cdot (b_2)_j} \cdot \frac{z^j}{j!} \\
&= a_2 \cdot \sum_{j=0}^{\infty} \frac{(a_1)_j \cdot (a_2 + 1)_j \cdot (a_3)_j}{(b_1)_j \cdot (b_2)_j} \cdot \frac{z^j}{j!} - a_3 \cdot \sum_{j=0}^{\infty} \frac{(a_1)_j \cdot (a_2)_j \cdot (a_3 + 1)_j}{(b_1)_j \cdot (b_2)_j} \cdot \frac{z^j}{j!} \\
&= a_2 \cdot {}_3F_2\left(\begin{matrix} a_1, a_2 + 1, a_3 \\ b_1, b_2 \end{matrix} ; z \right) - a_3 \cdot {}_3F_2\left(\begin{matrix} a_1, a_2, a_3 + 1 \\ b_1, b_2 \end{matrix} ; z \right).
\end{aligned}$$

□

3 Visuelle Kryptographie und Lineare Programmierung

Aufbauend auf der Arbeit [8] von Naor und Shamir haben Hofmeister, Krause und Simon in [10] ein Lineares Programm $L(k, n)$ angegeben, dessen Zielfunktionswert dem optimalen Kontrast eines (k, n)-Schemas der Visuellen Kryptographie entspricht. Die Grundlagen zur Verwendung dieser Linearen Programme wurden bereits in [5] diskutiert. Ebenfalls wurden Lösungen zu konkreten Schemata bestimmt. Im ersten Teil dieses Kapitels werden daher nur die wichtigsten Aussagen der Arbeit [10] von Hofmeister, Krause und Simon wiederholt. Im zweiten Teil dieses Kapitels werden allgemeine Struktureigenschaften zulässiger und optimaler Lösungen des Linearen Programms $L(k, n)$ vorgestellt.

3.1 Das Lineare Programm $L(k, n)$

Um den Begriff des (k, n)-Schemas definieren zu können, werden die folgenden Definitionen benötigt.

Definition 3.1 - Hamming-Gewicht:
Sei $v \in \{0, 1\}^n$ ein Vektor der Länge n mit Einträgen aus $\{0, 1\}$. Dann heißt

$$H(v) = |\{j | v_j = 1\}|$$

das *Hamming-Gewicht* von v (Anzahl an Einsen im Vektor v).

Definition 3.2 - komponentenweise Disjunktion:
Seien $v = (v_1, \ldots, v_n) \in \{0, 1\}^n$ und $w = (w_1, \ldots, w_n) \in \{0, 1\}^n$ zwei Vektoren. Dann ist die *(komponentenweise) Disjunktion* $v \vee w$ von v und w definiert durch

$$v \vee w = (v_1 \vee w_1, v_2 \vee w_2, \ldots, v_n \vee w_n),$$

wobei $v_i \vee w_i = 0$ nur dann gilt, wenn $v_i = w_i = 0$ ist. Ansonsten ist $v_i \vee w_i = 1$.

Mit Hilfe dieser Begriffe kann das (k, n)-Schema der Visuellen Kryptographie nach Naor und Shamir [8] wie folgt definiert werden.

Definition 3.3 - (k, n)-Schema:
Ein (k, n)-Schema der Visuellen Kryptographie besteht aus zwei Familien von Booleschen $n \times m$-Matrizen C_0 und C_1. Um ein weißes Pixel zu codieren, wird zufällig eine Matrix aus C_0 gewählt, für schwarze Pixel aus C_1. Die gewählte Matrix legt die Farben aller m Subpixel auf den n Folien fest. Das Schema wird als *gültig* (*valid*) bezeichnet, wenn die folgenden drei Bedingungen erfüllt sind:

1. Für jede Matrix M aus C_0 gilt:
   Sei v ein Vektor, der aus der komponentenweisen Disjunktion von k beliebigen Zeilen aus M entsteht. Dann gilt $H(v) \leq d - \alpha \cdot m$.

2. Für jede Matrix M aus C_1 gilt:
   Sei v ein Vektor, der aus der komponentenweisen Disjunktion von k beliebigen Zeilen aus M entsteht. Dann gilt $H(v) \geq d$.

3. Für alle Teilmengen $\{i_1, i_2, \ldots, i_q\} \subset \{1, \ldots, n\}$ mit $q < k$ gilt:
   Beschränkt man sich bei den Matrizen aus C_0 und C_1 auf die Zeilen $i_1, \ldots, i_q$, so entstehen die zwei Klassen D_0 und D_1, welche $q \times m$-Matrizen enthalten. Diese beiden Klassen sind nicht unterscheidbar in dem Sinn, dass sie die selben Matrizen mit den selben relativen Häufigkeiten enthalten.

Die ersten beiden Bedingungen werden als *Kontrastbedingungen*, die dritte als *Sicherheitsbedingung* bezeichnet. Durch sie wird garantiert, dass keine Informationen aus weniger als k verschiedenen Folien gewonnen werden können.
Aus den Kontrastbedingungen in Definition 3.3 folgt, dass die Anzahl m der Subpixel und der Kontrast α die zwei wichtigsten Parameter eines (k, n)-Schemas sind. Da ein Pixel bei praktischen Anwendungen nicht weiter zerlegt werden kann, muss ein Pixel bei der Codierung durch die m Subpixel ersetzt werden. Dadurch verliert das Gesamtbild gegenüber dem Originalbild an Auflösung. Aus diesem Grund wird der Parameter m auch als *Pixelexpansion* bezeichnet. Außerdem beeinflusst m den Aufwand der Codierung. Daher sollte der Wert für m möglichst klein sein.
Der Parameter d wird als Schwellwert bezeichnet. Alle schwarzen Pixel des Bildes müssen durch einen Grauton von mindestens d dargestellt werden, wohingegen weiße Pixel einen geringeren Grauton haben müssen. Die Differenz zwischen den Grautönen weißer und schwarzer Pixel ist entscheidend für die Erkennbarkeit des rekonstruierten Bildes. Daher soll der Kontrast α möglichst groß sein.

Ein (k, n)-Schema der Visuellen Kryptographie hat einen *optimalen Kontrast* α, wenn es keine Matrizenklassen C_0 und C_1 gibt, so dass diese einen größeren Kontrastwert als α liefern. Hofmeister, Krause und Simon haben in [10] nachgewiesen, dass das Problem, den optimalen Kontrast für ein (k, n)-Schema zu bestimmen, gelöst werden kann, indem ein bestimmtes Lineares Programm gelöst wird. Ebenfalls kann aus einer optimalen Lösung für dieses Lineare Programm ein kontrastoptimales (k, n)-Schema konstruiert werden. Die Pixelexpansion wird hierbei vernachlässigt, sodass durchaus andere Schemata existieren können, die den selben Kontrast liefern, jedoch einen geringeren Wert für die Pixelexpansion aufweisen. Details hierzu sind in [5] und [10] zu finden.
Das Lineare Programm $L(k, n)$ wird in [10] von Hofmeister, Krause und Simon wie folgt definiert.

Definition 3.4:
Das Lineare Programm $L(k, n)$ mit $n \geq 2$ und $k \in \{2, \ldots, n\}$ wird für die Variablen $((x_0, \ldots, x_n), (y_0, \ldots, y_n))$, welche rationale Zahlen sind, definiert als

Zielfunktion: $L(k, n) = \sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) \longrightarrow$ maximieren
Nebenbedingungen:

1. $x_j, y_j \geq 0, \qquad j = 0, \ldots, n$
2. $\sum_{j=0}^{n} x_j = \sum_{j=0}^{n} y_j = 1$
3. $\sum_{j=\ell}^{n-k+\ell+1} \binom{n-k+1}{j-\ell} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) = 0, \qquad \ell = 0, \ldots, k-1.$

In [10] wurde auch angemerkt, dass der optimale Zielfunktionswert von $L(k, n)$ immer positiv ist, da die Nebenbedingungen linear unabhängig von der Zielfunktion sind. Diese wichtige Aussage wird häufig benötigt, weswegen sie hier als Lemma formuliert werden soll.

Lemma 3.1 [10]:
Sei $(x, y) = ((x_0, x_1, \ldots, x_n), (y_0, y_1, \ldots, y_n))$ eine optimale Belegung der Variablen für das Lineare Programm $L(k, n)$ nach Definition 3.4. Dann ist der Zielfunktionswert, welcher durch diese Belegung erreicht wird, immer positiv.

Eine weitere wichtige Eigenschaft formuliert das folgende Lemma, welches ebenfalls in [10] bewiesen wird.

Lemma 3.2 [10]:
Seien die Vektoren $(x, y) = ((x_0, \ldots, x_n), (y_0, \ldots, y_n))$ eine optimale Lösung des Linearen Programms $L(k, n)$ mit positivem Zielfunktionswert. Dann gilt $x_j = 0$ oder $y_j = 0$ für alle $j = 0, \ldots, n$.

Beweis: Sei j beliebig und es gelte $x_j \geq y_j$.
Falls $y_j = 0$ ist, muss nichts gezeigt werden. Sei daher $y_j > 0$.
Fall I: $y_j = 1$:

Da x und y eine optimale Lösung von $L(k, n)$ sind, erfüllen sie die Nebenbedingungen. Dann folgt $x_j = 1$, da $x_j \geq y_j$ gelten soll, und alle anderen Komponenten der Vektoren sind gleich Null, also $x_i = y_i = 0$ für alle $i \neq j$. Das wiederum bedeutet $x = y$, woraus folgt, dass der Zielfunktionswert gleich Null ist. Dieses stellt jedoch einen Widerspruch zur Voraussetzung dar. Somit muss $y_j < 1$ gelten.

Fall II: $0 < y_j < 1$:

Wir definieren mit

$$x'_i := \begin{cases} x_i & \text{für } i \neq j \\ x_i - y_i & \text{für } i = j \end{cases}$$

und

$$y'_i := \begin{cases} y_i & \text{für } i \neq j \\ y_i - y_i = 0 & \text{für } i = j \end{cases}$$

zwei neue Vektoren $x' = (x'_1, \ldots, x'_n)$ und $y' = (y'_1, \ldots, y'_n)$. Durch diese Konstruktion erfüllen sie die Nebenbedingungen 1 und 3, die zweite jedoch nicht, da

$$\sum_{i=0}^{n} x'_i = \sum_{i=0}^{n} x_i - y_j = 1 - y_j = \sum_{i=0}^{n} y_i - y_j = \sum_{i=0}^{n} y'_i$$

gilt. Werden die Vektoren nun noch normiert, erfüllen sie auch die Nebenbedingung 2. Hierfür wird $s := \sum_{i=0}^{n} x'_i = \sum_{i=0}^{n} y'_i = 1 - y_j$ definiert. Da $0 < y_j < 1$ gilt, folgt $0 < s < 1$. Die normierten Vektoren x'' und y'' ergeben sich nun zu $x''_i := \frac{x'_i}{s}$ und $y''_i := \frac{y'_i}{s}$ für $i = 0, \ldots, n$. Jetzt erfüllen x'' und y'' alle drei Nebenbedingungen, jedoch ist für sie der Zielfunktionswert um den Faktor $\frac{1}{s}$ gewachsen, da $s < 1$ ist. Somit haben wir eine Lösung konstruiert, die einen größeren Zielfunktionswert hat, als eine optimale Lösung (nach Voraussetzung). Da dieses ein Widerspruch ist, muss $y_j = 0$ gelten.

Für $x_j \leq y_j$ verfährt man analog.
Somit folgt $x_j = 0$ oder $y_j = 0$ für alle $j = 0, \ldots, n$. □

Für $z_i := (x_i - y_i)$ lässt sich ein Lineares Programm definieren, dessen optimale Lösungen leicht in optimale Lösungen für $L(k,n)$ transformiert werden können.

Definition 3.5:
Das Lineare Programm $L(k,n)_z$ mit $n \geq 2$ und $k \in \{2,\ldots,n\}$ wird für die Variablen $(z_0,\ldots,z_n)$, welche rationale Zahlen sind, definiert als

Zielfunktion: $L(k,n)_z = \sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot z_j \longrightarrow$ maximieren
Nebenbedingungen:

1. $-1 \leq z_j \leq 1, \qquad j = 0,\ldots,n$
2. $\sum_{j=0}^{n} z_j = 0$
   a) $\sum_{\substack{j=0 \\ z_j>0}}^{n} z_j = 1$
   b) $\sum_{\substack{j=0 \\ z_j<0}}^{n} z_j = -1$
3. $\sum_{j=\ell}^{n-k+\ell+1} \binom{n-k+1}{j-\ell} \cdot \binom{n}{j}^{-1} \cdot z_j = 0, \qquad \ell = 0,\ldots,k-1.$

Durch Lemma 3.2 lassen sich optimale Lösungen $\hat{z}$ für $L(k,n)_z$ in optimale Lösungen $(\hat{x},\hat{y})$ für $L(k,n)$ transformieren. Dazu definiert man

$$\hat{x}_j := \begin{cases} \hat{z}_j & \text{falls } \hat{z}_j > 0 \\ 0 & \text{sonst} \end{cases}$$

und

$$\hat{y}_j := \begin{cases} \hat{z}_j & \text{falls } \hat{z}_j < 0 \\ 0 & \text{sonst} \end{cases}$$

für $j = 0,1,\ldots,n$. Somit kann mit dem Linearen Programm $L(k,n)_z$ gearbeitet werden, das nur halb so viele Variablen enthält, wie das Lineare Programm $L(k,n)$.

3.2 Allgemeine Eigenschaften von $L(k,n)_z$

In [5] wurden verschiedene Eigenschaften von zulässigen und optimalen Lösungen für das Lineare Programm $L(k-1,k)_z$ gezeigt. Daraus entstand die Vermutung, dass diese Eigenschaften auch im Allgemeinen Gültigkeit besitzen. Durch die Hilfe von Prof. Dr. Volker

Strehl werden diese Vermutungen bewiesen. Die folgenden zwei Lemmata ermöglichen es, die Variablen $z_{n-k+1}, z_{n-k+2}, \ldots, z_n$ in Abhängigkeit der Variablen $z_0, z_1, \ldots, z_{n-k}$ darzustellen. Darauf aufbauend können dann weitere Eigenschaften gezeigt werden.

Lemma 3.3 [11]:
Sei

$$c(t) = \sum_{j \geq 0} c_j \cdot t^j$$

eine formale Reihe und es gelte

$$(1+t)^{k+1} \cdot c(t) = \sum_{j=0}^{k} p_j \cdot t^j + \sum_{j \geq n+1} p_j \cdot t^j$$

für ein $k \geq 0$ und ein $n > k$. Dann gilt

$$c_m = (-1)^{m-k} \cdot \binom{m}{k+1} \cdot \sum_{i=0}^{k} c_i \cdot \frac{k+1-i}{m-i} \cdot \binom{k+1}{i}$$

für alle m mit $k < m \leq n$.

Beweis: Die Terme $(1+t)^{k+1}$ und $c(t)$ können als erzeugende Funktionen interpretiert werden, da sie sich als Potenzreihe darstellen lassen. Da das Produkt zweier erzeugender Funktionen gleich der Faltung der entsprechenden Folgen ist, gilt für die Koeffizienten p_m mit $0 \leq m \leq k$

$$\begin{aligned} p_m = [t^m](c(t) \cdot (1+t)^{k+1}) &= [t^m] \left(\left[\sum_{j \geq 0} c_j \cdot t^j \right] \cdot \left[\sum_{j \geq 0} \binom{k+1}{j} \cdot t^j \right] \right) \\ &= \sum_{j=0}^{m} c_j \cdot \binom{k+1}{m-j} \end{aligned} \tag{3.1}$$

durch Koeffizientenvergleich.
Nach Voraussetzung gilt

$$(1+t)^{k+1} \cdot c(t) = \sum_{j \geq 0} p_j \cdot t^j$$

$$\begin{aligned}
\iff \quad c(t) &= \left[\sum_{j\geq 0} p_j \cdot t^j\right] \cdot (1+t)^{-k-1} \\
&= \left[\sum_{j\geq 0} p_j \cdot t^j\right] \cdot \left[\sum_{j\geq 0} \binom{-k-1}{j} \cdot t^j\right] \\
&= \underbrace{\left[\sum_{j\geq 0} p_j \cdot t^j\right] \cdot \left[\sum_{j\geq 0} \binom{k+j}{j} \cdot (-t)^j\right]}_{A} && \text{nach Lemma 2.6.}
\end{aligned}$$

Betrachtet man A wieder als Multiplikation zweier erzeugender Funktionen, dann erhält man für m mit $k < m \leq n$

$$\begin{aligned}
c_m = [t^m]A &= \sum_{j=0}^{m} p_j \cdot \binom{k+m-j}{m-j} \cdot (-1)^{m-j} \\
&= \sum_{j=0}^{m} p_j \cdot \binom{k+m-j}{k} \cdot (-1)^{m-j} && \text{nach Lemma 2.4} \\
&= \sum_{j=0}^{k} p_j \cdot \binom{k+m-j}{k} \cdot (-1)^{m-j}, && (3.2)
\end{aligned}$$

da $p_j = 0$ für $j \in \{k+1, \ldots, m\}$. Setzt man (3.1) für die p_j in (3.2) ein, folgt für $k < m \leq n$

$$\begin{aligned}
c_m &= \sum_{j=0}^{k} p_j \cdot \binom{k+m-j}{k} \cdot (-1)^{m-j} \\
&= \sum_{j=0}^{k} \sum_{i=0}^{j} c_i \cdot \binom{k+1}{j-i} \cdot \binom{k+m-j}{k} \cdot (-1)^{m-j} \\
&= \sum_{j=0}^{k} (-1)^{m-j} \cdot \sum_{i=0}^{j} c_i \cdot \binom{k+1}{j-i} \cdot \binom{k+m-j}{k} \\
&= \sum_{i=0}^{k} c_i \cdot \sum_{j=i}^{k} (-1)^{m-j} \cdot \binom{k+1}{j-i} \cdot \binom{k+m-j}{k} \\
&= \sum_{i=0}^{k} c_i \cdot \sum_{j=0}^{k-i} (-1)^{m-j-i} \cdot \binom{k+1}{j} \cdot \binom{k+m-j-i}{k} \\
&= \sum_{i=0}^{k} c_i \cdot (-1)^{m-i} \cdot \sum_{j=0}^{k-i} (-1)^{j} \cdot \binom{k+1}{j} \cdot \binom{k+m-i}{k} \cdot \frac{\binom{m-i}{j}}{\binom{m+k-i}{j}} \\
&= \sum_{i=0}^{k} c_i \cdot (-1)^{m-i} \cdot \binom{k+m-i}{k} \cdot \underbrace{\sum_{j=0}^{k-i} \frac{(-k-1)_j \cdot (i-m)_j}{(i-k-m)_j \cdot j!}}_{B} && \text{nach Lemma 2.1.}
\end{aligned}$$

