TECHNISCHE UNIVERSITÄT CHEMNITZ

Fakultät für Informatik
Professur Theoretische Informatik und Informationssicherheit

- Bachelorarbeit -

Visuelle Kryptographie und (k, n)-Schemata

vorgelegt von

Jakob Juhnke

Chemnitz, 3. März 2011

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 bedanken, der mich auf das interessante Themengebiet der Visuellen Kryptographie aufmerksam gemacht und mich dafür begeistert hat. Ich danke für die umfassende Betreuung und Unterstützung in allen Phasen dieser Arbeit.

Mein Dank gilt ebenfalls Kai Plociennik, der mir bei mathematischen Fragen und Problemen hilfreich zur Seite stand.

Ein ganz besonderer Dank gilt Herrn Knut Odermann als Zweitgutachter.

Ich bedanke mich an dieser Stelle bei Robert Hertel, Susanne Lindner, Anna Richter und meiner Familie für ihre Geduld und Mühe bei der Korrektur meiner Arbeit.
Bei meinen Eltern möchte ich mich darüber hinaus auch dafür bedanken, dass sie mir das Studium überhaupt erst ermöglicht und mich währenddessen immer unterstützt haben.

1 Einleitung

Das allgemeine *Secret Sharing Problem* wurde erstmals 1979 von Adi Shamir in [1] betrachtet. Ziel ist dabei, ein Geheimnis so auf mehrere Personen aufzuteilen, dass nur durch die Kooperation mehrerer Personen das Geheimnis rekonstruiert werden kann. Genauer gesagt erhalten n Personen bestimmte Teilinformationen, wobei mindestens k Personen ($k \leq n$) ihre Teilinformationen zusammenlegen müssen, um die Gesamtinformation zu erhalten. Weniger als k Personen sollen allerdings nicht in der Lage sein, Rückschlüsse auf das Geheimnis ziehen zu können.
Shamir benutzt hierfür Polynome vom Grad $k-1$, wobei das Polynom selbst das Geheimnis darstellt. Jede der n Personen bekommt einen anderen Punkt des Polynoms als Teilinformation. Um das Polynom rekonstruieren zu können, müssen somit mindestens k Geheimnisträger kooperieren. Erst dann ist das Polynom eindeutig bestimmt.
Ein Nachteil solcher *Secret Sharing Verfahren* ist allerdings, dass sie sehr rechenintensiv sind, da ein Gleichungssystem mit k Gleichungen und k Variablen gelöst werden muss. Mit der *Visuellen Kryptographie* haben Naor und Shamir in [17] ein Verfahren vorgestellt, bei dem dieser Nachteil nicht auftritt. Lediglich für die Bestimmung der Teilgeheimnisse wird ein Computer benötigt.
Moni Naor und Adi Shamir stellten dieses Verfahren 1994 auf der EUROCRYPT vor (siehe [17]). Die zu schützenden Informationen sind Bilder, welche in Pixeln vorliegen. Aus einem (schwarz-weißen) Bild werden mehrere Folien generiert. Einzeln betrachtet enthält eine Folie nur Rauschen. Werden jedoch ausreichend viele Folien übereinander gelegt, ergibt sich, mit einem gewissen Kontrastverlust, wieder das Originalbild. Für die Geheimnisrekonstruktion wird also das menschliche Auge genutzt, weswegen auf Computer zunächst verzichtet werden kann. Somit kann die Visuelle Kryptographie zum Beispiel für gedruckte Medien genutzt werden.

In dieser Bachelorarbeit soll die schwarz-weiße Visuelle Kryptographie betrachtet werden. Ausgehend von einer Arbeit von Naor und Shamir [17] treten hierbei sogenannte (k, n)-Schemata auf, die auf zwei Klassen von geeigneten Matrizen basieren. Von besonderem Interesse sind hierbei (k, n)-Schemata mit (fast) optimalem Kontrast.

Zu diesen Schemata lassen sich Lineare Programme formulieren, deren optimale Lösungen Werte für den maximal erzielbaren Kontrast liefern. Untersucht werden sollen in diesem Zusammenhang speziell die beiden Fragen:

1. Sind die Lösungen des Linearen Programms eindeutig?
2. Sind bei optimalem Kontrast eines (k, n)-Schemas die entsprechenden Matrizenklassen eindeutig, auch wenn nicht totalsymmetrische Matrizen betrachtet werden?

Weiterhin sollen in der Arbeit aktuelle Forschungsergebnisse zu dieser Thematik recherchiert und analysierend dargestellt werden.