Für die Summe B gilt

$$\begin{aligned}
B &= \sum_{j\geq 0} \frac{(-k-1)_j \cdot (i-m)_j}{(i-k-m)_j \cdot j!} - \sum_{j>k-i} \frac{(-k-1)_j \cdot (i-m)_j}{(i-k-m)_j \cdot j!} \\
&= {}_2F_1\left[\begin{matrix}(-k-1),(i-m)\\(i-k-m)\end{matrix};1\right] - \sum_{j>k-i} \frac{(-k-1)_j \cdot (i-m)_j}{(i-k-m)_j \cdot j!} && \text{nach Definition 2.5} \\
&= \frac{(-k)_{k+1}}{(i-k-m)_{k+1}} - \sum_{j>k-i} \frac{(-k-1)_j \cdot (i-m)_j}{(i-k-m)_j \cdot j!} && \text{nach Satz 2.1} \\
&= 0 - \sum_{j>k-i} \frac{(-k-1)_j \cdot (i-m)_j}{(i-k-m)_j \cdot j!} \\
&= -\sum_{j\geq 0} \frac{(-k-1)_{j+k-i+1} \cdot (i-m)_{j+k-i+1}}{(i-k-m)_{j+k-i+1} \cdot (j+k-i+1)!} \\
&= -\sum_{j\geq 0} \frac{(-k-1)_{j+k-i+1} \cdot (i-m)_{j+k-i+1}}{(i-k-m)_{j+k-i+1} \cdot (1)_{j+k-i+1}} \\
&= -\sum_{j\geq 0} \frac{(-k-1)_{k-i+1} \cdot (-i)_j \cdot (i-m)_{k-i+1} \cdot (k+1-m)_j}{(i-k-m)_{k-i+1} \cdot (1-m)_j \cdot (1)_{k-i+1} \cdot (k+2-i)_j} && \text{nach Lemma 2.2} \\
&= -\frac{(-k-1)_{k-i+1} \cdot (i-m)_{k-i+1}}{(i-k-m)_{k-i+1} \cdot (1)_{k-i+1}} \cdot \sum_{j\geq 0} \frac{(-i)_j \cdot (k+1-m)_j}{(1-m)_j \cdot (k+2-i)_j} \\
&= (-1)^{k-i} \cdot \frac{\binom{k+1}{k-i+1} \cdot \binom{m-i}{k-i+1}}{\binom{m+k-i}{k-i+1}} \cdot \sum_{j\geq 0} \frac{(k+1-m)_j \cdot (-i)_j}{(1-m)_j \cdot (k+2-i)_j} && \text{nach Lemma 2.1} \\
&= (-1)^{k-i} \cdot \frac{\binom{k+1}{k-i+1} \cdot \binom{m-i}{k-i+1}}{\binom{m+k-i}{k-i+1}} \cdot {}_3F_2\left[\begin{matrix}-m+k+1,1,-i\\-m+1,k-i+2\end{matrix};1\right] && \text{nach Definition 2.5} \\
&= (-1)^{k-i} \cdot \frac{\binom{k+1}{k-i+1} \cdot \binom{m-i}{k-i+1}}{\binom{m+k-i}{k-i+1}} \cdot \frac{(-k)_i \cdot (-m)_i}{(-m+1)_i \cdot (-k-1)_i} && \text{nach Satz 2.2} \\
&= (-1)^{k-i} \cdot \frac{\binom{k+1}{k-i+1} \cdot \binom{m-i}{k-i+1}}{\binom{m+k-i}{k-i+1}} \cdot \frac{k-i+1}{k+1} \cdot \frac{m}{m-i}
\end{aligned}$$

und damit für c_m mit $k < m \leq n$

$$\begin{aligned}
c_m &= \sum_{i=0}^{k} c_i \cdot (-1)^{m+k} \cdot \binom{k+m-i}{k} \cdot \frac{\binom{k+1}{k-i+1} \cdot \binom{m-i}{k-i+1}}{\binom{m+k-i}{k-i+1}} \cdot \frac{k-i+1}{k+1} \cdot \frac{m}{m-i} \\
&= \sum_{i=0}^{k} c_i \cdot (-1)^{m+k} \cdot \frac{k-i+1}{k+1} \cdot \frac{m}{m-i} \\
&\quad \cdot \frac{(k+m-i)! \cdot (k+1)! \cdot (m-i)! \cdot (k-i+1)! \cdot (m-1)!}{k! \cdot (m-i)! \cdot (k-i+1)! \cdot i! \cdot (k-i+1)! \cdot (m-k-1)! \cdot (m+k-i)!} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{nach Definition 2.2}
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{k} c_i \cdot (-1)^{m+k} \cdot \frac{k-i+1}{k+1} \cdot \frac{m}{m-i} \cdot \frac{(k+1)! \cdot (m-1)!}{k! \cdot i! \cdot (k-i+1)! \cdot (m-k-1)!} \\
&= \sum_{i=0}^{k} c_i \cdot (-1)^{m+k} \cdot \frac{k-i+1}{k+1} \cdot \frac{m}{m-i} \cdot \binom{k+1}{i} \cdot \binom{m-1}{k} \qquad \text{nach Definition 2.2} \\
&= (-1)^{m-k} \cdot \binom{m}{k+1} \cdot \sum_{i=0}^{k} c_i \cdot \frac{k-i+1}{m-i} \cdot \binom{k+1}{i},
\end{aligned}
$$

wie behauptet. □

Lemma 3.4 [11]:
Die Variablen des Linearen Programms $L(k,n)_z$ lassen sich darstellen als

$$z_\ell = (-1)^{\ell-n+k} \cdot \binom{k-1}{n-\ell} \cdot \sum_{j=0}^{n-k} \binom{n-j}{k-1} \cdot z_j \cdot \frac{n-k+1-j}{\ell-j}$$

für $\ell \in \{n-k+1, \ldots, n\}$.

Beweis: Die dritte Nebenbedingung ist

$$\sum_{j=\ell}^{n-k+\ell+1} \binom{n-k+1}{j-\ell} \cdot \binom{n}{j}^{-1} \cdot z_j = 0$$

für alle $\ell \in \{0, 1, \ldots, k-1\}$.
Für $g = n-k$ gilt

$$
\begin{aligned}
0 &= \sum_{j=\ell}^{g+\ell+1} \binom{g+1}{j-\ell} \cdot \binom{n}{j}^{-1} \cdot z_j \\
&= \sum_{j=0}^{g+1} \binom{g+1}{j} \cdot \binom{n}{j+\ell}^{-1} \cdot z_{j+\ell} \\
&= \sum_{j=0}^{g+1} \binom{g+1}{g+1-j} \cdot \binom{n}{j+\ell}^{-1} \cdot z_{j+\ell} \qquad \text{nach Lemma 2.4}
\end{aligned}
$$

für alle $\ell \in \{0, 1, \ldots, k-1\}$.
Definiert man

$$c_j := \begin{cases} z_j \cdot \binom{n}{j}^{-1} & 0 \le j \le n \\ 0 & j > n \end{cases}$$

und betrachtet das Produkt von erzeugenden Funktionen

$$(1+t)^{g+1} \cdot \sum_{j\geq 0} c_j \cdot t^j,$$

dann gilt für alle $\ell \in \mathbb{N}$

$$[t^{g+1+\ell}] \left((1+t)^{g+1} \cdot \sum_{j\geq 0} c_j \cdot t^j \right) = \sum_{j\geq 0} \binom{g+1}{g+1+\ell-j} \cdot c_j = \sum_{j=\ell}^{g+1+\ell} \binom{g+1}{g+1+\ell-j} \cdot c_j$$
$$= \sum_{j=0}^{g+1} \binom{g+1}{g+1-j} \cdot c_{j+\ell}. \tag{3.3}$$

Für alle $\ell \in \{0, 1, \ldots, k-1\}$ kann $c_{j+\ell}$ durch $z_{j+\ell} \cdot \binom{n}{j+\ell}^{-1}$ ersetzt werden. Dann gilt für (3.3)

$$[t^{g+1+\ell}] \left((1+t)^{g+1} \cdot \sum_{j\geq 0} c_j \cdot t^j \right) = \sum_{j=0}^{g+1} \binom{g+1}{g+1-j} \cdot \binom{n}{j+\ell}^{-1} \cdot z_{j+\ell}.$$

Dieses ist identisch zur Summe der dritten Nebenbedingung. Da diese den Wert 0 annehmen muss, sind die Koeffizienten vor $[t^{g+1+\ell}]$ gleich 0 für alle $\ell \in \{0, 1, \ldots, k-1\}$. Somit gilt

$$(1+t)^{g+1} \cdot \sum_{j\geq 0} c_j \cdot t^j = \sum_{j=0}^{g} p_j \cdot t^j + \sum_{j\geq g+1+k} p_j \cdot t^j.$$

Damit sind die Voraussetzungen erfüllt, um das Lemma 3.3 anwenden zu können und man erhält

$$c_m = z_m \cdot \binom{n}{m}^{-1} = (-1)^{m-g} \cdot \binom{m}{g+1} \cdot \sum_{i=0}^{g} z_i \cdot \binom{n}{i}^{-1} \cdot \frac{g-i+1}{m-i} \cdot \binom{g+1}{i}$$

für alle m mit $g < m \leq g+k$.
Führt man die Rücksubstitution von $g = n-k$ durch, folgt

$$z_m = (-1)^{m-n+k} \cdot \binom{n}{m} \cdot \binom{m}{n-k+1}$$
$$\cdot \sum_{i=0}^{n-k} z_i \cdot \binom{n}{i}^{-1} \cdot \frac{n-k-i+1}{m-i} \cdot \binom{n-k+1}{i}$$

$$= (-1)^{m-n+k} \cdot \binom{n}{n-k+1} \cdot \binom{k-1}{n-m} \cdot \sum_{i=0}^{n-k} \binom{n-k+1}{i} \cdot \binom{n}{i}^{-1} \cdot z_i \cdot \frac{n-k+1-i}{m-i}$$

nach Lemma 2.7

$$= (-1)^{m-n+k} \cdot \binom{n}{n-k+1} \cdot \binom{k-1}{n-m} \cdot \sum_{i=0}^{n-k} \binom{n-i}{k-1} \cdot \binom{n}{n-k+1}^{-1} \cdot z_i \cdot \frac{n-k+1-i}{m-i}$$

nach Lemma 2.7

$$= (-1)^{m-n+k} \cdot \binom{k-1}{n-m} \cdot \sum_{i=0}^{n-k} \binom{n-i}{k-1} \cdot z_i \cdot \frac{n-k+1-i}{m-i}.$$

Mit $\ell = m$ gilt daher

$$z_\ell = (-1)^{\ell-n+k} \cdot \binom{k-1}{n-\ell} \cdot \sum_{j=0}^{n-k} \binom{n-j}{k-1} \cdot z_j \cdot \frac{n-k+1-j}{\ell-j}$$

für $\ell \in \{n-k+1, \ldots, n\}$, wie behauptet. □

Diese Formel kann nun anstatt der dritten Nebenbedingung verwendet werden, da lediglich eine Umformung der dritten Nebenbedingung stattgefunden hat. Diese Formel ist also äquivalent zur Nebenbedingung 3. Allerdings gilt sie zunächst nicht für alle Variablen z_i mit $i \in \{0, \ldots, n\}$. Durch einige Umformungen wird aber auch dieses ermöglicht.

Lemma 3.5:
Die Variablen des Linearen Programms $L(k, n)_z$ lassen sich darstellen als

$$z_\ell = (-1)^{\ell-(n-k)} \cdot \binom{n}{\ell} \cdot \sum_{j=0}^{n-k} \frac{(\ell-(n-k))_{n-k-j} \cdot (\ell+1-j)_j}{(n+1-j)_j \cdot (n-k-j)!} \cdot z_j$$

für alle $\ell \in \{0, \ldots, n\}$, wobei $(a)_i$ das Pochhammer-Symbol nach Definition 2.4 ist.

Beweis: Nach Lemma 3.4 gilt für $\ell \in \{n-k+1, \ldots, n\}$:

$$
\begin{aligned}
z_\ell &= (-1)^{\ell-n+k} \cdot \binom{k-1}{n-\ell} \cdot \sum_{j=0}^{n-k} \binom{n-j}{k-1} \cdot z_j \cdot \frac{n-k+1-j}{\ell-j} \\
&= (-1)^{\ell-n+k} \cdot \frac{(k-1)!}{(n-\ell)! \cdot (\ell-(n-k+1))!} \cdot \sum_{j=0}^{n-k} \binom{n-j}{k-1} \cdot z_j \cdot \frac{n-k+1-j}{\ell-j} \\
&\qquad\qquad \text{nach Definition 2.2} \\
&= \frac{(-1)^{\ell-n+k} \cdot (k-1)!}{(n-\ell)! \cdot \ell!} \cdot \sum_{j=0}^{n-k} \binom{n-j}{k-1} \cdot z_j \cdot (n-k+1-j) \cdot (\ell-(n-k))_{n-k-j} \cdot (\ell+1-j)_j \\
&= \frac{(-1)^{\ell-n+k}}{(n-\ell)! \cdot \ell!} \cdot \sum_{j=0}^{n-k} \frac{(n-j)! \cdot z_j \cdot (n-k+1-j) \cdot (\ell-(n-k))_{n-k-j} \cdot (\ell+1-j)_j}{(n-k+1-j)!} \\
&\qquad\qquad \text{nach Definition 2.2} \\
&= (-1)^{\ell-n+k} \cdot \binom{n}{\ell} \cdot \sum_{j=0}^{n-k} \frac{z_j \cdot (n-k+1-j) \cdot (\ell-(n-k))_{n-k-j} \cdot (\ell+1-j)_j}{(n-k+1-j)! \cdot (n+1-j)_j} \\
&\qquad\qquad \text{nach Definition 2.2} \\
&= (-1)^{\ell-n+k} \cdot \binom{n}{\ell} \cdot \sum_{j=0}^{n-k} \frac{(\ell-(n-k))_{n-k-j} \cdot (\ell+1-j)_j}{(n-k-j)! \cdot (n+1-j)_j} \cdot z_j. \qquad (3.4)
\end{aligned}
$$

Bis hierhin wurde die Eigenschaft $\ell \in \{n-k+1, \ldots, n\}$ ausgenutzt, da der Term $\ell - j$ für kleinere ℓ gleich 0 gewesen wäre und dieses zu einer Division durch 0 geführt hätte. Betrachtet man (3.4) nun für $\ell \in \{0, \ldots, n-k\}$, gilt

$$(\ell-(n-k))_{n-k-j} = 0 \Longleftrightarrow j < \ell$$

und

$$(\ell+1-j)_j = 0 \Longleftrightarrow j > \ell.$$

Somit tritt für kleine ℓ genau ein Term in der Summe auf und es gilt

$$
\begin{aligned}
z_\ell &= (-1)^{\ell-n+k} \cdot \binom{n}{\ell} \cdot \frac{(\ell-(n-k))_{n-k-\ell} \cdot (\ell+1-\ell)_\ell}{(n-k-\ell)! \cdot (n+1-\ell)_\ell} \cdot z_\ell \\
&= (-1)^{k-n} \cdot \frac{(-n)_\ell}{\ell!} \cdot \frac{(\ell-(n-k))_{n-k-\ell} \cdot (1)_\ell}{(n-k-\ell)! \cdot (n+1-\ell)_\ell} \cdot z_\ell \qquad \text{nach Lemma 2.1} \\
&= (-1)^{k-n} \cdot (-n)_\ell \cdot \frac{(-1)^{n-k-\ell} \cdot (1)_{n-k-\ell}}{(n-k-\ell)! \cdot (-1)^\ell \cdot (-n)_\ell} \cdot z_\ell = z_\ell. \qquad \text{nach Lemma 2.3}
\end{aligned}
$$

Demnach gilt (3.4) für alle $\ell \in \{0, \ldots, n\}$, wie behauptet. □

Lemma 3.6:
Werden alle Variablen $z_\ell, \ell \in \{n-k+1, \ldots, n\}$, nach Lemma 3.4 bestimmt, dann ist die Nebenbedingung 2 erfüllt.

Beweis: Für die Nebenbedingung 2 gilt:

$$\begin{aligned}
\sum_{j=0}^{n} z_j &= \sum_{j=0}^{n-k} z_j + \sum_{j=n-k+1}^{n} z_j \\
&= \sum_{j=0}^{n-k} z_j + \sum_{j=n-k+1}^{n} \left(-\binom{k-1}{n-j} \sum_{i=0}^{n-k} \binom{n-i}{k-1} z_i (-1)^{j-(n-k+1)} \frac{(n-k+1-i)}{(j-i)} \right) \\
&\qquad \text{nach Lemma 3.4} \\
&= \sum_{j=0}^{n-k} z_j - \sum_{j=n-k+1}^{n} \sum_{i=0}^{n-k} \binom{k-1}{n-j} \binom{n-i}{k-1} z_i (-1)^{j-(n-k+1)} \frac{(n-k+1-i)}{(j-i)} \\
&= \sum_{j=0}^{n-k} z_j - \sum_{i=0}^{n-k} \sum_{j=n-k+1}^{n} \binom{k-1}{n-j} \binom{n-i}{k-1} z_i (-1)^{j-(n-k+1)} \frac{(n-k+1-i)}{(j-i)} \\
&= \sum_{j=0}^{n-k} z_j - \sum_{i=0}^{n-k} \binom{n-i}{k-1} z_i (n-k+1-i) \sum_{j=n-k+1}^{n} \binom{k-1}{n-j} (-1)^{j-(n-k+1)} \frac{1}{(j-i)} \\
&= \sum_{j=0}^{n-k} z_j - \sum_{i=0}^{n-k} \binom{n-i}{k-1} z_i (n-k+1-i) \cdot \\
&\qquad \cdot \sum_{j=n-k+1}^{n} \binom{k-1}{j-(n-k+1)} (-1)^{j-(n-k+1)} \frac{1}{(j-i)} \\
&= \sum_{j=0}^{n-k} z_j - \sum_{i=0}^{n-k} \binom{n-i}{k-1} z_i (n-k+1-i) \sum_{j=0}^{k-1} \binom{k-1}{j} (-1)^j \frac{1}{(j+n-k+1-i)}
\end{aligned}$$

Für $a = (n-k+1-i) \geq 1$ kann Lemma 2.18 angewandt werden:

$$\begin{aligned}
&= \sum_{j=0}^{n-k} z_j - \sum_{i=0}^{n-k} \binom{n-i}{k-1} z_i (n-k+1-i) \frac{1}{(n-k+1-i)\binom{k-1+(n-k+1-i)}{(n-k+1-i)}} \\
&= \sum_{j=0}^{n-k} z_j - \sum_{i=0}^{n-k} \binom{n-i}{k-1} z_i \binom{n-i}{k-1}^{-1} \\
&= \sum_{j=0}^{n-k} z_j - \sum_{i=0}^{n-k} z_i = 0.
\end{aligned}$$

□

Bemerkung 3.1:
Hieraus folgt, dass die Nebenbedingung 2 linear abhängig von der Nebenbedingung 3 ist. Jede Belegung z, welche die dritte Nebenbedingung erfüllt, erfüllt also auch die zweite Nebenbedingung. Somit gilt für die Nebenbedingungen $2a$ und $2b$

$$\sum_{j=0}^{n} z_j = \sum_{\substack{j=0 \\ z_j>0}}^{n} z_j + \sum_{\substack{j=0 \\ z_j<0}}^{n} z_j = 0$$
$$\iff \sum_{\substack{j=0 \\ z_j>0}}^{n} z_j = -\sum_{\substack{j=0 \\ z_j<0}}^{n} z_j$$

für jede Belegung z, welche die Nebenbedingung 3 erfüllt. Allerdings ist der Wert der Summe der positiven Variablen nicht notwendiger Weise gleich 1. Die Nebenbedingungen $2a$ und $2b$ sind daher linear unabhängig von der dritten Nebenbedingung. Wird eine der Nebenbedingungen $2a$ oder $2b$ erfüllt, dann ist auch die entsprechend andere erfüllt. Gleichzeitig sind dadurch alle Variablenwerte aus dem Intervall $[-1, 1]$, was die erste Nebenbedingung erfüllt. Dieses gilt, da die Summe der positiven Werte 1 ergibt und daher kein Wert größer als 1 sein kann. Analog gilt für die negativen, dass kein Wert kleiner als -1 sein kann. Zusammenfassend gilt also

Nebenbedingung 3 $\implies$ Nebenbedingung 2, sowie
Nebenbedingung 3 und Nebenbedingung $2a$ $\implies$ Nebenbedingung $2b$ und Nebenbedingung 1 $\implies$ die Belegung ist zulässig.

Lemma 3.7:
Seien $z' = (z'_0, \ldots, z'_n)$ und $z'' = (z''_0, \ldots, z''_n)$ zwei zulässige Belegungen des Linearen Programms $L(k, n)_z$, die den selben positiven Zielfunktionswert α liefern. Dann lässt sich eine neue Belegung $z''' = (z'''_0, \ldots, z'''_n)$ mit $z'''_i = \lambda \cdot z'_i + (1 - \lambda) \cdot z''_i$ für $i = 0, \ldots, n$ und $\lambda \in [0, 1]$ konstruieren, für die gilt:

1. entweder ist z''' zulässig und liefert den selben Zielfunktionswert α wie die Belegungen z' und z'', oder

2. z''' ist nicht zulässig, jedoch kann eine zulässige Belegung z'''' konstruiert werden, die einen Zielfunktionswert $\alpha^* > \alpha$ liefert.

Beweis: Die Belegung z''' erfüllt die dritte Nebenbedingung:
Für alle $\ell = 0, \ldots, k-1$ gilt:

$$\begin{aligned}
&\sum_{i=\ell}^{n-k+\ell+1} \binom{n-k+1}{i-\ell} \cdot \binom{n}{i}^{-1} \cdot z_i''' \\
&\quad = \sum_{i=\ell}^{n-k+\ell+1} \binom{n-k+1}{i-\ell} \cdot \binom{n}{i}^{-1} \cdot [\lambda z_i' + (1-\lambda) z_i''] \\
&\quad = \lambda \cdot \sum_{i=\ell}^{n-k+\ell+1} \binom{n-k+1}{i-\ell} \cdot \binom{n}{i}^{-1} \cdot z_i' + (1-\lambda) \cdot \sum_{i=\ell}^{n-k+\ell+1} \binom{n-k+1}{i-\ell} \cdot \binom{n}{i}^{-1} \cdot z_i'' \\
&\quad = \lambda \cdot 0 + (1-\lambda) \cdot 0 = 0.
\end{aligned}$$

Für die Nebenbedingung $2a$ gilt:

$$\sum_{\substack{i=0 \\ z_i'''>0}}^{n} z_i''' = \underbrace{\sum_{\substack{i=0 \\ z_i'''>0}}^{n} [\lambda z_i' + (1-\lambda) z_i'']}_{A} \leq \underbrace{\lambda \cdot \sum_{\substack{i=0 \\ z_i'>0}}^{n} z_i' + (1-\lambda) \cdot \sum_{\substack{i=0 \\ z_i''>0}}^{n} z_i''}_{B} = 1.$$

Da z' und z'' zulässige Belegungen sind, gilt $B = 1$. Durch die Linearkombination $\lambda z_i' + (1-\lambda) z_i''$ ist es nicht möglich, dass $A > B$ gilt. Allerdings könnte $A < B$ gelten, nämlich genau dann, wenn $\operatorname{sgn}(z_i') = -\operatorname{sgn}(z_i'') \neq 0$ für mindestens ein i ist.

Fall I: $A = B = 1$:

Da $A = 1$ gilt, ist nach Bemerkung 3.1 die Belegung z''' zulässig. Der Zielfunktionswert dieser Belegung ist

$$\begin{aligned}
&\sum_{i=0}^{n-k} \binom{n-k}{i} \cdot \binom{n}{i}^{-1} \cdot z_i''' \\
&\quad = \sum_{i=0}^{n-k} \binom{n-k}{i} \cdot \binom{n}{i}^{-1} \cdot [\lambda z_i' + (1-\lambda) z_i''] \\
&\quad = \lambda \cdot \sum_{i=0}^{n-k} \binom{n-k}{i} \cdot \binom{n}{i}^{-1} \cdot z_i' + (1-\lambda) \cdot \sum_{i=0}^{n-k} \binom{n-k}{i} \cdot \binom{n}{i}^{-1} \cdot z_i'' \\
&\quad = \lambda \cdot \alpha + (1-\lambda) \cdot \alpha = \alpha.
\end{aligned}$$

Damit ist die Aussage 1 des Lemmas gezeigt.

Fall II: $A < B = 1$:

Die Belegung z''' ist nicht zulässig, da die Nebenbedingung $2a$ nicht erfüllt wird.
Nun definiert man eine neue Belegung z'''' mit

$$s := \sum_{\substack{i=0 \\ z_i'''>0}}^{n} z_i''' < 1$$

und

$$z_i'''' := \frac{1}{s} \cdot z_i'''.$$

Der Wert s ist größer 0, denn es muss mindestens ein positives z_i''' existieren. Andernfalls wären alle $z_i''' \leq 0$. Dann wäre aber entweder die dritte Nebenbedingung nicht erfüllt, oder es würde $z''' = \vec{0}$ gelten. Die Belegung z''' erfüllt jedoch die Nebenbedingung 3. Wenn $s = 0$ gelten würde, müsste demnach $\lambda \cdot z_i' + (1-\lambda) \cdot z_i'' = 0 \iff z_i' = -\frac{1-\lambda}{\lambda} z_i''$ für alle $i = 0, \ldots, n$ gelten. Dann würden die Belegungen z' und z'' aber nicht den selben positiven Zielfunktionswert α liefern, da z_i' genau dann positiv wäre, wenn z_i' negativ ist. Dieses stellt jedoch einen Widerspruch zur Annahme dar, also muss $s > 0$ gelten.
Die Belegung z'''' ist demnach wohldefiniert und erfüllt alle Nebenbedingungen:
Nebenbedingung 3: für alle $\ell = 0, \ldots, k-1$ gilt:

$$\begin{aligned}
\sum_{i=\ell}^{n-k+\ell+1} \binom{n-k+1}{i-\ell} \cdot \binom{n}{i}^{-1} \cdot z_i'''' &= \sum_{i=\ell}^{n-k+\ell+1} \binom{n-k+1}{i-\ell} \cdot \binom{n}{i}^{-1} \cdot \frac{z'''}{s} \\
&= \frac{1}{s} \cdot \sum_{i=\ell}^{n-k+\ell+1} \binom{n-k+1}{i-\ell} \cdot \binom{n}{i}^{-1} \cdot z_i''' \\
&= \frac{1}{s} \cdot 0 = 0.
\end{aligned}$$

Nebenbedingung $2a$:

$$\sum_{\substack{i=0 \\ z_i''''>0}}^{n} z_i'''' = \sum_{\substack{i=0 \\ z_i'''>0}}^{n} \frac{z_i'''}{s} = \frac{1}{s} \cdot \sum_{\substack{i=0 \\ z_i'''>0}}^{n} z_i''' = \frac{s}{s} = 1.$$

Die Nebenbedingungen $2b, 2$ und 1 folgen hieraus, nach Bemerkung 3.1.

Der Zielfunktionswert von z'''' ist nach dieser Konstruktion jedoch

$$\begin{aligned}
\sum_{i=0}^{n-k}\binom{n-k}{i}\cdot\binom{n}{i}^{-1}\cdot z_i'''' &= \sum_{i=0}^{n-k}\binom{n-k}{i}\cdot\binom{n}{i}^{-1}\cdot\frac{z_i'''}{s}\\
&= \frac{1}{s}\cdot\sum_{i=0}^{n-k}\binom{n-k}{i}\cdot\binom{n}{i}^{-1}\cdot[\lambda z_i' + (1-\lambda)z_i'']\\
&= \frac{\lambda}{s}\cdot\sum_{i=0}^{n-k}\binom{n-k}{i}\cdot\binom{n}{i}^{-1}\cdot z_i' + \frac{(1-\lambda)}{s}\cdot\sum_{i=0}^{n-k}\binom{n-k}{i}\cdot\binom{n}{i}^{-1}\cdot z_i''\\
&= \frac{\lambda}{s}\cdot\alpha + \frac{(1-\lambda)}{s}\cdot\alpha = \frac{1}{s}\cdot(\lambda+(1-\lambda))\cdot\alpha = \frac{1}{s}\cdot\alpha = \alpha^*
\end{aligned}$$

und somit größer als α, denn es gilt $s < 1$. Damit ist die Aussage 2 des Lemmas gezeigt. □

Lemma 3.8:
Sei $z = (z_0, z_1, \ldots, z_n)$ eine zulässige Belegung des Linearen Programms $L(k,n)_z$ mit dem Zielfunktionswert α. Dann ist auch $z' = (z_0', z_1', \ldots, z_n')$ mit $z_i' := (-1)^k \cdot z_{n-i}$ und $i = 0, \ldots, n$ eine zulässige Belegung für $L(k,n)_z$, die den selben Zielfunktionswert liefert.

Beweis: Die Belegung z' ist zulässig, da alle Nebenbedingungen erfüllt werden:
Nebenbedingung $2a$:
Für gerades k gilt

$$\sum_{\substack{i=0\\ z_i'>0}}^{n} z_i' = \sum_{\substack{i=0\\ z_{n-i}>0}}^{n} (-1)^k \cdot z_{n-i} = \sum_{\substack{i=0\\ z_i>0}}^{n} z_i = 1,$$

da z eine zulässige Belegung ist. Analog gilt für ungerades k

$$\sum_{\substack{i=0\\ z_i'>0}}^{n} z_i' = \sum_{\substack{i=0\\ z_{n-i}<0}}^{n} (-1)^k \cdot z_{n-i} = -\sum_{\substack{i=0\\ z_i<0}}^{n} z_i = -(-1) = 1.$$

Nebenbedingung 3:
In jeder der k Gleichungen aus Nebenbedingung 3 wird eine gewichtete Summe von $n-k+2$ konsekutiven Variablen betrachtet, welche den Wert 0 annehmen muss. Betrachtet man die

Summen nicht für steigendes ℓ, sondern für fallendes, erhält man für alle $\ell = 0, \ldots, k-1$

$$\begin{aligned}\sum_{i=\ell}^{n-k+\ell+1} \binom{n-k+1}{i-\ell} \cdot \binom{n}{i}^{-1} \cdot z'_i &= \sum_{i=\ell}^{n-k+\ell+1} \binom{n-k+1}{i-\ell} \cdot \binom{n}{i}^{-1} \cdot (-1)^k \cdot z_{n-i} \\ &= \sum_{i=k-1-\ell}^{n-\ell} \binom{n-k+1}{i-k+1+\ell} \cdot \binom{n}{i}^{-1} \cdot (-1)^k \cdot z_{n-i} \\ &= (-1)^k \cdot \sum_{i=k-1-\ell}^{n-\ell} \binom{n-k+1}{n-i-\ell} \cdot \binom{n}{n-i}^{-1} \cdot z_{n-i} = 0,\end{aligned}$$

da z eine zulässige Belegung ist.
Somit sind, nach Bemerkung 3.1, alle Nebenbedingungen erfüllt und die Belegung z' ist ebenfalls zulässig. Für die Bestimmung des Zielfunktionswerts der Belegung z' ist eine Fallunterscheidung notwendig.

Fall I: $n - k < \frac{n}{2} \iff n - k < k$:

Die Zielfunktion ist

$$\sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot z'_j = \sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot (-1)^k \cdot z_{n-j}$$

Da $n - k < k$ gilt, ist Lemma 3.4 für alle Variablen z_{n-j} anwendbar. Somit folgt

$$\begin{aligned}&= (-1)^k \cdot \sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot (-1)^{k-j} \cdot \binom{k-1}{j} \cdot \sum_{i=0}^{n-k} \binom{n-i}{k-1} \cdot z_i \cdot \frac{n-k+1-i}{n-j-i} \\ &= \sum_{i=0}^{n-k} \sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot (-1)^j \cdot \binom{k-1}{j} \cdot \binom{n-i}{k-1} \cdot z_i \cdot \frac{n-k+1-i}{n-j-i} \\ &= \sum_{i=0}^{n-k} \binom{n-i}{k-1} \cdot z_i \cdot (n-k+1-i) \cdot \underbrace{\sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot (-1)^j \cdot \binom{k-1}{j} \cdot \frac{1}{n-j-i}}_{A}\end{aligned} \tag{3.5}$$

Nach Lemma 2.1 gilt für die Summe A

$$A = \sum_{j=0}^{n-k} \frac{(k-n)_j \cdot (1-k)_j}{(-n)_j \cdot j!} \cdot \frac{1}{n-j-i} = \frac{1}{n-i} \cdot \sum_{j=0}^{n-k} \frac{(k-n)_j \cdot (1-k)_j \cdot (i-n)_j}{(-n)_j \cdot (i-n+1)_j \cdot j!}.$$

Für den Term $(k-n)_j$ mit $j \geq n-k+1$ gilt $(k-n)_j = 0$. Deshalb kann die obere Summationsgrenze $n-k$ entfallen und durch unendlich ersetzt werden. Nach Definition

2.5 gilt dann

$$A = \frac{1}{n-i} \cdot {}_3F_2\left(\begin{matrix} k-n, 1-k, i-n \\ -n, i-n+1 \end{matrix} ; 1 \right). \tag{3.6}$$

Zur Auswertung dieser ${}_3F_2$-Reihe kann Satz 2.2 nicht benutzt werden, da die Voraussetzungen für den Parameter d nicht erfüllt sind. Jedoch lässt sie sich mit Lemma 2.19 geeignet umformen. Es gilt also

$$\begin{aligned}
&(-k) \cdot {}_3F_2\left(\begin{matrix} k-n, 1-k, i-n \\ -n, i-n+1 \end{matrix} ; 1 \right) \\
&= (n-i-k) \cdot {}_3F_2\left(\begin{matrix} k-n, -k, i-n \\ -n, i-n+1 \end{matrix} ; 1 \right) + (i-n) \cdot {}_3F_2\left(\begin{matrix} k-n, -k, i-n+1 \\ -n, i-n+1 \end{matrix} ; 1 \right) \\
&= (n-i-k) \cdot {}_3F_2\left(\begin{matrix} k-n, i-n, -k \\ -n, i-n+1 \end{matrix} ; 1 \right) + (i-n) \cdot {}_2F_1\left(\begin{matrix} k-n, -k \\ -n \end{matrix} ; 1 \right) \\
&= (n-i-k) \cdot \frac{(-k)_k \cdot (-i)_k}{(-n)_k \cdot (n-k-i)_k} + (i-n) \cdot {}_2F_1\left(\begin{matrix} -k, k-n \\ -n \end{matrix} ; 1 \right) && \text{nach Satz 2.2} \\
&= (n-i-k) \cdot \frac{(-k)_k \cdot (-i)_k}{(-n)_k \cdot (n-k-i)_k} + (i-n) \cdot \frac{(-k)_k}{(-n)_k} && \text{nach Satz 2.1}
\end{aligned}$$

und damit für A

$$\begin{aligned}
A &= -\frac{1}{k \cdot (n-i)} \cdot \left[(n-i-k) \cdot \frac{(-k)_k \cdot (-i)_k}{(-n)_k \cdot (n-k-i)_k} + (i-n) \cdot \frac{(-k)_k}{(-n)_k} \right] && (3.7) \\
&= \frac{1}{k} \cdot \frac{(-k)_k}{(-n)_k} && \text{da } (-i)_k = 0, \text{ für } i \in \{0, \ldots, n-k\} \text{ und } n-k < k \\
&= \frac{1}{k} \cdot (-1)^k \cdot \frac{k!}{(-n)_k} = \frac{1}{k} \cdot \binom{n}{k}^{-1}. && \text{nach Lemma 2.1}
\end{aligned}$$

Setzt man A in (3.5) ein, erhält man

$$\begin{aligned}
&\sum_{i=0}^{n-k} \binom{n-i}{k-1} \cdot z_i \cdot (n-k+1-i) \cdot \frac{1}{k} \cdot \binom{n}{k}^{-1} \\
&\quad = \sum_{i=0}^{n-k} z_i \cdot \frac{(n-k+1-i) \cdot (n-i)!}{(k-1)! \cdot (n-i-k+1)! \cdot k} \cdot \binom{n}{k}^{-1} && \text{nach Definition 2.2} \\
&\quad = \sum_{i=0}^{n-k} z_i \cdot \binom{n-i}{k} \cdot \binom{n}{k}^{-1} = \sum_{i=0}^{n-k} z_i \cdot \binom{n-k}{i} \cdot \binom{n}{i}^{-1} && \text{nach Lemma 2.7,}
\end{aligned}$$

was dem Zielfunktionswert entspricht, der bereits durch die Belegung z erreicht wurde.

Fall II: $n-k \geq \frac{n}{2} \Longleftrightarrow n-k \geq k$:

Die Zielfunktion ist

$$\sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot z'_j = \sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot (-1)^k \cdot z_{n-j}.$$

Da $n-k \geq k$ gilt, ist Lemma 3.4 nicht für alle Variablen z_{n-j} anwendbar. Somit folgt

$$\begin{aligned}
&= (-1)^k \cdot \sum_{j=0}^{k-1} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot (-1)^{k-j} \cdot \binom{k-1}{j} \cdot \sum_{i=0}^{n-k} \binom{n-i}{k-1} \cdot z_i \cdot \frac{n-k+1-i}{n-j-i} \\
&\quad + (-1)^k \cdot \sum_{j=k}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} z_{n-j} \\
&= \sum_{i=0}^{n-k} \sum_{j=0}^{k-1} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot (-1)^j \cdot \binom{k-1}{j} \cdot \binom{n-i}{k-1} \cdot z_i \cdot \frac{n-k+1-i}{n-j-i} \\
&\quad + (-1)^k \cdot \sum_{j=k}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} z_{n-j} \\
&= \sum_{i=0}^{n-k} \binom{n-i}{k-1} \cdot z_i \cdot (n-k+1-i) \cdot \underbrace{\sum_{j=0}^{k-1} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot (-1)^j \cdot \binom{k-1}{j} \cdot \frac{1}{n-j-i}}_{B} \\
&\quad + (-1)^k \cdot \sum_{j=k}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} z_{n-j} \qquad (3.8)
\end{aligned}$$

Nach Lemma 2.1 gilt für die Summe B

$$B = \sum_{j=0}^{k-1} \frac{(k-n)_j \cdot (1-k)_j}{(-n)_j \cdot j!} \cdot \frac{1}{n-j-i} = \frac{1}{n-i} \cdot \sum_{j=0}^{k-1} \frac{(k-n)_j \cdot (1-k)_j \cdot (i-n)_j}{(-n)_j \cdot (i-n+1)_j \cdot j!}$$

Für den Term $(1-k)_j$ mit $j \geq k$ gilt $(1-k)_j = 0$. Deshalb kann die obere Summationsgrenze $k-1$ entfallen und durch unendlich ersetzt werden. Nach Definition 2.5 gilt dann

$$B = \frac{1}{n-i} \cdot {}_3F_2\left(\begin{matrix} k-n, 1-k, i-n \\ -n, i-n+1 \end{matrix} ; 1 \right).$$

Dieses entspricht dem Term A aus (3.6), welcher ausgewertet identisch zu (3.7) ist.