Das zweite Kapitel beschäftigt sich zunächst mit der Visuellen Kryptographie, wie sie von Naor und Shamir in [17] vorgestellt wurde. Hierbei wird die grundlegende Idee der Aufteilung eines Pixel in Subpixel erklärt und wie mit ihrer Hilfe Informationen verschlüsselt werden können. Die Darstellung der Subpixel als 0/1-Matrix bildet anschließend die Grundlage für mathematische Überlegungen und Schlussfolgerungen. Als eine der wichtigsten Kenngrößen wird der Kontrast α betrachtet, der sich aus den gewählten Matrizen ergibt. Als mathematische Abstraktion der Visuellen Kryptographie wird anschließend der Begriff des (k, n)-Schemas definiert. Außerdem werden erste Schlussfolgerungen aus dem Modell gezogen und das von Naor und Shamir angegebene $(2, n)$-Schema wird exemplarisch betrachtet.

Nachdem die Grundlagen der Visuellen Kryptographie erklärt wurden, wird im dritten Kapitel der optimale Kontrast und damit verbunden der Zusammenhang zwischen (k, n)-Schemata und Linearen Programmen, mit deren Hilfe der optimale Kontrast eines (k, n)-Schemas bestimmt werden kann, behandelt. Für $(2, n)$-Schemata wird eine Konstruktionsmöglichkeit angegeben, welche den optimalen Kontrast liefert und auf *Hadamard-Matrizen* beruht. Die hierfür notwendigen Definitionen und Lemmata werden im ersten Teil des Kapitels angegeben.
Im zweiten Teil des dritten Kapitels wird das Lineare Programm $L(k, n)$ entwickelt, welches auf einer Arbeit von Hofmeister, Krause und Simon [20] basiert. Für einige Spezialfälle wird anschließend der optimale Kontrast bestimmt. Darüber hinaus wird untersucht, ob für beliebige Werte von k und n die Lösung des Linearen Programms eindeutig ist und ob durch den optimalen Kontrast eines (k, n)-Schemas die entsprechenden Matrizenklassen eindeutig bestimmt sind.

Abschließend werden im vierten Kapitel aktuelle Entwicklungen in der Visuellen Kryptographie überblicksmäßig vorgestellt.
Ausgehend vom Modell der schwarz-weißen Visuellen Kryptographie aus Kapitel 2, wurden viele Erweiterungen und Verallgemeinerungen entwickelt. Durch die Verwendung von *General Access Structures* ist es möglich, die Mengen von Teilnehmern, welche das geheime Bild rekonstruieren können, genauer zu spezifizieren. Auf Visueller Kryptographie mit *General Access Structures* aufbauend, kann die erweiterte Visuelle Kryptographie definiert werden (EVCS genannt). Hierbei sollen bereits Bilder auf den einzelnen Folien der Teilnehmer zu erkennen sein, um die Existenz einer verschlüsselten Nachricht zu verbergen. Sollen auch beim Übereinanderlegen einiger Folien Bilder entstehen, obwohl weniger Folien vorhanden sind als für die Rekonstruktion des geheimen Bildes notwendig, kann dies durch S-EVCS erreicht werden.
Als weitere Verallgemeinerung wird die Visuelle Kryptographie für Graustufenbilder und Farbbilder vorgestellt. Die farbige Visuelle Kryptographie stellt den momentanen Forschungsschwerpunkt innerhalb der Visuellen Kryptographie dar. Allerdings sind die mathematischen Verfahren recht kompliziert und werden hier nicht näher betrachtet.

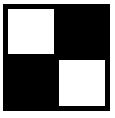
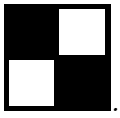
2 Einführung in die Visuelle Kryptographie

Nachfolgend wird die von Naor und Shamir 1994 vorgestellte Arbeit [17] erläutert. Ausgehend von der prinzipiellen Idee der Visuellen Kryptographie werden unterschiedliche mathematische Abstraktionen dazu genutzt, das Modell des (k, n)-Schemas zu entwickeln und zu definieren.