Allerdings muss berücksichtigt werden, dass $(-i)_k \neq 0$ gelten kann. Mit

$$\begin{aligned}
B &= -\frac{1}{k\cdot(n-i)}\cdot\left[(n-i-k)\cdot\frac{(-k)_k\cdot(-i)_k}{(-n)_k\cdot(n-k-i)_k}+(i-n)\cdot\frac{(-k)_k}{(-n)_k}\right]\\
&= -\frac{1}{k\cdot(n-i)}\cdot\frac{(-k)_k}{(-n)_k}\cdot\left[(n-i-k)\cdot\frac{(-i)_k}{(n-k-i)_k}+(i-n)\right]\\
&= -\frac{1}{k\cdot(n-i)}\cdot\binom{n}{k}^{-1}\cdot\left[(n-i-k)\cdot\frac{(-i)_k\cdot k!\cdot(-1)^k}{(n-k-i)_k\cdot k!\cdot(-1)^k}+(i-n)\right]\\
&\qquad\qquad\text{nach Lemma 2.1}\\
&= -\frac{1}{k\cdot(n-i)}\cdot\binom{n}{k}^{-1}\cdot\left[(n-i-k)\cdot\binom{i}{k}\cdot\binom{n-k-i}{k}^{-1}+(i-n)\right]\\
&\qquad\qquad\text{nach Lemma 2.1}\\
&= \frac{1}{n-i}\cdot\binom{n}{k}^{-1}\cdot\left[\frac{n-i}{k}-(-1)^k\cdot\binom{i}{k}\cdot\binom{n-i-1}{k-1}^{-1}\right]\qquad\text{nach Lemma 2.6}
\end{aligned}$$

folgt für (3.8)

$$\begin{aligned}
&\sum_{i=0}^{n-k}\binom{n-i}{k-1}\cdot z_i\cdot\frac{n-k+1-i}{n-i}\cdot\binom{n}{k}^{-1}\cdot\left[\frac{n-i}{k}-(-1)^k\cdot\binom{i}{k}\cdot\binom{n-i-1}{k-1}^{-1}\right]\\
&\quad\underbrace{+(-1)^k\cdot\sum_{j=k}^{n-k}\binom{n-k}{j}\cdot\binom{n}{j}^{-1}z_{n-j}}_{C}\\
&=\sum_{i=0}^{n-k}\binom{n-i}{k-1}\cdot z_i\cdot\frac{n-k+1-i}{n-i}\cdot\binom{n}{k}^{-1}\cdot\frac{n-i}{k}+C\\
&\quad\underbrace{-\sum_{i=0}^{n-k}\binom{n-i}{k-1}\cdot z_i\cdot\frac{n-k+1-i}{n-i}\cdot\binom{n}{k}^{-1}\cdot(-1)^k\cdot\binom{i}{k}\cdot\binom{n-i-1}{k-1}^{-1}}_{D}.
\end{aligned}\tag{3.9}$$

Die Summe D lässt sich vereinfachen zu

$$\begin{aligned}
D &= -(-1)^k\cdot\sum_{i=0}^{n-k}z_i\cdot\binom{n}{k}^{-1}\cdot\binom{i}{k}\\
&\qquad\cdot\frac{(n-k+1-i)\cdot(n-i)!\cdot(k-1)!\cdot(n-i-1-k+1)!}{(n-i)\cdot(k-1)!\cdot(n-i-k+1)!\cdot(n-i-1)!}\\
&\qquad\qquad\text{nach Definition 2.2}\\
&= -(-1)^k\cdot\sum_{i=0}^{n-k}z_i\cdot\binom{n}{k}^{-1}\cdot\binom{i}{k} = -(-1)^k\cdot\sum_{i=k}^{n-k}z_i\cdot\binom{n}{k}^{-1}\cdot\binom{i}{k}\\
&\qquad\qquad\text{da }\tbinom{i}{k}=0\quad\forall i<k
\end{aligned}$$

$$= -(-1)^k \cdot \sum_{i=k}^{n-k} z_i \cdot \binom{n-k}{i-k} \cdot \binom{n}{i}^{-1} \qquad \text{nach Lemma 2.7.}$$

Für $C + D$ folgt damit

$$\begin{aligned} C + D &= -(-1)^k \cdot \sum_{i=k}^{n-k} z_i \cdot \binom{n-k}{i-k} \cdot \binom{n}{i}^{-1} + (-1)^k \cdot \sum_{j=k}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} z_{n-j} \\ &= -(-1)^k \cdot \sum_{i=k}^{n-k} z_{n-i} \cdot \binom{n-k}{n-k-i} \cdot \binom{n}{n-i}^{-1} + (-1)^k \cdot \sum_{j=k}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} z_{n-j} \\ &= -(-1)^k \cdot \sum_{i=k}^{n-k} z_{n-i} \cdot \binom{n-k}{i} \cdot \binom{n}{i}^{-1} + (-1)^k \cdot \sum_{j=k}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} z_{n-j} \\ &= 0. \end{aligned} \tag{3.10}$$

Zusammenfassend gilt für (3.9)

$$\begin{aligned} &\sum_{i=0}^{n-k} \binom{n-i}{k-1} \cdot z_i \cdot \frac{n-k+1-i}{n-i} \cdot \binom{n}{k}^{-1} \cdot \frac{n-i}{k} \\ &\quad = \sum_{i=0}^{n-k} z_i \cdot \frac{(n-k+1-i) \cdot (n-i)!}{(k-1)! \cdot (n-i-k+1)! \cdot k} \cdot \binom{n}{k}^{-1} = \sum_{i=0}^{n-k} z_i \cdot \binom{n-i}{k} \cdot \binom{n}{k}^{-1} \\ &\qquad \text{nach Definition 2.2} \\ &\quad = \sum_{i=0}^{n-k} z_i \cdot \binom{n-k}{i} \cdot \binom{n}{i}^{-1} \qquad \text{nach Lemma 2.7,} \end{aligned}$$

was dem Zielfunktionswert entspricht, der bereits durch die Belegung z erreicht wurde. Damit ist die Behauptung bewiesen. □

Korollar 3.1:
Für das Lineare Programm $L(k, n)_z$ existiert immer eine optimale Lösung $z = (z_0, z_1, \ldots, z_n)$ mit $z_i = (-1)^k \cdot z_{n-i}$.

Beweis: Sei $z' = (z'_0, z'_1, \ldots, z'_n)$ eine optimale Belegung des Linearen Programms $L(k, n)_z$. Dann ist nach Lemma 3.8 auch $z'' = (z''_0, z''_1, \ldots, z''_n)$ mit $z''_i := (-1)^k \cdot z'_{n-i}$ eine optimale Belegung. Nun kann die Belegung $z''' = (z'''_0, z'''_1, \ldots, z'''_n)$ mit $z'''_i := \frac{1}{2} \cdot (z'_i + z''_i)$ definiert werden. Diese ist nach Lemma 3.7 Punkt 1 ebenfalls optimal. Wäre diese Belegung nicht optimal, könnte durch Lemma 3.7 Punkt 2 eine Belegung konstruiert werden, welche einen größeren Zielfunktionswert liefert. Dieses wäre jedoch ein Widerspruch zur Optimalität

der Belegungen z' und z''. Für z''' gilt

$$\begin{aligned} z'''_i &= \frac{1}{2} \cdot (z'_i + z''_i) = \frac{1}{2} \cdot (z'_i + (-1)^k \cdot z'_{n-i}) \\ z'''_{n-i} &= \frac{1}{2} \cdot (z'_{n-i} + z''_{n-i}) = \frac{1}{2} \cdot (z'_{n-i} + (-1)^k \cdot z'_i) \\ \Longrightarrow \qquad z'''_i &= (-1)^k \cdot z'''_{n-i}. \end{aligned}$$

Somit gilt die Behauptung. □

Mit Hilfe dieser Struktureigenschaft einer optimalen Lösung für das Lineare Programm $L(k,n)_z$ ist es nun möglich, die Variablenanzahl auf $\lceil \frac{n-k}{2} + 1 \rceil$ zu senken. Im folgenden Kapitel wird die Vorgehensweise dafür anhand spezieller Linearer Programme aufgezeigt.

4 Anwendungen

Im vorigen Kapitel wurden einige Eigenschaften einer optimalen Belegung des Linearen Programms $L(k,n)_z$ gezeigt. Diese können nun dazu genutzt werden, optimale Belegungen zu finden. In diesem Kapitel werden diese Anwendungen aufgezeigt.
In [7] haben Krause und Simon gezeigt, dass für den optimalen Kontrast $\alpha_{k,n}$ eines (k,n)-Schemas der Visuellen Kryptographie die Schranke gilt

$$4^{-k+1} \leq \alpha_{k,n} \leq \frac{4^{-k+1} \cdot n^k}{(n-k+1)_k}.$$

Wenn n gegen unendlich geht, gilt damit $\alpha = 4^{-k+1}$. Wenn $k = 2$ und n gerade ist oder $k = 3$ und n durch 4 teilbar ist, gilt

$$\alpha_{k,n} = \frac{4^{-k+1} \cdot n^k}{(n-k+1)_k}.$$

Krause und Simon haben diese Aussagen durch die Verwendung von Linearen Programmen der Typen *Best Approximating Vector* und *Best Approximating Polynomial* bewiesen. Details hierzu sind in [7] zu finden.

4.1 Das Lineare Programm $L(k,k)_z$

Das Lineare Programm $L(k,k)_z$ ist nach Definition 3.5 wie folgt definiert.

Definition 4.1:
Das Lineare Programm $L(k,k)_z$ mit $k \geq 2$ wird für die Variablen $(z_0, \ldots, z_k)$, welche rationale Zahlen sind, definiert als

Zielfunktion: $L(k,k)_z = z_0 \longrightarrow$ maximieren
Nebenbedingungen:

1. $-1 \leq z_j \leq 1, \qquad j = 0, \ldots, k$
2. $\sum_{j=0}^{k} z_j = 0$

a) $\sum\limits_{\substack{j=0 \\ z_j>0}}^{k} z_j = 1$

b) $\sum\limits_{\substack{j=0 \\ z_j<0}}^{k} z_j = -1$

3. $\binom{k}{\ell}^{-1} \cdot z_\ell + \binom{k}{\ell+1}^{-1} \cdot z_{\ell+1} = 0, \qquad \ell = 0, \ldots, k-1.$

Nach Lemma 3.5 gilt für alle $\ell \in \{0, \ldots, k\}$

$$\begin{aligned} z_\ell &= (-1)^{\ell-(n-k)} \cdot \binom{n}{\ell} \cdot \sum_{j=0}^{n-k} \frac{(\ell-(n-k))_{n-k-j} \cdot (\ell+1-j)_j}{(n+1-j)_j \cdot (n-k-j)!} \cdot z_j \\ &= (-1)^\ell \cdot \binom{k}{\ell} \cdot \sum_{j=0}^{0} \frac{(\ell)_{-j} \cdot (\ell+1-j)_j}{(k+1-j)_j \cdot (-j)!} \cdot z_j \\ &= (-1)^\ell \cdot \binom{k}{\ell} \cdot z_0. \end{aligned} \tag{4.1}$$

Aus der Zielfunktion wird bereits deutlich, dass für eine optimale Belegung $z_0 > 0$ gelten muss. Somit kann (4.1) verwendet werden, um die Summe über die positiven Variablen zu bestimmen, welche den Wert 1 annehmen muss. Damit folgt

$$1 \stackrel{!}{=} \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} z_j = \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j} \cdot z_0 = z_0 \cdot \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j} = z_0 \cdot 2^{k-1} \qquad \text{nach Lemma 2.10}$$

$$\Longleftrightarrow$$

$$z_0 = 2^{-k+1}.$$

Dieses entspricht auch gerade dem Zielfunktionswert. Desweiteren ist diese optimale Belegung eindeutig, da sie direkt aus den Nebenbedingungen folgt.
Bereits Naor und Shamir haben in [8] einen Beweis der Optimalität dieses Kontrastes angegeben, allerdings unter Verwendung der approximativen Inklusion-Exklusion.

4.2 Das Lineare Programm $L(k-1,k)_z$

Das Lineare Programm $L(k-1,k)_z$ ist nach Definition 3.5 wie folgt definiert.

Definition 4.2:
Das Lineare Programm $L(k-1,k)_z$ mit $k \geq 3$ wird für die Variablen $(z_0, \ldots, z_k)$, welche rationale Zahlen sind, definiert als

Zielfunktion: $L(k-1,k)_z = z_0 + \frac{z_1}{k} \longrightarrow$ maximieren
Nebenbedingungen:

1. $-1 \leq z_j \leq 1, \qquad j = 0, \ldots, k$
2. $\sum_{j=0}^{k} z_j = 0$
   a) $\sum_{\substack{j=0 \\ z_j>0}}^{k} z_j = 1$
   b) $\sum_{\substack{j=0 \\ z_j<0}}^{k} z_j = -1$
3. $\binom{k}{\ell}^{-1} \cdot z_\ell + 2 \cdot \binom{k}{\ell+1}^{-1} \cdot z_{\ell+1} + \binom{k}{\ell+2}^{-1} \cdot z_{\ell+2} = 0, \qquad \ell = 0, \ldots, k-2.$

Nach Lemma 3.5 gilt für alle $\ell \in \{0, \ldots, k\}$

$$\begin{aligned} z_\ell &= (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot \sum_{j=0}^{1} \frac{(\ell-1)_{1-j} \cdot (\ell+1-j)_j}{(k+1-j)_j \cdot (1-j)!} \cdot z_j \\ &= (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot \left[(\ell-1) \cdot z_0 + \frac{\ell}{k} \cdot z_1 \right] \\ &= (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot \left(\frac{1}{k} \cdot z_1 + (\ell-1) \left(z_0 + \frac{1}{k} \cdot z_1 \right) \right). \end{aligned} \tag{4.2}$$

Diese Formel wurde bereits in [5] durch einen Induktionsbeweis gezeigt.
Nach Korollar 3.1 muss eine optimale Belegung der Variablen existieren, für die $z_\ell = (-1)^{k-1} \cdot z_{k-\ell}$ gilt. Damit folgt für eine optimale Belegung

$$\begin{aligned} 0 &= (-1)^{k-1} \cdot z_{k-\ell} - z_\ell \\ &= (-1)^{k-1} \cdot (-1)^{k-\ell-1} \cdot \binom{k}{k-\ell} \cdot \left(\frac{1}{k} \cdot z_1 + (k-\ell-1) \left(z_0 + \frac{1}{k} \cdot z_1 \right) \right) \\ &\quad - (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot \left(\frac{1}{k} \cdot z_1 + (\ell-1) \left(z_0 + \frac{1}{k} \cdot z_1 \right) \right) \qquad \text{nach (4.2)} \\ &= (-1)^{\ell} \cdot \binom{k}{\ell} \cdot \left(\frac{2}{k} \cdot z_1 + (k-2) \left(z_0 + \frac{1}{k} \cdot z_1 \right) \right) \\ \iff \qquad 0 &= \frac{2}{k} \cdot z_1 + (k-2) \cdot \left(z_0 + \frac{1}{k} \cdot z_1 \right) = (k-2) \cdot z_0 + z_1 \\ \iff \qquad z_0 &= -\frac{z_1}{k-2}. \end{aligned} \tag{4.3}$$

Setzt man diese Beziehung in (4.2) ein, gilt für alle $\ell \in \{0, \ldots, k\}$

$$\begin{aligned} z_\ell &= (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot \left(\frac{1}{k} \cdot z_1 + (\ell - 1) \left(\frac{1}{k} \cdot z_1 - \frac{z_1}{k-2} \right) \right) \\ &= (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot z_1 \cdot \frac{k - 2 \cdot \ell}{(k-2) \cdot k}. \end{aligned} \tag{4.4}$$

Als Zielfunktion ergibt sich aus (4.3)

$$z_0 + \frac{1}{k} \cdot z_1 = z_1 \cdot \left(\frac{1}{k} - \frac{1}{k-2} \right) = -z_1 \cdot \frac{2}{(k-2) \cdot k},$$

weswegen $z_1 < 0$ gelten muss, da der Zielfunktionswert sonst negativ wäre, was bei einer optimalen Belegung nicht möglich ist.
Damit die Nebenbedingung $2a$ erfüllt wird, kann die Summe über alle positiven Variablen bestimmt werden, unter Zuhilfenahme von (4.4). Allerdings muss hierbei beachtet werden, dass k gerade oder ungerade sein kann.