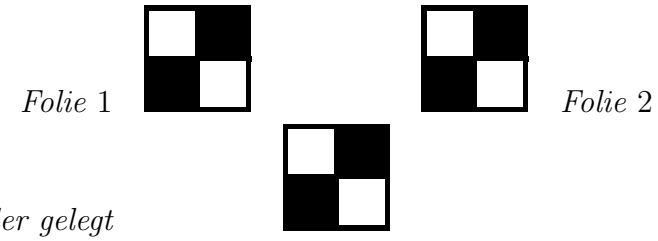
2.1 Die Idee

Die Visuelle Kryptographie ist eine spezielle Variante des *Secret Sharing Problems*. Demnach soll ein Geheimnis auf mehrere Personen aufgeteilt werden. Die zu verschlüsselnden Informationen sind hier Rastergrafiken, bei denen ein einzelnes Pixel weiß oder schwarz sein kann. Für die Aufteilung in Teilgeheimnisse werden aus dem *Originalbild* n verschiedene (transparente) Folien gebildet, so dass beim Übereinanderlegen von mindestens k Folien ein *Gesamtbild* entsteht, aus dem die vollständigen Informationen wieder extrahiert werden können. Weniger als k Folien sollen dabei keine Informationen liefern.
Da die Farbe eines einzelnen Pixels bereits eine Information darstellt, dürfen die Folien keine Pixel aus dem Originalbild enthalten. Es muss also eine geeignete Codierung für die Pixel gefunden werden, die keine Informationen über das Originalbild trägt und trotzdem eine korrekte Rekonstruktion des Geheimnisses erlaubt. Hierfür zerlegt man jedes Pixel in m gleich große Teile. Diese Teile werden als *Subpixel* bezeichnet. Ein einzelnes Subpixel kann schwarz oder weiß sein. Für eine geeignete Codierung kann jedoch nicht jede Anordnung und Färbung der Subpixel genutzt werden. Um zu verhindern, dass eine Folie eine Information liefert, müssen schwarze und weiße Pixel mit den selben Subpixel-Anordnungen codiert werden. Dadurch sind schwarze von weißen Pixeln auf einer Folie nicht unterscheidbar. Zusammengelegt mit anderen Folien ergeben sich dann die ursprünglichen Farben der Pixel.

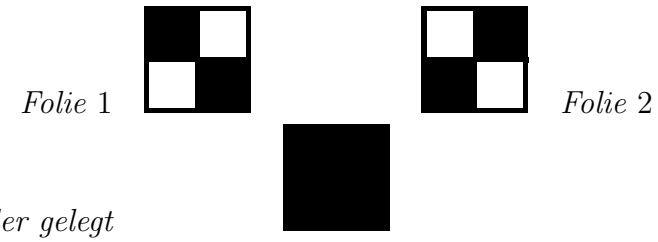
Beispiel 2.1. *Man möchte ein Originalbild auf* 2 *Folien aufteilen, wobei eine Folie keine Rückschlüsse auf die Pixel zulässt. Beide Folien übereinander gelegt sollen jedoch das geheime Bild enthalten. Dabei soll ein Pixel durch* 4 *Subpixel codiert werden. Mögliche Subpixel-Anordnungen wären dann*

 *und*  .

Ein weißes Pixel könnte man dann folgendermaßen codieren:



Bei schwarzen Pixeln muss man die Codierung anders wählen:



Wie das Beispiel zeigt, können weiße Pixel durch die gleiche Codierung auf den Folien dargestellt werden, schwarze Pixel durch verschiedene Codierungen auf den Folien. Dadurch enthalten weiße Pixel auch schwarze Subpixel. Die durch das Übereinanderlegen entstandenen Pixel werden als grau wahrgenommen, da die Subpixel sehr klein sind. An dieser Stelle tritt also ein Kontrastverlust auf. Ist dieser Kontrastverlust nicht zu groß, kann die codierte Information trotzdem erkannt werden.
Um bei der Codierung die selben Subpixel-Anordnungen für schwarze und weiße Pixel zu verwenden, muss jedes Pixel zufällig codiert werden. Das heißt, beim Codieren wird eine bestimmte Subpixel-Anordnung ausgewürfelt und für die Folien entsprechend der Pixelfarbe verwendet. Da durch das Auswürfeln jede Subpixel-Anordnung für ein Pixel gleichwahrscheinlich ist, kann ein potentieller Angreifer beim Betrachten der Subpixel-Anordnung nicht entscheiden, ob ein schwarzes oder ein weißes Pixel codiert wurde. Somit ist es nicht möglich, das Originalbild zu rekonstruieren. Erst durch k Folien sollen genügend Informationen vorliegen, um das Originalbild wiederherzustellen. Auf weniger als k Folien ist folglich nur „zufälliges Rauschen“ zu erkennen. Diese Eigenschaft wird als *perfekte Sicherheit* bezeichnet.
Werden jedoch die Subpixel schlecht gewählt, könnten Rückschlüsse möglich sein. Anordnungen, in denen beispielsweise 3 der 4 Subpixel schwarz sind, können nicht zum Codieren von weißen Pixeln genutzt werden, da sonst Informationen verloren gehen. Das menschliche Auge würde solche Codierungen als schwarze Pixel identifizieren. Deshalb kann man nur schwarze Pixel mit solchen Subpixeln codieren. Allerdings würde ein Angreifer aus dieser Codierung Informationen erhalten. Somit sind solche Auswahlen von Subpixeln nicht geeignet.
Um die Konstruktion geeigneter Codierungen sowie beweisbare Aussagen und Schlussfolgerungen zu ermöglichen, benötigt man ein mathematisches Modell für die Visuelle Kryptographie. Dieses Modell muss sowohl Bedingungen an die Codierung stellen, als