Der Fall k gerade

Aus (4.4) wird ersichtlich, dass für $\ell < \frac{k}{2}$ die z_ℓ positiv sind, bei denen ℓ eine gerade Zahl ist, da $z_1 < 0$ gilt. Für $\ell > \frac{k}{2}$ sind hingegen die z_ℓ positiv, bei denen ℓ eine ungerade Zahl ist. Durch die Beziehung $z_\ell = (-1)^{k-1} \cdot z_{k-\ell} = -z_{k-\ell}$ ist die Summe der positiven z_ℓ für $\ell > \frac{k}{2}$ gleich dem Betrag der Summe der negativen z_ℓ für $\ell < \frac{k}{2}$. Somit kann die Summe der positiven z_ℓ durch die Summe der negativen z_ℓ, mit -1 multipliziert, ersetzt werden. Dieses vereinfacht die Summenberechnung:

$$1 \overset{!}{=} \sum_{\substack{j=0 \\ z_j > 0}}^{k} z_j = \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k/2} z_j - \sum_{\substack{j=1 \\ j \text{ ungerade}}}^{k/2} z_j = -\sum_{j=0}^{k/2} \left(\frac{1}{k} z_1 + (j-1) \left(-\frac{z_1}{k-2} + \frac{1}{k} z_1 \right) \right) \binom{k}{j}$$

nach (4.2) und (4.3)

$$\begin{aligned} &= -\sum_{j=0}^{k/2} z_1 \left(\frac{j}{k} - \frac{j-1}{k-2} \right) \binom{k}{j} \\ &= -z_1 \cdot \left[\frac{1}{k} \cdot \sum_{j=0}^{k/2} \binom{k}{j} \cdot j - \frac{1}{k-2} \cdot \sum_{j=0}^{k/2} \binom{k}{j} \cdot j + \frac{1}{k-2} \cdot \sum_{j=0}^{k/2} \binom{k}{j} \right] \\ &= -z_1 \cdot \left[\frac{1}{k} \cdot \frac{k \cdot 2^k}{4} - \frac{1}{k-2} \cdot \frac{k \cdot 2^k}{4} + \frac{1}{k-2} \cdot \left(2^{k-1} + \frac{1}{2} \cdot \binom{k}{\frac{k}{2}} \right) \right] \end{aligned}$$

nach Lemma 2.12 und 2.11

$$= -z_1 \cdot \left[2^{k-2} \cdot \left(1 - \frac{k}{k-2} + \frac{2}{k-2} \right) + \frac{1}{2 \cdot (k-2)} \binom{k}{\frac{k}{2}} \right] = -\frac{z_1}{2 \cdot (k-2)} \binom{k}{\frac{k}{2}}$$

$$\iff \quad z_1 = (4-2k) \binom{k}{\frac{k}{2}}^{-1}. \tag{4.5}$$

Aus (4.3) und (4.5) folgt

$$z_0 = -\frac{z_1}{k-2} = -\frac{1}{k-2}(4-2k) \binom{k}{\frac{k}{2}}^{-1} = 2 \binom{k}{\frac{k}{2}}^{-1}$$

und damit gilt für den optimalen Zielfunktionswert

$$z_0 + \frac{z_1}{k} = 2 \binom{k}{\frac{k}{2}}^{-1} + \frac{4-2k}{k} \binom{k}{\frac{k}{2}}^{-1} = \frac{4}{k} \binom{k}{\frac{k}{2}}^{-1}.$$

Eine optimale Belegung für das Lineare Programm $L(k-1,k)$ für k gerade ist damit für $\ell = 0, \ldots, k$ gegeben durch

$$z_\ell = (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot \binom{k}{\frac{k}{2}}^{-1} \left(\frac{4 \cdot \ell}{k} - 2 \right) \qquad \text{nach (4.2).}$$

Diese Belegung ist eindeutig, was aus dem folgenden Lemma folgt.

Lemma 4.1:
Sei k gerade und $z = (z_0, \ldots, z_k)$ eine optimale Belegung für das Lineare Programm $L(k-1,k)_z$. Dann gilt $z_{\frac{k}{2}} = 0$.

Beweis:
Sei $z' = (z'_0, \ldots, z'_k)$ eine optimale Belegung für das Lineare Programm $L(k-1,k)_z$ mit $z'_{\frac{k}{2}} \neq 0$. Dann ist $z'' = (z''_0, \ldots, z''_k)$ mit $z''_i := -z'_{k-i}$ ebenfalls eine optimale Belegung, nach Lemma 3.8. Diese beiden Belegungen sind verschieden, da $z''_{\frac{k}{2}} = -z'_{\frac{k}{2}}$ gilt und nach Annahme diese Werte ungleich 0 sind. Nun konstruiert man die Belegung $z''' = (z'''_0, \ldots, z'''_k)$ mit $z'''_i := \frac{1}{2}(z'_i + z''_i)$. Im Beweis von Lemma 3.7 wird gezeigt, dass diese Belegung nur dann zulässig ist, wenn für kein i die Beziehung $\operatorname{sgn}(z'_i) = -\operatorname{sgn}(z''_i) \neq 0$ gilt. Für $i = \frac{k}{2}$ gilt diese Beziehung jedoch. Also ist z''' nicht zulässig. Somit kann, nach Lemma 3.7 Punkt 2, eine weitere Belegung z'''', durch Skalierung der Belegung z''', definiert werden, die einen größeren Zielfunktionswert liefert, als die Belegungen z' und z'' und für die $z''''_{\frac{k}{2}} = 0$ gilt. □

Mit $z_{\frac{k}{2}} = 0$ folgt für jede optimale Belegung

$$\begin{aligned} & 0 = (-1)^{\frac{k}{2}-1} \cdot z_\ell = (-1)^{\frac{k}{2}-1} \cdot \binom{k}{\frac{k}{2}} \cdot \left(\frac{1}{k} \cdot z_1 + \left(\frac{k}{2} - 1 \right) \left(z_0 + \frac{1}{k} \cdot z_1 \right) \right) \\ \iff \quad & 0 = \frac{2}{k} \cdot z_1 + (k-2) \cdot \left(z_0 + \frac{1}{k} \cdot z_1 \right) \\ & \quad = (k-2) \cdot z_0 + z_1 \\ \iff \quad & z_0 = -\frac{z_1}{k-2}, \end{aligned}$$

also die selbe Beziehung, wie sie durch (4.3) ausgedrückt wird. Da hieraus, zusammen mit der Nebenbedingung $2a$, die bereits angegebene Belegung folgt, ist diese eindeutig.
Das selbe Resultat haben Blundo, D'Arco, De Santis und Stinson in [1] durch die Verwendung von *kanonischen Matrizen* nachgewiesen.

Der Fall k ungerade

Um die Nebenbedingung $2a$ mit $z_1 < 0$ zu erfüllen, muss die Summe der positiven Variablen gleich 1 sein. Aus (4.4) wird ersichtlich, dass für $\ell < \frac{k}{2}$ die Variablen z_ℓ mit geradem ℓ positiv sind. Für $\ell > \frac{k}{2}$ sind die Variablen z_ℓ mit ungeradem ℓ positiv. Somit muss gelten

$$1 \stackrel{!}{=} \sum_{\substack{\ell=0 \\ \ell \text{ gerade}}}^{\frac{k-1}{2}} (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot z_1 \cdot \frac{k - 2 \cdot \ell}{(k-2) \cdot k} + \sum_{\substack{\ell=\frac{k+1}{2} \\ \ell \text{ ungerade}}}^{k} (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot z_1 \cdot \frac{k - 2 \cdot \ell}{(k-2) \cdot k}.$$

Da $z_\ell = z_{k-\ell}$ nach Korollar 3.1 gilt und für ungerade ℓ der Term $k - \ell$ eine gerade Zahl ist, lässt sich diese Summe vereinfachen zu

$$\begin{aligned} 1 &= 2 \cdot \sum_{\substack{\ell=0 \\ \ell \text{ gerade}}}^{\frac{k-1}{2}} (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot z_1 \cdot \frac{k - 2 \cdot \ell}{(k-2) \cdot k} \\ &= -\frac{2 \cdot z_1}{(k-2) \cdot k} \cdot \sum_{\substack{\ell=0 \\ \ell \text{ gerade}}}^{\frac{k-1}{2}} \binom{k}{\ell} \cdot (k - 2 \cdot \ell) \\ &= -\frac{2 \cdot z_1}{(k-2) \cdot k} \cdot \left[k \cdot \sum_{\substack{\ell=0 \\ \ell \text{ gerade}}}^{\frac{k-1}{2}} \binom{k}{\ell} - 2 \cdot \sum_{\substack{\ell=0 \\ \ell \text{ gerade}}}^{\frac{k-1}{2}} \binom{k}{\ell} \cdot \ell \right] \end{aligned}$$

$$= -\frac{2 \cdot z_1}{(k-2) \cdot k} \cdot \left[k \cdot \left(2^{k-2} + \frac{(-1)^{\frac{k-1}{2}}}{2} \binom{k-1}{\frac{k-1}{2}} \right) \right. \qquad \text{nach Lemma 2.14}$$

$$\left. - 2 \cdot k \cdot \left(2^{k-3} - \frac{1-(-1)^{\frac{k-1}{2}}}{4} \binom{k-1}{\frac{k-1}{2}} \right) \right]$$

nach Lemma 2.16

$$= -\frac{z_1}{(k-2)} \cdot \binom{k-1}{\frac{k-1}{2}}$$

$$\iff \quad z_1 = -(k-2) \cdot \binom{k-1}{\frac{k-1}{2}}^{-1}.$$

Damit folgt für z_0

$$z_0 = -\frac{z_1}{k-2} = \binom{k-1}{\frac{k-1}{2}}^{-1} \qquad \text{nach (4.3)}$$

und für den Zielfunktionswert gilt

$$z_0 + \frac{1}{k} \cdot z_1 = \binom{k-1}{\frac{k-1}{2}}^{-1} - \frac{1}{k} \cdot (k-2) \cdot \binom{k-1}{\frac{k-1}{2}}^{-1} = \binom{k-1}{\frac{k-1}{2}}^{-1} \cdot \frac{2}{k},$$

was dem Zielfunktionswert entspricht, der von Blundo, D'Arco, De Santis und Stinson in [1] angegeben wurde.
Damit ist für ungerades k eine optimale Belegung der Variablen gegeben durch

$$z_\ell = (-1)^\ell \cdot \binom{k}{\ell} \cdot \binom{k-1}{\frac{k-1}{2}}^{-1} \cdot \frac{k-2 \cdot \ell}{k} \qquad \text{nach (4.2)}$$

für alle $\ell \in \{0, \ldots, k\}$. Allerdings muss diese Belegung nicht eindeutig sein, denn durch die Verwendung von Korollar 3.1 werden mögliche optimale Belegungen, bei denen $z_\ell = z_{k-\ell}$ nicht gilt, ignoriert.

4.3 Das Lineare Programm $L(k-2,k)_z$

Das Lineare Programm $L(k-2,k)_z$ ist nach Definition 3.5 wie folgt definiert.

Definition 4.3:
Das Lineare Programm $L(k-2,k)_z$ mit $k \geq 4$ wird für die Variablen $(z_0, \ldots, z_k)$, welche rationale Zahlen sind, definiert als

Zielfunktion: $L(k-2,k)_z = z_0 + \frac{2}{k} \cdot z_1 + \frac{2}{k(k-1)} \cdot z_2 \longrightarrow$ maximieren

Nebenbedingungen:

1. $-1 \leq z_j \leq 1, \qquad j = 0, \ldots, k$
2. $\sum_{j=0}^{k} z_j = 0$
   a) $\sum_{\substack{j=0 \\ z_j>0}}^{k} z_j = 1$
   b) $\sum_{\substack{j=0 \\ z_j<0}}^{k} z_j = -1$
3. $\binom{k}{\ell}^{-1} \cdot z_\ell + 3 \cdot \binom{k}{\ell+1}^{-1} \cdot z_{\ell+1} + 3 \cdot \binom{k}{\ell+2}^{-1} \cdot z_{\ell+2} + \binom{k}{\ell+3}^{-1} \cdot z_{\ell+3} = 0, \qquad \ell = 0, \ldots, k-3.$

Nach Lemma 3.5 gilt für alle $\ell \in \{0, \ldots, k\}$

$$\begin{aligned} z_\ell &= (-1)^{\ell-(n-k)} \cdot \binom{n}{\ell} \cdot \sum_{j=0}^{n-k} \frac{(\ell-(n-k))_{n-k-j} \cdot (\ell+1-j)_j}{(n+1-j)_j \cdot (n-k-j)!} \cdot z_j \\ &= (-1)^\ell \binom{k}{\ell} \left[\frac{(\ell-2)(\ell-1)}{2} z_0 + \frac{(\ell-2)\ell}{k} z_1 + \frac{(\ell-1)\ell}{k(k-1)} z_2 \right]. \end{aligned} \tag{4.6}$$

Nach Korollar 3.1 existiert eine optimale Belegung der Variablen, für die $z_\ell = (-1)^{k-2} \cdot z_{k-\ell}$ gilt. Für z_2 folgt damit

$$\begin{aligned} z_2 &= (-1)^{k-2} \cdot z_{k-2} = \binom{k}{2} \left[\frac{(k-4)(k-3)}{2} z_0 + \frac{(k-4)(k-2)}{k} z_1 + \frac{(k-3)(k-2)}{k(k-1)} z_2 \right] \\ &= \frac{k(k-1)}{2} \left[\frac{(k-4)(k-3)}{2} z_0 + \frac{(k-4)(k-2)}{k} z_1 \right] + \frac{(k-3)(k-2)}{2} z_2 \end{aligned}$$

$\iff$

$$z_2 \cdot \left[1 - \frac{(k-3)(k-2)}{2} \right] = \left[\frac{(k-4)(k-3)(k-1)k}{4} z_0 + \frac{(k-4)(k-2)(k-1)}{2} z_1 \right]$$

$\iff$

$$\begin{aligned} z_2 &= \left[\frac{(k-4)(k-3)(k-1)k}{4} z_0 + \frac{(k-4)(k-2)(k-1)}{2} z_1 \right] \cdot \left[-\frac{2}{(k-4)(k-1)} \right] \\ &= -\frac{(k-3)k}{2} z_0 - (k-2) z_1. \end{aligned}$$

Für die Zielfunktion gilt somit

$$\begin{aligned} z_0 + \frac{2}{k} \cdot z_1 + \frac{2}{k(k-1)} \cdot z_2 &= z_0 + \frac{2}{k} \cdot z_1 - \frac{(k-3)}{(k-1)} z_0 - \frac{2(k-2)}{k(k-1)} z_1 \\ &= \frac{2}{(k-1)} z_0 + \frac{2}{k(k-1)} z_1 = \frac{2}{k-1} \left(z_0 + \frac{1}{k} z_1 \right). \end{aligned} \tag{4.7}$$

Setzt man z_2 in (4.6) ein, folgt für alle $\ell \in \{0, \ldots, k\}$

$$\begin{aligned} z_\ell &= (-1)^\ell \binom{k}{\ell} \left[\frac{(\ell-2)(\ell-1)}{2} z_0 + \frac{(\ell-2)\ell}{k} z_1 + \frac{(\ell-1)\ell}{k(k-1)} \cdot \left(-\frac{(k-3)k}{2} z_0 - (k-2) z_1 \right) \right] \\ &= (-1)^\ell \binom{k}{\ell} \left[\frac{(\ell-1)(\ell+1-k)}{k-1} z_0 - \frac{\ell(k-\ell)}{k(k-1)} z_1 \right] \\ &= (-1)^\ell \binom{k}{\ell} \left[\frac{\ell^2 - k\ell - 1 + k}{k-1} z_0 - \frac{\ell k - \ell^2}{k(k-1)} z_1 \right] \\ &= (-1)^\ell \binom{k}{\ell} \underbrace{\frac{1}{k-1} \left(z_0 + \frac{1}{k} z_1 \right)}_{A} \underbrace{\left(\ell^2 - k\ell + \frac{z_0 k(k-1)}{z_0 k + z_1} \right)}_{B}. \end{aligned} \tag{4.8}$$

Der Term A ist identisch zur Hälfte der Zielfunktion. Daher kann dieser Wert als positiv angenommen werden. Damit entscheidet der Term B darüber, welche Variablen z_ℓ positiv und negativ sind. Die Nullstellen ℓ_1 und ℓ_2 von B sind

$$\begin{aligned} B = 0 \quad \Longleftrightarrow \quad \ell_1 &= \frac{k}{2} - \sqrt{\frac{k^2}{4} - \frac{z_0 k(k-1)}{z_0 k + z_1}} \\ \ell_2 &= \frac{k}{2} + \sqrt{\frac{k^2}{4} - \frac{z_0 k(k-1)}{z_0 k + z_1}}. \end{aligned}$$

Allerdings muss noch untersucht werden, ob die Diskriminante positiv, gleich 0 oder negativ ist.

Annahme: Die Diskriminante ist negativ.

Da die Diskriminante negativ ist, hat die nach oben geöffnete Parabel B keine Nullstellen. Also ist $B > 0$ für alle $\ell \in \{0, \ldots, k\}$. Somit kann die Summe über die positiven Variablen z_ℓ bestimmt werden:

$$1 \overset{!}{=} \sum_{\substack{j=0 \\ z_j > 0}}^{k} z_j = \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j} \frac{1}{k-1} \left(z_0 + \frac{1}{k} z_1 \right) \left(j^2 - kj + \frac{z_0 k(k-1)}{z_0 k + z_1} \right)$$

$$= \frac{1}{k-1}\left(z_0 + \frac{1}{k}z_1\right) \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j}\left(j^2 - kj + \frac{z_0 k(k-1)}{z_0 k + z_1}\right)$$

$$\iff \quad \underbrace{\frac{1}{k-1}\left(z_0 + \frac{1}{k}z_1\right)}_{A} = \left[\sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j}\left(j^2 - kj + \frac{z_0 k(k-1)}{z_0 k + z_1}\right)\right]^{-1}.$$

Wie bereits erwähnt wurde, entspricht der Term A der Hälfte der Zielfunktion. Diese lässt sich also darstellen als

$$2 \cdot \left[\sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j}\left(j^2 - kj + \frac{z_0 k(k-1)}{z_0 k + z_1}\right)\right]^{-1} \longrightarrow \text{ maximieren.}$$

Da der Zähler dieses Bruches konstant ist, wird die Zielfunktion maximal, wenn die Summe minimal wird. Für die Summe gilt

$$\begin{aligned}
\sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j}\left(j^2 - kj + \frac{z_0 k(k-1)}{z_0 k + z_1}\right) &= \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j}(j^2 - kj) + \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j}\frac{z_0 k(k-1)}{z_0 k + z_1} \\
&= \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j} \cdot j^2 - k \cdot \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j} \cdot j + \frac{z_0 k(k-1)}{z_0 k + z_1} \cdot \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j} \\
&= k(k+1)2^{k-3} - k^2 \cdot 2^{k-2} + \frac{z_0 k(k-1)}{z_0 k + z_1} \cdot 2^{k-1} \quad \text{nach Lemma 2.17, 2.15 und 2.10} \\
&= 2^{k-3}(k - k^2) + \underbrace{\frac{z_0 k(k-1)}{z_0 k + z_1}}_{C} 2^{k-1}
\end{aligned}$$

und damit ist die Zielfunktion

$$\frac{2}{2^{k-3}(k-k^2) + C \cdot 2^{k-1}}.$$

Es wird also ein C gesucht, so dass diese Funktion maximal wird. Dabei muss $C > \frac{k^2}{4}$ gelten, da andernfalls das Polynom B eine Nullstelle hätte. Daraus folgt, dass der Zielfunktionswert kleiner als

$$\frac{2}{2^{k-3}(k-k^2) + \left(\frac{k^2}{4}\right) \cdot 2^{k-1}} = \frac{2^{4-k}}{k} = \frac{16}{2^k k} \tag{4.9}$$

sein muss. Damit erhält man eine obere Schranke für den Zielfunktionswert, wenn die Diskriminante negativ ist.

Annahme: Die Diskriminante ist nicht negativ.

Da die Diskriminante nicht negativ ist, existiert mindestens eine Nullstelle. Hierbei sind zwei Fälle zu unterscheiden:

- entweder existieren zwei Nullstellen außerhalb des Bereiches $(0, k)$, oder
- es existiert mindestens eine Nullstelle im Bereich $(0, k)$.