auch für die Sicherheit des Systems sorgen. Naor und Shamir haben dies in [17] durch die Definition des (k, n)-Schemas erreicht. Diese (k, n)-Schemata sollen im folgenden Abschnitt näher betrachtet werden.

2.2 Das Modell

Die Farben Schwarz und Weiß eignen sich nicht für eine mathematische Abstraktion der Visuellen Kryptographie. Deshalb werden die Farben eines Pixels durch Zahlen repräsentiert. Eine 0 stellt damit ein weißes Pixel dar, eine 1 hingegen ein schwarzes. Analog dazu werden auch die Subpixel durch 0 oder 1 dargestellt. Beim Übereinanderlegen der Folien ergibt sich somit die Farbarithmetik

weiß	weiß	weiß	‖	0	0	0
weiß	schwarz	schwarz	‖	0	1	1
schwarz	weiß	schwarz	‖	1	0	1
schwaz	schwarz	schwarz	‖	1	1	1

für die Subpixel, die der logischen *OR*-Operation $\vee$ entspricht.
Desweiteren wird die Anordnung der Subpixel auf den Folien vernachlässigt. Die Subpixel werden als ein Zeilenvektor der Länge m betrachtet. Ein solcher Vektor stellt also ein Pixel auf einer Folie dar. Wird das selbe Pixel für alle Folien betrachtet, ergibt sich eine Matrix mit n Zeilen und m Spalten mit Einträgen aus $\{0, 1\}$. Die i'te Zeile gibt demnach die Färbung der Subpixel auf der Folie i an. Daraus ergibt sich die Farbe f eines Subpixels j beim Übereinanderlegen der n Folien als

$$f_j = m_{1,j} \vee m_{2,j} \vee \ldots \vee m_{n,j}.$$

Damit lässt sich nun der Grauton definieren.

Definition 2.1:
Der Grauton g eines Pixels ist

$$g = |\{j | f_j = 1\}|.$$

Der Grauton gibt somit an, wie viele der m Subpixel eines Pixels nach dem Übereinanderlegen der n Folien schwarz sind. Für $g = 0$ bedeutet dies somit *ganz weiß*, für $g = m$ *ganz schwarz*.
Da der Grauton eines weißen Pixels nicht zu hoch sein darf, weil er sonst als schwarz interpretiert wird, eignen sich nur bestimmte Matrizen für die Codierung von weißen Pixeln. Analog gilt dies für schwarze Pixel, die jedoch einen gewissen Grauton nicht unterschreiten dürfen. Dementsprechend bilden sich zwei Klassen von Matrizen heraus. Die Klasse, mit der weiße Pixel codiert werden, wird mit C_0, die Klasse für schwarze Pixel mit C_1 bezeichnet.
Der Grenzwert, der die Grenze zwischen weißen und schwarzen Pixeln darstellt, wird

als *Schwellwert* d bezeichnet. Der Schwellwert ergibt sich aus den gewählten Matrizenklassen C_0 und C_1. Jedoch hat er keinen so hohen Einfluss auf die Erkennbarkeit des Gesamtbildes wie der *Kontrast* α. Das heißt, ist der Kontrast zu gering, sind die Grautöne von schwarzen und weißen Pixeln kaum unterscheidbar. Dies wiederum kann dazu führen, dass die codierte Information nicht mehr korrekt extrahiert werden kann.