Nullstellen außerhalb des Bereiches $(0, k)$

Das Polynom B ist für alle zulässigen Werte von ℓ kleiner oder gleich 0. Daher sind in diesem Fall genau die z_ℓ positiv, bei denen ℓ eine ungerade Zahl ist. Bestimmt man die Summe über alle positiven z_ℓ, lässt sich analog zu dem Fall vorgehen, bei dem die Diskriminante negativ ist. Für die zu berechnenden Summen sind wieder die Lemmata 2.10, 2.15 und 2.17 anzuwenden. Deshalb ist die Zielfunktion wieder

$$\frac{2}{2^{k-3}(k-k^2)+C\cdot 2^{k-1}}.$$

Da die Nullstellen des Polynoms B außerhalb des Bereiches $(0, k)$ liegen, gilt $C \leq 0$. Sollte $z_0 = z_k = 0$ gelten, folgt $C = 0$ und damit ist die Zielfunktion

$$\frac{2^{4-k}}{k-k^2} < 0.$$

Falls $C < 0$ gilt, ist die Zielfunktion ebenfalls negativ. Deshalb kann dieser Fall für eine optimale Lösung nicht eintreten. Also muss für eine nichtnegative Diskriminante $0 < C \leq \frac{k^2}{4}$ gelten, um einen positiven Zielfunktionswert zu ermöglichen.

Nullstellen innerhalb des Bereiches $(0, k)$

Aus den bisherigen Fällen lässt sich schlussfolgern, dass das Polynom B entweder keine Nullstelle hat (und die Diskriminante ist negativ) oder es existiert genau eine Nullstelle im Bereich $\left(0, \frac{k}{2}\right] \subset \mathbb{R}$. Nur in diesen Fällen ist die Zielfunktion positiv. Die Nullstelle wird im Folgenden mit a bezeichnet. Sollte das Polynom nur eine (doppelte) Nullstelle aufweisen, muss diese bei $a = \frac{k}{2}$ liegen. Existieren zwei Nullstellen, befinden sich diese symmetrisch um die Stelle $\frac{k}{2}$ herum, also ist auch $(k - a)$ eine Nullstelle des Polynoms B.

Damit gilt

$$\begin{aligned}
0 = B &= \left(\ell^2 - k\ell + \frac{z_0 k(k-1)}{z_0 k + z_1}\right) \\
\iff & \\
0 &= \left(a^2 - ka\right)(z_0 k + z_1) + z_0 k(k-1) \\
&= a^2 k z_0 - a k^2 z_0 + a^2 z_1 - a k z_1 + k^2 z_0 - k z_0 \\
&= z_0(a^2 k - a k^2 + k^2 - k) + z_1(a^2 - ak) \\
\iff & \\
-z_1 &= \frac{z_0(a^2 k - a k^2 + k^2 - k)}{(a^2 - ak)} \\
\iff & \\
z_1 &= -z_0 \frac{k(a-1)(k-a-1)}{a(k-a)}.
\end{aligned}$$

Für die Zielfunktion folgt damit

$$\frac{2}{k-1}\left(z_0 + \frac{1}{k} z_1\right) = \frac{2 z_0}{k-1}\left(1 - \frac{(a-1)(k-a-1)}{a(k-a)}\right) = \frac{2}{a(k-a)} z_0 \tag{4.10}$$

und für alle $\ell \in \{0, \ldots, k\}$ gilt

$$\begin{aligned}
z_\ell &= (-1)^\ell \binom{k}{\ell} \left[\frac{\ell^2 - k\ell - 1 + k}{k-1} z_0 - \frac{\ell k - \ell^2}{k(k-1)} z_1\right] \\
&= (-1)^\ell \binom{k}{\ell} z_0 \left[\frac{\ell^2 - k\ell - 1 + k}{k-1} + \frac{(\ell k - \ell^2)(a-1)(k-a-1)}{a(k-a)(k-1)}\right] \\
&= (-1)^\ell \binom{k}{\ell} z_0 \frac{(a-\ell)(k-a-\ell)}{a(k-a)}.
\end{aligned} \tag{4.11}$$

Aus der Zielfunktion (4.10) folgt, dass $z_0 > 0$ gelten muss. Deshalb sind genau die Variablen z_ℓ positiv, für welche die folgenden Eigenschaften gelten:

- $\ell < a$ und ℓ gerade,
- $a < \ell < k - a$ und ℓ ungerade,
- $k - a < \ell$ und ℓ gerade.

Nun kann die Summe über die positiven Variablen gebildet werden. Es gilt

$$
\begin{aligned}
1 &\overset{!}{=} \sum_{\substack{j=0\\ j \text{ gerade}}}^{\lfloor a \rfloor} z_j + \sum_{\substack{j=\lceil a \rceil\\ j \text{ ungerade}}}^{\lfloor k-a \rfloor} z_j + \sum_{\substack{j=\lceil k-a \rceil\\ j \text{ gerade}}}^{k} z_j \\
&= \frac{z_0}{a(k-a)} \Bigg[\underbrace{\sum_{\substack{j=0\\ j \text{ gerade}}}^{\lfloor a \rfloor} \binom{k}{j} (a-j)(k-a-j)}_{S_A} + \underbrace{\sum_{\substack{j=\lceil a \rceil\\ j \text{ ungerade}}}^{\lfloor k-a \rfloor} \binom{k}{j} (j-a)(k-a-j)}_{S_B} \\
&\qquad + \underbrace{\sum_{\substack{j=\lceil k-a \rceil\\ j \text{ gerade}}}^{k} \binom{k}{j} (j-a)(j+a-k)}_{S_C} \Bigg] \\
\iff \quad & \frac{z_0}{a(k-a)} = \frac{1}{S_A + S_B + S_C}.
\end{aligned}
$$

Der Term $\frac{z_0}{a(k-a)}$ entspricht der Hälfte der Zielfunktion. Daher lässt sich diese auch darstellen als

$$
\frac{2}{S_A + S_B + S_C} \longrightarrow \text{ maximieren.} \tag{4.12}
$$

Da der Zähler dieses Bruches konstant ist, wird die Zielfunktion genau dann maximal, wenn die Summe $S_A + S_B + S_C$ minimal wird. Gesucht sind demnach die Werte für a, bei welchen die Summe $S_A + S_B + S_C$ einen minimalen Wert annimmt. Dabei kann a als ganzzahlig angenommen werden, wie im Folgenden gezeigt wird.
Aus (4.8) folgt, dass die Zielfunktion im Allgemeinen dargestellt werden kann als

$$
\begin{aligned}
&2 \cdot \left[\sum_{z_\ell > 0} (-1)^\ell \binom{k}{\ell} \left(\ell^2 - k\ell + \frac{z_0 k(k-1)}{z_0 k + z_1} \right) \right]^{-1} \\
&\quad = 2 \cdot \left[\sum_{z_\ell > 0} (-1)^\ell \binom{k}{\ell} \left(\ell^2 - k\ell \right) + \sum_{z_\ell > 0} (-1)^\ell \binom{k}{\ell} \frac{z_0 k(k-1)}{z_0 k + z_1} \right]^{-1} \longrightarrow \text{ maximieren.}
\end{aligned}
$$

Die exakten Summationsgrenzen werden dabei durch die Nullstellen des Polynoms B bestimmt, welche wiederum von dem Term $\frac{z_0 k(k-1)}{z_0 k + z_1}$ abhängen. Sei nun $a \leq \frac{k}{2}$ eine nichtganzzahlige Nullstelle des Polynoms B. Vergrößert (verkleinert) man a um einen kleinen Wert δ, ohne dabei eine ganze Zahl zu überschreiten (unterschreiten), dann verändert sich damit auch der Term $\frac{z_0 k(k-1)}{z_0 k + z_1}$ um einen bestimmten Wert ε. Die Summationsgrenzen bleiben allerdings bestehen, da beim Verändern von a keine ganze Zahl überschritten

(unterschritten) wurde. Somit kann sich nur die Summe

$$\sum_{z_\ell>0}(-1)^\ell\binom{k}{\ell}\left(\frac{z_0k(k-1)}{z_0k+z_1}\pm\varepsilon\right)$$

verändert haben. Falls der Zielfunktionswert dabei konstant geblieben ist, kann a bis auf die nächste ganze Zahl verschoben werden, ohne den Zielfunktionswert zu verringern oder die Summationsgrenzen zu beeinflussen. Andernfalls kann durch eine geeignete Wahl von ε der Zielfunktionswert erhöht werden. Dadurch ist es möglich ε so zu wählen, dass a ganzzahlig wird und der Zielfunktionswert erhöht wird. Die Summationsgrenzen bleiben auch hierbei bestehen. Somit kann a im Allgemeinen als ganzzahlig angenommen werden.

Da a als ganzzahlig angenommen wird, kann bei den Summationsgrenzen der Summen S_A, S_B und S_C das Runden entfallen. Für die Monotonieuntersuchungen seien die folgenden Funktionen definiert:

$$f_A(j,a) := (a-j)(k-a-j) \qquad \Longrightarrow \qquad S_A = \sum_{\substack{j=0\\ j \text{ gerade}}}^{a-1}\binom{k}{j}\cdot f_A(j,a)$$

$$f_B(j,a) := (j-a)(k-a-j) \qquad \Longrightarrow \qquad S_B = \sum_{\substack{j=a+1\\ j \text{ ungerade}}}^{k-a-1}\binom{k}{j}\cdot f_B(j,a)$$

$$f_C(j,a) := (j-a)(j+a-k) \qquad \Longrightarrow \qquad S_C = \sum_{\substack{j=k-a+1\\ j \text{ gerade}}}^{k}\binom{k}{j}\cdot f_C(j,a).$$

Wenn die Summe $S_A + S_B + S_C$ fallend in a ist, muss gelten

$$G := \sum_{\substack{j=0\\ j \text{ gerade}}}^{a-1}\binom{k}{j}\cdot f_A(j,a) + \sum_{\substack{j=a+1\\ j \text{ ungerade}}}^{k-a-1}\binom{k}{j}\cdot f_B(j,a) + \sum_{\substack{j=k-a+1\\ j \text{ gerade}}}^{k}\binom{k}{j}\cdot f_C(j,a)$$
$$- \sum_{\substack{j=0\\ j \text{ gerade}}}^{a}\binom{k}{j}\cdot f_A(j,a+1) - \sum_{\substack{j=a+2\\ j \text{ ungerade}}}^{k-a-2}\binom{k}{j}\cdot f_B(j,a+1) - \sum_{\substack{j=k-a\\ j \text{ gerade}}}^{k}\binom{k}{j}\cdot f_C(j,a+1) > 0.$$

Da sich die Summationsbereiche verändern können, sobald a um 1 erhöht wird, müssen folgende Fälle unterschieden werden:

Fall I: a, k gerade	Fall II: a ungerade, k gerade
Fall III: a gerade, k ungerade	Fall IV: a, k ungerade.

Es ist also für jeden Fall ein a zu bestimmen, für welches die Summe $S_A + S_B + S_C$ minimal wird, um den Zielfunktionswert zu maximieren. Da das Vorgehen in allen vier Fällen identisch ist, wird nur der Fall I ausführlich dargestellt. Bei den anderen Fällen werden lediglich die Resultate angegeben.

Fall I: a, k gerade:

Die Summe G kann durch Paarbildung der einzelnen Summen ausgewertet werden. Da a und k nach Annahme gerade Zahlen sind, gilt

$$\begin{aligned}
&\sum_{\substack{j=0\\ j \text{ gerade}}}^{a-1} \binom{k}{j} \cdot f_A(j,a) - \sum_{\substack{j=0\\ j \text{ gerade}}}^{a} \binom{k}{j} \cdot f_A(j,a+1) \\
&\quad = \sum_{\substack{j=0\\ j \text{ gerade}}}^{a-2} \binom{k}{j} \cdot f_A(j,a) - \sum_{\substack{j=0\\ j \text{ gerade}}}^{a} \binom{k}{j} \cdot f_A(j,a+1) \\
&\quad = \sum_{\substack{j=0\\ j \text{ gerade}}}^{a-2} \binom{k}{j} \cdot [f_A(j,a) - f_A(j,a+1)] - \binom{k}{a}(k-2a-1) \\
&\quad = -(k-2a-1) \sum_{\substack{j=0\\ j \text{ gerade}}}^{a-2} \binom{k}{j} - \binom{k}{a}(k-2a-1) \\
&\quad = -(k-2a-1) \sum_{\substack{j=0\\ j \text{ gerade}}}^{a} \binom{k}{j}.
\end{aligned}$$

Analog gelten auch

$$\begin{aligned}
&\sum_{\substack{j=a+1\\ j \text{ ungerade}}}^{k-a-1} \binom{k}{j} \cdot f_B(j,a) - \sum_{\substack{j=a+2\\ j \text{ ungerade}}}^{k-a-2} \binom{k}{j} \cdot f_B(j,a+1) \\
&\quad = \sum_{\substack{j=a+1\\ j \text{ ungerade}}}^{k-a-1} \binom{k}{j} \cdot f_B(j,a) - \sum_{\substack{j=a+3\\ j \text{ ungerade}}}^{k-a-3} \binom{k}{j} \cdot f_B(j,a+1) \\
&\quad = \binom{k}{a+1}(k-2a-1) + \binom{k}{k-a-1}(k-2a-1) \\
&\qquad + \sum_{\substack{j=a+3\\ j \text{ ungerade}}}^{k-a-3} \binom{k}{j} \cdot [f_B(j,a) - f_B(j,a+1)]
\end{aligned}$$

$$= 2\binom{k}{a+1}(k-2a-1) + (k-2a-1)\sum_{\substack{j=a+3\\ j \text{ ungerade}}}^{k-a-3}\binom{k}{j}$$

$$= (k-2a-1)\sum_{\substack{j=a+1\\ j \text{ ungerade}}}^{k-a-1}\binom{k}{j}$$

und

$$\sum_{\substack{j=k-a+1\\ j \text{ gerade}}}^{k}\binom{k}{j}\cdot f_C(j,a) - \sum_{\substack{j=k-a\\ j \text{ gerade}}}^{k}\binom{k}{j}\cdot f_C(j,a+1)$$

$$= \sum_{\substack{j=k-a+2\\ j \text{ gerade}}}^{k}\binom{k}{j}\cdot f_C(j,a) - \sum_{\substack{j=k-a\\ j \text{ gerade}}}^{k}\binom{k}{j}\cdot f_C(j,a+1)$$

$$= \sum_{\substack{j=k-a+2\\ j \text{ gerade}}}^{k}\binom{k}{j}\cdot [f_C(j,a) - f_C(j,a+1)] - \binom{k}{a}(k-2a-1)$$

$$= -(k-2a-1)\sum_{\substack{j=k-a+2\\ j \text{ gerade}}}^{k}\binom{k}{j} - \binom{k}{a}(k-2a-1)$$

$$= -(k-2a-1)\sum_{\substack{j=k-a\\ j \text{ gerade}}}^{k}\binom{k}{j}.$$

Kombiniert man diese Teilergebnisse, folgt für G

$$G = -(k-2a-1)\sum_{\substack{j=0\\ j \text{ gerade}}}^{a}\binom{k}{j} + (k-2a-1)\sum_{\substack{j=a+1\\ j \text{ ungerade}}}^{k-a-1}\binom{k}{j} - (k-2a-1)\sum_{\substack{j=k-a\\ j \text{ gerade}}}^{k}\binom{k}{j}$$

$$= (k-2a-1)\left[\sum_{\substack{j=a+1\\ j \text{ ungerade}}}^{k-a-1}\binom{k}{j} - 2\sum_{\substack{j=0\\ j \text{ gerade}}}^{a}\binom{k}{j}\right] \overset{!}{>} 0$$

Der Term $(k-2a-1)$ ist für alle $a < \frac{k-1}{2}$ positiv und streng monoton fallend in a. Die Summe über die ungeraden Binomialkoeffizienten ist für steigendes a ebenfalls fallend, da die Anzahl der Summanden reduziert wird. Hingegen ist die Summe über die geraden Binomialkoeffizienten steigend in a. Da diese Summe jedoch von der ersten subtrahiert wird, ist der gesamte Ausdruck innerhalb der Klammern fallend in a. Daher ist es ausreichend den maximalen Wert für a zu bestimmen, für den $G > 0$ gilt.

Wenn $\frac{k}{2}$ eine gerade Zahl ist, lässt sich der Term innerhalb der Klammern umformen zu

$$\begin{aligned}
&\sum_{\substack{j=a+1\\ j \text{ ungerade}}}^{k-a-1} \binom{k}{j} - 2 \sum_{\substack{j=0\\ j \text{ gerade}}}^{a} \binom{k}{j} = 2 \sum_{\substack{j=a+1\\ j \text{ ungerade}}}^{\frac{k}{2}-1} \binom{k}{j} - 2 \sum_{\substack{j=0\\ j \text{ gerade}}}^{a} \binom{k}{j} \\
&\quad = 2 \cdot \left[\sum_{\substack{j=0\\ j \text{ ungerade}}}^{\frac{k}{2}} \binom{k}{j} - \sum_{j=0}^{a} \binom{k}{j} \right] = 2 \cdot \left[\sum_{j=0}^{\frac{k}{2}} \binom{k}{j} - \sum_{\substack{j=0\\ j \text{ gerade}}}^{\frac{k}{2}} \binom{k}{j} - \sum_{j=0}^{a} \binom{k}{j} \right] \\
&\quad = 2 \cdot \left[2^{k-2} - \sum_{j=0}^{a} \binom{k}{j} \right] \qquad \text{nach Lemma 2.11 und 2.13.}
\end{aligned}$$

Somit gilt

$$G > 0 \quad \Longleftrightarrow \quad 2^{k-2} > \sum_{j=0}^{a} \binom{k}{j} \quad \wedge \quad a < \frac{k-1}{2}.$$

Aus Lemma 2.11 folgt, dass a nicht den Wert $\frac{k}{2}$ annehmen kann, da die Summe in diesem Fall größer wäre als 2^{k-2}. Um eine Abschätzung für a bestimmen zu können, für welche diese Ungleichung erfüllt ist, kann die Stirlingformel genutzt werden. In ihrer einfachsten Form lautet sie

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{\mathrm{e}} \right)^n, \tag{4.13}$$

wobei $\pi = 3.1415926535\ldots$ die Kreiszahl und $\mathrm{e} = 2.7182818284\ldots$ die Eulersche Zahl ist. Schätzt man mit Hilfe der Stirlingformel (4.13) die Binomialkoeffizienten ab, gilt für positive reelle Konstanten c, c_i

$$\begin{aligned}
&\binom{k}{\frac{k}{2}} \approx \frac{2^{k-1}}{c_1 \cdot \sqrt{k}}, \qquad \binom{k}{\frac{k}{2}-1} \approx \frac{2^{k-1}}{c_2 \cdot \sqrt{k}}, \qquad \binom{k}{\frac{k}{2}-2} \approx \frac{2^{k-1}}{c_3 \cdot \sqrt{k}}, \qquad \ldots \\
&\Longrightarrow \qquad \sum_{j=\frac{k}{2}-c\cdot\sqrt{k}}^{\frac{k}{2}} \binom{k}{j} \approx 2^{k-2}.
\end{aligned}$$

Hieraus folgt, dass $a < \frac{k}{2} - c \cdot \sqrt{k}$ gelten muss, für eine positive reelle Konstante c. Sollte $\frac{k}{2}$ ungerade sein, kann durch analoge Umformungen der Summe G die selbe Abschätzung für a hergeleitet werden. Diese Abschätzung ist allerdings ungeeignet, um Aussagen über den optimalen Zielfunktionswert ableiten zu können. Da die Stirlingformel (4.13) für kleine n jedoch ungenau ist, könnte die Ungleichung $G > 0$ für kleine k erfüllt sein. Daher werden im Folgenden Werte für k bestimmt, bei denen $G > 0$ gilt.

Nach Annahme ist k eine gerade Zahl, also gilt $k = 4m$ oder $k = 4m + 2$ für ein $m \in \mathbb{N}$. Da a ebenfalls eine natürliche Zahl ist, kann a nur die Werte $\frac{k}{2}, \frac{k}{2} - 1, \frac{k}{2} - 2, \ldots$ annehmen.
Sei $a = \frac{k}{2}$. Dann ist G

$$G = -\left[0 - 2 \sum_{\substack{j=0 \\ j \text{ gerade}}}^{\frac{k}{2}} \binom{k}{j}\right] = 2 \cdot \left(2^{k-2} + \frac{1}{2}\binom{k}{\frac{k}{2}}\right) = 2^{k-1} + \binom{k}{\frac{k}{2}} > 0.$$

Da $G > 0$ gilt, erhält man einen größeren Zielfunktionswert, wenn man anstatt der Stelle $\frac{k}{2}$ den Wert $a = \frac{k}{2} + 1$ wählt. Dann ist aber auch $k - (\frac{k}{2} + 1) = \frac{k}{2} - 1$ eine Nullstelle. Somit ist der Zielfunktionswert größer, wenn man $a = \frac{k}{2} - 1$ wählt, als wenn man $a = \frac{k}{2}$ wählen würde.
Sei $a = \frac{k}{2} - 1$. Dann ist G

$$G = 1 \cdot \left[\sum_{\substack{j=\frac{k}{2} \\ j \text{ ungerade}}}^{\frac{k}{2}} \binom{k}{j} - 2 \sum_{\substack{j=0 \\ j \text{ gerade}}}^{\frac{k}{2}-1} \binom{k}{j}\right] = \binom{k}{\frac{k}{2}} - 2^{k-1} < 0 \quad \text{für} \quad k \geq 4.$$

Da $G < 0$ ist, bewirkt eine Verschiebung der Nullstelle von $\frac{k}{2} - 1$ auf $\frac{k}{2}$ keine Erhöhung des Zielfunktionswertes.
Sei $a = \frac{k}{2} - 2$. Dann ist G

$$\begin{aligned} G &= 3\left[\sum_{\substack{j=\frac{k}{2}-1 \\ j \text{ ungerade}}}^{\frac{k}{2}+1} \binom{k}{j} - 2 \sum_{\substack{j=0 \\ j \text{ gerade}}}^{\frac{k}{2}-2} \binom{k}{j}\right] = 3\left[2\binom{k}{\frac{k}{2}-1} - 2\left(2^{k-2} - \frac{1}{2}\binom{k}{\frac{k}{2}}\right)\right] \\ &= 3\left[2\binom{k}{\frac{k}{2}-1} + \binom{k}{\frac{k}{2}} - 2^{k-1}\right] \overset{!}{>} 0. \end{aligned}$$

Diese Ungleichung ist für alle geraden k mit $2 \leq k \leq 18$ erfüllt. Da $a = \frac{k}{2} - 2$ eine gerade Zahl ist, muss k durch 4 teilbar sein. Außerdem muss $k \geq 8$ gelten, da a nicht negativ sein kann. Somit erhält man einen größeren Zielfunktionswert, wenn man $a = \frac{k}{2} - 1$ wählt und $k = 8, k = 12$ oder $k = 16$ gilt.

Sei $a = \frac{k}{2} - 3$. Dann ist G

$$G = 5\left[\sum_{\substack{j=\frac{k}{2}-2 \\ j \text{ ungerade}}}^{\frac{k}{2}+2} \binom{k}{j} - 2 \sum_{\substack{j=0 \\ j \text{ gerade}}}^{\frac{k}{2}-3} \binom{k}{j}\right] = 5\left[2\binom{k}{\frac{k}{2}-2} + \binom{k}{\frac{k}{2}} - 2\left(2^{k-2} - \binom{k}{\frac{k}{2}-1}\right)\right]$$
$$= 5\left[2\binom{k}{\frac{k}{2}-2} + 2\binom{k}{\frac{k}{2}-1} + \binom{k}{\frac{k}{2}} - 2^{k-1}\right] \overset{!}{>} 0.$$

Diese Ungleichung ist für alle geraden k mit $4 \leq k \leq 54$ erfüllt. Da $a = \frac{k}{2} - 3$ eine gerade Zahl ist, ist k gerade, aber nicht durch 4 teilbar. Außerdem muss $k \geq 10$ gelten, da a positiv sein muss. Somit erhält man einen größeren Zielfunktionswert, wenn man $a = \frac{k}{2} - 2$ wählt und k eine nicht durch 4 teilbare, gerade Zahl kleiner als 55 ist.
Sei $a = \frac{k}{2} - 4$. Dann ist G

$$G = 7\left[\sum_{\substack{j=\frac{k}{2}-3 \\ j \text{ ungerade}}}^{\frac{k}{2}+3} \binom{k}{j} - 2 \sum_{\substack{j=0 \\ j \text{ gerade}}}^{\frac{k}{2}-4} \binom{k}{j}\right]$$
$$= 7\left[2\binom{k}{\frac{k}{2}-3} + 2\binom{k}{\frac{k}{2}-1} - 2\left(2^{k-2} - \frac{1}{2}\binom{k}{\frac{k}{2}} - \binom{k}{\frac{k}{2}-2}\right)\right]$$
$$= 7\left[2\binom{k}{\frac{k}{2}-3} + 2\binom{k}{\frac{k}{2}-2} + 2\binom{k}{\frac{k}{2}-1} + \binom{k}{\frac{k}{2}} - 2^{k-1}\right] \overset{!}{>} 0.$$

Diese Ungleichung ist für alle geraden k mit $6 \leq k \leq 106$ erfüllt. Da $a = \frac{k}{2} - 4$ eine gerade Zahl ist, muss k durch 4 teilbar sein. Außerdem muss $k \geq 12$ gelten, da a positiv sein muss. Somit erhält man einen größeren Zielfunktionswert, wenn man $a = \frac{k}{2} - 3$ wählt und k eine durch 4 teilbare Zahl kleiner als 107 ist.

Für $a = \frac{k}{2} - 5$ ist $G > 0$, wenn $k \leq 176$ ist, für $a = \frac{k}{2} - 6$ muss $k \leq 264$ gelten.
Wie zu erkennen ist, steigt der Zielfunktionswert für kleine k, je näher man a an $\frac{k}{2}$ wählt. Die folgende Tabelle zeigt, welche Nullstelle einen maximalen Zielfunktionswert liefert, in Abhängigkeit des Wertes k.

Bereich für k	**optimale Nullstelle a**	**Bedingung**
$4 \leq k \leq 18$	$\frac{k}{2} - 1$	k durch 4 teilbar
$20 \leq k \leq 54$	$\frac{k}{2} - 2$	k gerade, nicht durch 4 teilbar
$56 \leq k \leq 106$	$\frac{k}{2} - 3$	k durch 4 teilbar
$108 \leq k \leq 176$	$\frac{k}{2} - 4$	k gerade, nicht durch 4 teilbar
$178 \leq k \leq 264$	$\frac{k}{2} - 5$	k durch 4 teilbar

Die Abschätzung $a < \frac{k}{2} - c \cdot \sqrt{k}$ ist demnach für kleine k zu ungenau.

In den folgenden drei Fällen lässt sich die selbe Abschätzung treffen, analog zu dem oben dargestellten Vorgehen. Um aber für kleine k auch in den anderen Fällen exakte Werte für die optimalen Nullstellen zu erhalten, werden nur die entsprechenden Bereiche für k bestimmt.

Fall II: a ungerade, k gerade:

Unter Berücksichtigung der Summationsgrenzen ist wieder die Summe G zu bestimmen, analog zum Vorgehen im Fall I. Dann folgt

$$G = (k - 2a - 1) \left[\sum_{\substack{j=a+2 \\ j \text{ ungerade}}}^{k-a-2} \binom{k}{j} - 2 \sum_{\substack{j=0 \\ j \text{ gerade}}}^{a-1} \binom{k}{j} \right] \overset{!}{>} 0.$$

Nach Annahme ist k eine gerade Zahl, also gilt $k = 4m$ oder $k = 4m + 2$ für ein $m \in \mathbb{N}$. Da a ebenfalls eine natürliche Zahl ist, kann a nur die Werte $\frac{k}{2}, \frac{k}{2} - 1, \frac{k}{2} - 2, \ldots$ annehmen.
Sei $a = \frac{k}{2}$. Dann ist G

$$G = - \left[0 - 2 \sum_{\substack{j=0 \\ j \text{ gerade}}}^{\frac{k}{2}-1} \binom{k}{j} \right] = 2^{k-1} > 0.$$

Da $G > 0$ gilt, erhält man einen größeren Zielfunktionswert, wenn man anstatt der Stelle $\frac{k}{2}$ den Wert $a = \frac{k}{2} + 1$ wählt. Dann ist aber auch $k - (\frac{k}{2} + 1) = \frac{k}{2} - 1$ eine Nullstelle. Somit ist der Zielfunktionswert größer, wenn man $a = \frac{k}{2} - 1$ wählt, als wenn man $a = \frac{k}{2}$ wählen würde.
Sei $a = \frac{k}{2} - 1$. Dann ist G

$$G = 1 \cdot \left[0 - 2 \sum_{\substack{j=0 \\ j \text{ gerade}}}^{\frac{k}{2}-2} \binom{k}{j} \right] < 0$$

Da $G < 0$ ist, bewirkt eine Verschiebung der Nullstelle von $\frac{k}{2} - 1$ auf $\frac{k}{2}$ keine Erhöhung des Zielfunktionswertes.

Sei $a = \frac{k}{2} - 2$. Dann ist G

$$G = 3\left[\sum_{\substack{j=\frac{k}{2} \\ j \text{ ungerade}}}^{\frac{k}{2}} \binom{k}{j} - 2\sum_{\substack{j=0 \\ j \text{ gerade}}}^{\frac{k}{2}-3} \binom{k}{j}\right] = 3\left[\binom{k}{\frac{k}{2}} - 2^{k-1} + 2\binom{k}{\frac{k}{2}-1}\right]$$
$$= 3\left[2\binom{k}{\frac{k}{2}-1} + \binom{k}{\frac{k}{2}} - 2^{k-1}\right] > 0.$$

Man erkennt, dass der Fall II dem Fall I entspricht, wobei die Parität von a geändert wurde. Die Werte von G sind für die selben Werte a identisch zu denen aus Fall I. Also gelten die Einschränkungen an den Wertebereich von k in diesem Fall genauso wie im Fall I. Nur die Bedingungen, ob k eine durch 4 teilbare Zahl sein muss oder nicht, wird geändert. Zusammenfassend gilt daher

Bereich für k	**optimale Nullstelle a**	**Bedingung**
$6 \leq k \leq 18$	$\frac{k}{2} - 1$	k gerade, nicht durch 4 teilbar
$20 \leq k \leq 54$	$\frac{k}{2} - 2$	k durch 4 teilbar
$56 \leq k \leq 106$	$\frac{k}{2} - 3$	k gerade, nicht durch 4 teilbar
$108 \leq k \leq 176$	$\frac{k}{2} - 4$	k durch 4 teilbar
$178 \leq k \leq 264$	$\frac{k}{2} - 5$	k gerade, nicht durch 4 teilbar.

Fall III: a gerade, k ungerade:

Unter Berücksichtigung der Summationsgrenzen ist wieder die Summe G zu bestimmen, analog zum Vorgehen im Fall I. Dann folgt

$$G = (k - 2a - 1)\left[\sum_{\substack{j=a+1 \\ j \text{ ungerade}}}^{k-a-2} \binom{k}{j} - \sum_{j=0}^{a} \binom{k}{j}\right] \overset{!}{>} 0.$$

Zu beachten gilt hierbei, dass die hintere Summe keine Einschränkungen mehr an die Parität der Laufvariablen stellt.
Nach Annahme ist k eine ungerade Zahl, also gilt $k = 4m+1$ oder $k = 4m+3$ für ein $m \in \mathbb{N}$. Da a ebenfalls eine natürliche Zahl ist, kann a nur die Werte $\frac{k-1}{2}, \frac{k-1}{2} - 1, \frac{k-1}{2} - 2, \ldots$ annehmen.
Sei $a = \frac{k-1}{2}$. Dann ist G

$$G = 0 \cdot \left[0 - \sum_{j=0}^{\frac{k-1}{2}} \binom{k}{j}\right] = 0 \cdot 2^{k-1} = 0.$$

Wenn $a = \frac{k-1}{2}$ eine Nullstelle ist, dann ist auch $k - (\frac{k-1}{2}) = \frac{k+1}{2}$ eine Nullstelle. Der Zielfunktionswert kann sich also in diesem Fall nicht ändern, da an der Lösung nichts geändert wird.
Sei $a = \frac{k-1}{2} - 1$. Dann ist G

$$G = 2 \cdot \left[\sum_{\substack{j=\frac{k-1}{2} \\ j \text{ ungerade}}}^{\frac{k-1}{2}} \binom{k}{j} - \sum_{j=0}^{\frac{k-1}{2}-1} \binom{k}{j} \right] = 2 \left[\binom{k}{\frac{k-1}{2}} - \left(2^{k-1} - \binom{k}{\frac{k-1}{2}} \right) \right]$$
$$= 4 \binom{k}{\frac{k-1}{2}} - 2^k \overset{!}{>} 0.$$

Diese Ungleichung ist für ungerade k nur dann erfüllt, wenn $k = 5$ oder $k = 7$ gilt. Für $k \geq 9$ ist $G < 0$.
Sei $a = \frac{k-1}{2} - 2$. Dann ist G

$$G = 4 \left[\sum_{\substack{j=\frac{k-3}{2} \\ j \text{ ungerade}}}^{\frac{k+1}{2}} \binom{k}{j} - \sum_{j=0}^{\frac{k-5}{2}} \binom{k}{j} \right] = 4 \left[\binom{k}{\frac{k-3}{2}} + \binom{k}{\frac{k+1}{2}} - \left(2^{k-1} - \binom{k}{\frac{k-1}{2}} - \binom{k}{\frac{k-3}{2}} \right) \right]$$
$$= 8 \binom{k}{\frac{k-3}{2}} + 8 \binom{k}{\frac{k-1}{2}} - 2^{k+1} \overset{!}{>} 0.$$

Diese Ungleichung ist für alle ungeraden k mit $5 \leq k \leq 35$ erfüllt. Da $a = \frac{k-1}{2} - 2$ eine gerade Zahl ist, muss $k = 4m + 1$ für ein $m \in \mathbb{N}$ sein. Außerdem muss $k > 7$ gelten, da a positiv sein muss. Somit erhält man einen größeren Zielfunktionswert, wenn man $a = \frac{k-1}{2} - 1$ wählt.
Sei $a = \frac{k-1}{2} - 3$. Dann ist G

$$G = 6 \cdot \left[\sum_{\substack{j=\frac{k-5}{2} \\ j \text{ ungerade}}}^{\frac{k+3}{2}} \binom{k}{j} - \sum_{j=0}^{\frac{k-7}{2}} \binom{k}{j} \right]$$
$$= 6 \left[\binom{k}{\frac{k-5}{2}} + \binom{k}{\frac{k-1}{2}} + \binom{k}{\frac{k+3}{2}} - \left(2^{k-1} - \binom{k}{\frac{k-1}{2}} - \binom{k}{\frac{k-3}{2}} - \binom{k}{\frac{k-5}{2}} \right) \right]$$
$$= 6 \left[2 \binom{k}{\frac{k-5}{2}} + 2 \binom{k}{\frac{k-3}{2}} + 2 \binom{k}{\frac{k-1}{2}} - 2^{k-1} \right] \overset{!}{>} 0.$$

Diese Ungleichung ist für alle ungeraden k mit $7 \leq k \leq 79$ erfüllt. Da $a = \frac{k-1}{2} - 3$ eine gerade Zahl ist, muss $k = 4m + 3$ für ein $m \in \mathbb{N}$ sein. Außerdem muss $k > 9$ gelten,

da a positiv sein muss. Somit erhält man einen größeren Zielfunktionswert, wenn man $a = \frac{k-1}{2} - 2$ wählt.

Analog zum Fall I ist zu erkennen, dass der Zielfunktionswert steigt, je näher man a an $\frac{k-1}{2}$ wählt. Auch hier ist somit die Abschätzung $a < \frac{k}{2} - c \cdot \sqrt{k}$ für kleine k zu ungenau. Die optimalen Nullstellen in Abhängigkeit von k sind in der folgenden Tabelle dargestellt.

Bereich für k	**optimale Nullstelle a**	**Bedingung**
$k = 7$	$\frac{k-1}{2}$	-
$9 \leq k \leq 35$	$\frac{k-1}{2} - 1$	$k = 4m + 1$ für ein $m \in \mathbb{N}$
$37 \leq k \leq 79$	$\frac{k-1}{2} - 2$	$k = 4m + 3$ für ein $m \in \mathbb{N}$
$81 \leq k \leq 139$	$\frac{k-1}{2} - 3$	$k = 4m + 1$ für ein $m \in \mathbb{N}$
$141 \leq k \leq 219$	$\frac{k-1}{2} - 4$	$k = 4m + 3$ für ein $m \in \mathbb{N}$

Fall IV: a, k ungerade:

Unter Berücksichtigung der Summationsgrenzen ist wieder die Summe G zu bestimmen, analog zum Vorgehen im Fall I. Dann folgt

$$G = (k - 2a - 1) \left[\sum_{\substack{j=a+2 \\ j \text{ ungerade}}}^{k-a-1} \binom{k}{j} - \sum_{j=0}^{a} \binom{k}{j} \right] \overset{!}{>} 0.$$

Zu beachten gilt hierbei, dass die hintere Summe keine Einschränkungen mehr an die Parität der Laufvariablen stellt.
Nach Annahme ist k eine ungerade Zahl, also gilt $k = 4m+1$ oder $k = 4m+3$ für ein $m \in \mathbb{N}$. Da a ebenfalls eine natürliche Zahl ist, kann a nur die Werte $\frac{k-1}{2}, \frac{k-1}{2} - 1, \frac{k-1}{2} - 2, \ldots$ annehmen.
Sei $a = \frac{k-1}{2}$. Dann ist G

$$G = 0 \cdot \left[0 - \sum_{j=0}^{\frac{k-1}{2}} \binom{k}{j} \right] = 0 \cdot 2^{k-1} = 0.$$

Wenn $a = \frac{k-1}{2}$ eine Nullstelle ist, dann ist auch $k - (\frac{k-1}{2}) = \frac{k+1}{2}$ eine Nullstelle. Der Zielfunktionswert kann sich also in diesem Fall nicht ändern, da an der Lösung nichts geändert wird.