Definition 2.2 - 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 2.3 - 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

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

Durch die Überlegungen und Abstraktionen, ausgehend von der ursprünglichen Idee der Visuellen Kryptographie, ist es nun möglich, den Begriff des (k,n)-Schemas zu definieren:

Definition 2.4 - (k,n)-Schema:
Ein (k,n)-Schema der Visuellen Kryptographie besteht aus zwei Mengen von Boolschen $n \times m$-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 2.4 folgt, dass die Anzahl der Subpixel m 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.
Aus den Kontrastbedingungen wird ersichtlich, dass ein schwarzes Pixel durch einen Grauton von mindestens d dargestellt werden muss. Weiße Pixel müssen einen geringeren Grauton haben. Je größer die Differenz zwischen den Grautönen für weiße und schwarze Pixel ist, desto deutlicher kann das menschliche Auge die Informationen aus dem Gesamtbild entnehmen. Daraus folgt, dass der Kontrast α möglichst groß sein soll.
Durch die Sicherheitsbedingung wird ausgedrückt, dass es nicht möglich ist, mit weniger als k Folien Informationen über das Originalbild zu erhalten. Auf das Modell bezogen heißt das, beim Übereinanderlegen von höchstens $k-1$ Folien sind alle Grautöne höchstens $d - \alpha \cdot m$. Würde es eine Matrix geben, für die nach Auswahl von $k-1$ Zeilen ein Grauton entsteht, der größer als $d - \alpha \cdot m$ ist, muss diese Submatrix sowohl in C_0 als auch in C_1 enthalten sein. Die Existenz einer solchen Matrix ist aber nach Definition 2.4 Eigenschaft 1 nicht möglich, da alle Submatrizen aus C_0 höchstens einen Grauton von $d - \alpha \cdot m$ haben. Somit garantiert die Sicherheitsbedingung, dass durch weniger als k Folien keine Informationen rekonstruierbar sind.

2.3 Allgemeine Schlussfolgerungen

Der Kontrast stellt die wichtigste Eigenschaft eines (k, n)-Schemas dar. Bei der konkreten Entwicklung von Schemata ist demnach ein möglichst hoher Kontrast wünschenswert. Mit Hilfe der *Linearen Programmierung* kann für feste Werte von k und n der maximal erzielbare Kontrast bestimmt werden, wie in Kapitel 3 gezeigt wird. Eine erste grobe Abschätzung des Kontrastes ist jedoch auch allein durch das bisherige Modell der Visuellen Kryptographie möglich.
Für weiße Pixel gilt nach Definition 2.4 Eigenschaft 1, dass der Grauton höchstens den Wert $d - \alpha \cdot m$ annimmt. Dieser Wert ist somit kleiner als d, also höchstens $d-1$. Daraus ergibt sich

$$d - \alpha \cdot m \leq d - 1 \implies \alpha \geq \frac{1}{m}$$

als untere Schranke.
Für alle Matrizen der Klasse C_0 gilt weiter, dass der Grauton der Disjunktion von k Zeilen mindestens 1 ist. Zusätzlich ist d höchstens gleich m, da der Schwellwert nicht größer als die maximale Anzahl an Subpixeln sein kann. Daraus ergibt sich für den

Kontrast die obere Schranke

$$d - \alpha \cdot m \geq 1 \quad \wedge \quad d \leq m \quad \Longrightarrow \quad \alpha \leq \frac{m-1}{m}.$$

Aus dem Modell folgt jedoch nicht nur eine Abschätzung des Kontrastes, sondern es lassen sich auch Aussagen über die Struktur einiger (k, n)-Schemata aufstellen.
Die folgenden Aussagen basieren auf der Arbeit [19] von Droste. Dabei werden Schemata betrachtet, bei denen die Matrixklassen C_0 und C_1 durch die Matrizen M_0 und M_1 entstehen, indem die Spalten der Matrizen permutiert werden. Das heißt, jede Matrix einer Klasse entspricht einer Spaltenpermutation der zugrunde liegenden Matrix. Die Matrizen M_0 und M_1 werden dann als *Basismatrizen* bezeichnet. Sollte eine Basismatrix mehrere identische Spalten enthalten, entsteht durch die Permutationen eine Multimenge. Diese Multimengen werden mit $\widetilde{C_0}(M_0)$ bzw. $\widetilde{C_1}(M_1)$ bezeichnet. Sind die entstandenen Klassen keine Multimengen, ist ihre Bezeichnung $C_0(M_0)$ bzw. $C_1(M_1)$. Solche (k, n)-Schemata lassen sich einfacher untersuchen, als beliebige Zusammenstellungen von Matrizen.
Die folgenden drei Lemmata werden nun zeigen, dass, falls die Sicherheitsbedingung erfüllt wird, die Multimengen $\widetilde{C_0}(M_0)$ bzw. $\widetilde{C_1}(M_1)$ in die Mengen $C_0(M_0)$ bzw. $C_1(M_1)$ überführbar sind. Sollten sich anschließend die Kardinalitäten der Mengen unterscheiden, ist die Konstruktion eines (k, n)-Schemas basierend auf $C_0(M_0)$ und $C_1(M_1)$ möglich, bei dem die neu konstruierten Mengen C_0' bzw. C_1' die gleichen Kardinalitäten aufweisen. Dabei werden stets die Parameter d, α und m beibehalten.