Sei $a = \frac{k-1}{2} - 1$. Dann ist G

$$G = 2 \cdot \left[\sum_{\substack{j=\frac{k+1}{2} \\ j \text{ ungerade}}}^{\frac{k+1}{2}} \binom{k}{j} - \sum_{j=0}^{\frac{k-3}{2}} \binom{k}{j} \right] = 2 \left[\binom{k}{\frac{k+1}{2}} - \left(2^{k-1} - \binom{k}{\frac{k-1}{2}} \right) \right]$$
$$= 4 \binom{k}{\frac{k-1}{2}} - 2^k \overset{!}{>} 0.$$

Diese Ungleichung ist für ungerade k nur dann erfüllt, wenn $k = 5$ oder $k = 7$ gilt. Für $k \geq 9$ ist $G < 0$.
Sei $a = \frac{k-1}{2} - 2$. Dann ist G

$$G = 4 \left[\sum_{\substack{j=\frac{k-1}{2} \\ j \text{ ungerade}}}^{\frac{k+3}{2}} \binom{k}{j} - \sum_{j=0}^{\frac{k-5}{2}} \binom{k}{j} \right] = 4 \left[\binom{k}{\frac{k+3}{2}} + \binom{k}{\frac{k-1}{2}} - \left(2^{k-1} - \binom{k}{\frac{k-1}{2}} - \binom{k}{\frac{k-3}{2}} \right) \right]$$
$$= 8 \binom{k}{\frac{k-3}{2}} + 8 \binom{k}{\frac{k-1}{2}} - 2^{k+1} > 0.$$

Man erkennt, dass der Fall IV dem Fall III entspricht, wobei die Parität von a geändert wurde. Die Werte von G sind für die selben Werte a identisch zu denen aus Fall III. Also gelten die Einschränkungen an den Wertebereich von k in diesem Fall genauso wie im Fall III. Nur die Bedingungen, ob $k = 4m + 1$ oder $k = 4m + 3$ für ein $m \in \mathbb{N}$ ist, wird geändert. Zusammenfassend gilt daher für die optimalen Nullstellen

Bereich für k	**optimale Nullstelle a**	**Bedingung**
$k = 5$	$\frac{k-1}{2}$	-
$9 \leq k \leq 35$	$\frac{k-1}{2} - 1$	$k = 4m + 3$ für ein $m \in \mathbb{N}$
$37 \leq k \leq 79$	$\frac{k-1}{2} - 2$	$k = 4m + 1$ für ein $m \in \mathbb{N}$
$81 \leq k \leq 139$	$\frac{k-1}{2} - 3$	$k = 4m + 3$ für ein $m \in \mathbb{N}$
$141 \leq k \leq 219$	$\frac{k-1}{2} - 4$	$k = 4m + 1$ für ein $m \in \mathbb{N}$.

Zusammengefasst ist das Resultat dieser Monotonieuntersuchung, dass ganzzahlige Werte für a den nichtganzzahligen vorzuziehen sind und a möglichst groß gewählt werden sollte. Die Abschätzung $a < \frac{k}{2} - c \cdot \sqrt{k}$ ist dabei für kleine k zu ungenau. Für diese Werte sind die optimalen Nullstellen gegeben durch

Bereich für k	**optimale Nullstelle a**	**Bedingung**
$4 \leq k \leq 18$	$\frac{k}{2} - 1$	k gerade
$20 \leq k \leq 54$	$\frac{k}{2} - 2$	k gerade
$56 \leq k \leq 106$	$\frac{k}{2} - 3$	k gerade
$108 \leq k \leq 176$	$\frac{k}{2} - 4$	k gerade
$178 \leq k \leq 264$	$\frac{k}{2} - 5$	k gerade
$k = 5, k = 7$	$\frac{k-1}{2}$	-
$9 \leq k \leq 35$	$\frac{k-1}{2} - 1$	k ungerade
$37 \leq k \leq 79$	$\frac{k-1}{2} - 2$	k ungerade
$81 \leq k \leq 139$	$\frac{k-1}{2} - 3$	k ungerade
$141 \leq k \leq 219$	$\frac{k-1}{2} - 4$	k ungerade.

Diese Übersicht ließe sich weiter fortsetzen, jedoch wäre nur eine allgemeine Formel für die optimale Nullstelle a geeignet, um den optimalen Zielfunktionswert des Linearen Programms $L(k-2,k)_z$ allgemein bestimmen zu können. Wählt man hingegen eine feste Nullstelle, erhält man eine untere Schranke für den optimalen Zielfunktionswert. Falls diese größer ist, als die untere Schranke aus dem Fall der negativen Diskriminante (4.9), folgt daraus, dass mindestens eine Nullstelle in einer optimalen Lösung existieren muss. Im Folgenden wird solch eine Schranke für gerade und ungerade k bestimmt.

Der Fall k gerade

Aus den Monotonieuntersuchungen des vorigen Abschnitts wurde klar, dass $a = \frac{k-2}{2}$ in einer optimalen Belegung $z = (z_0, z_1, \ldots, z_k)$ gelten muss, wenn $k \leq 18$ gilt. Für $k > 18$ erhält man mit dieser Nullstelle eine untere Schranke für den optimalen Kontrast aller $(k-2,k)$-Schemata.
Mit $a = \frac{k-2}{2}$ folgt für (4.11)

$$\begin{aligned} z_\ell &= (-1)^\ell \binom{k}{\ell} z_0 \frac{(a-\ell)(k-a-\ell)}{a(k-a)} \\ &= (-1)^\ell \binom{k}{\ell} z_0 \frac{\left(\frac{k-2}{2}-\ell\right)\left(k-\frac{k-2}{2}-\ell\right)}{\left(\frac{k-2}{2}\right)\left(k-\frac{k-2}{2}\right)} \\ &= (-1)^\ell \binom{k}{\ell} z_0 \frac{(k-2\ell-2)(k-2\ell+2)}{(k-2)(k+2)}. \end{aligned} \tag{4.14}$$

Für die Zielfunktion gilt nach (4.10)

$$\frac{2}{a(k-a)} z_0 = \frac{2}{\left(\frac{k-2}{2}\right)\left(k-\frac{k-2}{2}\right)} z_0 = \frac{8}{(k-2)(k+2)} z_0. \tag{4.15}$$

Die Summe aller positiven Variablen ist damit

$$\begin{aligned} 1 &\stackrel{!}{=} \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} z_j - z_{\frac{k}{2}} && \text{für } \tfrac{k}{2} \text{ gerade, oder} \\ &\stackrel{!}{=} \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} z_j + z_{\frac{k}{2}} && \text{für } \tfrac{k}{2} \text{ ungerade.} \end{aligned}$$

In beiden Fällen wird zu der Summe der Wert

$$\frac{4}{(k+2)(k-2)}\binom{k}{\frac{k}{2}} z_0$$

addiert. Daraus folgt

$$\begin{aligned} 1 &\stackrel{!}{=} \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j} z_0 \frac{(k-2j-2)(k-2j+2)}{(k-2)(k+2)} + \frac{4}{(k+2)(k-2)}\binom{k}{\frac{k}{2}} z_0 \\ &= \frac{z_0}{(k-2)(k+2)} \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j}(k^2 - 4kj + 4j^2 - 4) + \frac{4}{(k+2)(k-2)}\binom{k}{\frac{k}{2}} z_0 \\ &= \frac{z_0}{(k-2)(k+2)} \left[(k^2-4) \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j} - 4k \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j} j + 4 \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j} j^2 \right] \\ &\qquad + \frac{4}{(k+2)(k-2)}\binom{k}{\frac{k}{2}} z_0 \\ &= \frac{z_0}{(k-2)(k+2)} \left[(k^2-4) \cdot 2^{k-1} - k^2 \cdot 2^k + k(k+1)2^{k-1} \right] + \frac{4}{(k+2)(k-2)}\binom{k}{\frac{k}{2}} z_0 \\ &\qquad \text{nach Lemma 2.10, 2.15 und 2.17} \\ &= z_0 \frac{2^{k-1}(k-4)}{(k+2)(k-2)} + \frac{4}{(k+2)(k-2)}\binom{k}{\frac{k}{2}} z_0 \end{aligned}$$

$$\Longleftrightarrow$$

$$z_0 = \frac{2(k+2)(k-2)}{2^k(k-4) + 8\binom{k}{\frac{k}{2}}}$$

und für die Zielfunktion gilt

$$\frac{8}{(k-2)(k+2)} z_0 = \frac{8}{(k-2)(k+2)} \cdot \frac{2(k+2)(k-2)}{2^k(k-4) + 8\binom{k}{\frac{k}{2}}} = \frac{16}{2^k(k-4) + 8\binom{k}{\frac{k}{2}}}. \tag{4.16}$$

Somit ist (4.16) eine untere Schranke für den Kontrast aller $(k-2,k)$-Schemata für gerade k und der optimale Zielfunktionswert für alle geraden $k \leq 18$. Für den Fall, das Polynom B hat keine Nullstelle, konnte mit (4.9) die obere Schranke $\alpha < \frac{2^{4-k}}{k}$ bestimmt werden. Verglichen mit der soeben bestimmten unteren Schranke gilt

$$\begin{aligned} & \frac{2^{4-k}}{k} < \frac{16}{2^k(k-4)+8\binom{k}{\frac{k}{2}}} \\ \iff \qquad & 4\left(2^k - 2\binom{k}{\frac{k}{2}}\right) > 0, \end{aligned}$$

womit gezeigt ist, dass für gerade k ein größerer Zielfunktionswert erreicht werden kann, wenn eine Nullstelle im Bereich $(0,k)$ vorhanden ist.

Der Fall k ungerade

Für ungerade k mit $9 \leq k \leq 35$ muss $z_{\frac{k-3}{2}} = 0$ in einer optimalen Belegung $z = (z_0, z_1, \ldots, z_k)$ gelten. Für ungerade $k > 35$ bestimmt man mit dieser Nullstelle eine untere Schranke für den optimalen Zielfunktionswert. Damit folgt für (4.11)

$$\begin{aligned} z_\ell &= (-1)^\ell \binom{k}{\ell} z_0 \frac{(a-\ell)(k-a-\ell)}{a(k-a)} \\ z_\ell &= (-1)^\ell \binom{k}{\ell} z_0 \frac{(\frac{k-3}{2}-\ell)(k-\frac{k-3}{2}-\ell)}{\frac{k-3}{2}(k-\frac{k-3}{2})} \\ &= (-1)^\ell \binom{k}{\ell} z_0 \frac{(k-2\ell-3)(k-2\ell+3)}{(k-3)(k+3)}. \end{aligned} \tag{4.17}$$

Für die Zielfunktion gilt nach (4.10)

$$\frac{2}{a(k-a)} z_0 = \frac{2}{\frac{k-3}{2}(k-\frac{k-3}{2})} z_0 = \frac{8}{(k-3)(k+3)} z_0. \tag{4.18}$$

Die Summe aller positiven Variablen ist damit

$$\begin{aligned} 1 &\overset{!}{=} \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} z_j - z_{\frac{k-1}{2}} + z_{\frac{k+1}{2}} && \text{für } \tfrac{k-1}{2} \text{ gerade, oder} \\ &\overset{!}{=} \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} z_j + z_{\frac{k-1}{2}} - z_{\frac{k+1}{2}} && \text{für } \tfrac{k-1}{2} \text{ ungerade.} \end{aligned}$$

In beiden Fällen wird zu der Summe der Wert

$$\frac{16}{(k-3)(k+3)}\binom{k}{\frac{k-1}{2}}z_0$$

addiert. Daraus folgt

$$\begin{aligned}
1 &\stackrel{!}{=} \sum_{\substack{j=0\\ j \text{ gerade}}}^{k}\binom{k}{j}z_0\frac{(k-2j-3)(k-2j+3)}{(k-3)(k+3)} + \frac{16}{(k-3)(k+3)}\binom{k}{\frac{k-1}{2}}z_0\\
&= \frac{z_0}{(k-3)(k+3)}\sum_{\substack{j=0\\ j \text{ gerade}}}^{k}\binom{k}{j}(k^2-4kj+4j^2-9) + \frac{16}{(k+3)(k-3)}\binom{k}{\frac{k-1}{2}}z_0\\
&= \frac{z_0}{(k-3)(k+3)}\left[(k^2-9)\sum_{\substack{j=0\\ j \text{ gerade}}}^{k}\binom{k}{j} - 4k\sum_{\substack{j=0\\ j \text{ gerade}}}^{k}\binom{k}{j}j + 4\sum_{\substack{j=0\\ j \text{ gerade}}}^{k}\binom{k}{j}j^2\right]\\
&\qquad + \frac{16}{(k+3)(k-3)}\binom{k}{\frac{k-1}{2}}z_0\\
&= \frac{z_0}{(k-3)(k+3)}\left[(k^2-9)\cdot 2^{k-1} - k^2\cdot 2^k + k(k+1)2^{k-1}\right] + \frac{16}{(k+3)(k-3)}\binom{k}{\frac{k-1}{2}}z_0\\
&\qquad \text{nach Lemma 2.10, 2.15 und 2.17}\\
&= z_0\frac{2^{k-1}(k-9)}{(k-3)(k+3)} + z_0\frac{16}{(k-3)(k+3)}\binom{k}{\frac{k-1}{2}}
\end{aligned}$$

$$\Longleftrightarrow$$

$$z_0 = \frac{2(k^2-9)}{32\binom{k}{\frac{k-1}{2}} + 2^k(k-9)}$$

und für die Zielfunktion gilt

$$\frac{8}{(k-3)(k+3)}z_0 = \frac{8}{(k-3)(k+3)}\cdot\frac{2(k-3)(k+3)}{32\binom{k}{\frac{k-1}{2}} + 2^k(k-9)} = \frac{16}{2^k(k-9)+32\binom{k}{\frac{k-1}{2}}}. \quad (4.19)$$

Für $k=5$ ist $(\frac{3}{8}, -\frac{5}{8}, 0, 0, \frac{5}{8}, -\frac{3}{8})$ eine optimale Belegung mit dem Zielfunktionswert $\alpha = \frac{1}{8}$. Für $k=7$ ist $(\frac{1}{8}, -\frac{7}{16}, \frac{7}{16}, 0, 0, -\frac{7}{16}, \frac{7}{16}, -\frac{1}{8})$ optimal mit dem Zielfunktionswert $\alpha = \frac{1}{48}$. Mit (4.19) wurde eine untere Schranke für den Kontrast aller $(k-2,k)$-Schemata für ungerade k bestimmt, welche optimal für ungerade k mit $9 \le k \le 35$ ist. Für den Fall, das Polynom B hat keine Nullstelle, konnte mit (4.9) die obere Schranke $\alpha < \frac{2^{4-k}}{k}$ bestimmt

werden. Verglichen mit der soeben bestimmten unteren Schranke gilt

$$\begin{aligned} & \frac{2^{4-k}}{k} < \frac{16}{2^k(k-9)+32\binom{k}{\frac{k-1}{2}}} \\ \iff \qquad & 9 \cdot 2^k - 32\binom{k}{\frac{k-1}{2}} > 0, \end{aligned}$$

womit gezeigt ist, dass für ungerade k ein größerer Zielfunktionswert erreicht werden kann, wenn eine Nullstelle im Bereich $(0, k)$ vorhanden ist. Da diese Eigenschaft auch für gerade k gilt, muss in einer optimalen Lösung für das Lineare Programm $L(k-2, k)_z$ eine Nullstelle im Bereich $(0, k)$ existieren.

4.4 Schlussbemerkungen

In diesem Kapitel wurden die optimalen Zielfunktionswerte und Variablenbelegungen für die Linearen Programme $L(k, k)_z$ und $L(k-1, k)_z$ bestimmt. Diese Ergebnisse entsprechen den Resultaten der Arbeiten [8] und [1].
Für das Lineare Programm $L(k-2, k)_z$ wurden die unteren Schranken (4.16) und (4.19) für den optimalen Zielfunktionswert bestimmt, unter Berücksichtigung der Parität von k. Wenn $k \leq 18$ gerade ist, dann ist die entsprechende Schranke optimal. Analoges gilt für ungerade k mit $9 \leq k \leq 35$. Aus diesen Schranken folgt weiter, dass mindestens eine Variable z_ℓ, mit $\ell \approx \frac{k}{2} - c \cdot \sqrt{k}$ für eine positive reelle Konstante c, des Linearen Programms $L(k-2, k)_z$ gleich 0 sein muss. Allerdings bleibt offen, welche Variable z_ℓ dieses betrifft. Daher kann der optimale Zielfunktionswert für $L(k-2, k)_z$ bisher nicht exakt angegeben werden. An dieser Stelle besteht also weiteres Forschungspotential.

Literaturverzeichnis

[1] Carlo Blundo, Paolo D'Arco, Alfredo De Santis und Douglas R. Stinson: *Contrast Optimal Threshold Visual Cryptography Schemes*. In: *SIAM Journal on Discrete Mathematics*, Band 16, Seiten 224–261. 2003.

[2] Earl D. Rainville: *Special Functions*. The Macmillan Company, 1960.

[3] George E. Andrews, Richard Askey und Ranjan Roy: *Special Functions*. Cambridge University Press, 1999.

[4] Herbert S. Wilf: *generatingfunctionality*. Academic Press, 1994.

[5] Jakob Juhnke: *Visuelle Kryptographie und* (k, n)*-Schemata*, 2011. Bachelorarbeit, Technische Universität Chemnitz.

[6] Marko Petkovšek, Herbert S. Wilf und Doron Zeilberger: $A{=}B$. Online-Ressource, URL: `http://www.math.upenn.edu/~wilf/AeqB.html`, 1997.

[7] Matthias Krause und Hans U. Simon: *Determining the Optimal Contrast for Secret Sharing Schemes in Visual Cryptography*. In: *Combinatorics, Probability and Computing*, Band 12, Seiten 285–229. 2003.

[8] Moni Naor und Adi Shamir: *Visual cryptography*. In: *Proceedings of the Conference on Advances in Cryptology – EUROCRYPT '94*, Band 950 der Reihe *Lecture Notes in Computer Science*, Seiten 1–12, 1995.

[9] Ronald L. Graham, Donald E. Knuth und Oren Patashnik: *Concrete Mathematics*. ADDISON-WESLEY, 1989.

[10] Thomas Hofmeister, Matthias Krause und Hans U. Simon: *Contrast-Optimal k out of n Secret Sharing Schemes in Visual Cryptography*. Band 240 der Reihe *Theoretical Computer Science*, Seiten 471–485, 2000.

[11] Volker Strehl: *persönliche Kommunikation*, Friedrich-Alexander-Universität Erlangen-Nürnberg, 2013.

TECHNISCHE UNIVERSITÄT CHEMNITZ

Zentrales Prüfungsamt
(Anschrift: TU Chemnitz, 09107 Chemnitz)

Selbstständigkeitserklärung*

Name: Juhnke Vorname: Jakob geb. am: 16.12.1986 Matr.-Nr.: 201229	**Bitte Ausfüllhinweise beachten:** 1. Nur Block- oder Maschinenschrift verwenden.

Ich erkläre gegenüber der Technischen Universität Chemnitz, dass ich die vorliegende Masterarbeit selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt habe.

Die vorliegende Arbeit ist frei von Plagiaten. Alle Ausführungen, die wörtlich oder inhaltlich aus anderen Schriften entnommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch bei keinem anderen Prüfer als Prüfungsleistung eingereicht und ist auch noch nicht veröffentlicht.

Datum: ..... Unterschrift: .....

* Diese Erklärung ist der eigenständig erstellten Arbeit als Anhang beizufügen.