Lemma 2.1:
Die aus den Spaltenpermutationen von M_0 bzw. M_1 entstehenden Multimengen $\widetilde{C_0}(M_0)$ bzw. $\widetilde{C_1}(M_1)$ erfüllen genau dann die Sicherheitsbedingung aus Definition 2.4, wenn für beliebige Teilmengen $\{i_1, \ldots, i_{k-1}\} \subset \{1, \ldots, n\}$ die Submatrix $M_0(i_1, \ldots, i_{k-1})$ eine Spaltenpermutation der Submatrix $M_1(i_1, \ldots, i_{k-1})$ ist. Dabei entstehen die Submatrizen $M_0(i_1, \ldots, i_{k-1})$ bzw. $M_1(i_1, \ldots, i_{k-1})$ aus der Matrix M_0 bzw. M_1 durch Einschränkung auf die Zeilen mit den Indizes $i_1, \ldots, i_{k-1}$.

Beweis: Es werden beide Implikationen gezeigt, woraus direkt die Äquivalenz folgt.
$\Longrightarrow$: Die Klassen $\widetilde{C_0}(M_0)$ und $\widetilde{C_1}(M_1)$ erfüllen die Sicherheitsbedingung. Nach Definition 2.4 Eigenschaft 3 enthalten die beiden Multimengen $\widetilde{C_0}(i_1, \ldots, i_q)$ und $\widetilde{C_1}(i_1, \ldots, i_q)$ für jede beliebige Teilmenge $\{i_1, \ldots, i_q\} \subset \{1, \ldots, n\}$ mit $q \in \{1, \ldots, k-1\}$ die selben Matrizen mit den selben relativen Häufigkeiten. Da beide Mengen gleichmächtig sind, sind sie gleich. Somit haben die Submatrizen $M_0(i_1, \ldots, i_q)$ und $M_1(i_1, \ldots, i_q)$ die selben Spalten in beliebiger Reihenfolge. Da dies für alle Teilmengen $\{i_1, \ldots, i_q\} \subset \{1, \ldots, n\}$ mit $q \in \{1, \ldots, k-1\}$ gilt, ist es natürlich auch für $q = k-1$ gültig.

$\Longleftarrow$: Die Multimenge $\widetilde{C_0}(i_1, \ldots, i_{k-1})$ enthält alle Matrizen, die durch Spaltenpermutationen aus $M_0(i_1, \ldots, i_{k-1})$ entstehen. Gleiches gilt für $\widetilde{C_1}(i_1, \ldots, i_{k-1})$ in Bezug auf $M_1(i_1, \ldots, i_{k-1})$. Weiterhin ist bekannt, dass $M_0(i_1, \ldots, i_{k-1})$ und $M_1(i_1, \ldots, i_{k-1})$ für alle Teilmengen $\{i_1, \ldots, i_{k-1}\} \subset \{1, \ldots, n\}$ die selben Spalten in beliebiger Reihenfolge enthalten. Daraus folgt, dass auch die Submatrizen $M_0(j_1, \ldots, j_\ell)$ und $M_1(j_1, \ldots, j_\ell)$, mit $\{j_1, \ldots, j_\ell\} \subset \{i_1, \ldots, i_{k-1}\}$ und $\ell < k-1$, die selben Spalten in beliebiger Reihenfolge enthalten. Hieraus folgt wiederum die Gleichheit der Multimengen $\widetilde{C_0}(i_1, \ldots, i_q)$ und $\widetilde{C_1}(i_1, \ldots, i_q)$, mit $\{i_1, \ldots, i_q\} \subset \{1, \ldots, n\}$ und $q \in \{1, \ldots, k-1\}$, was die Erfüllung der Sicherheitsbedingung impliziert. □

Lemma 2.2:
Für alle Matrizen $M_0, M_1 \in \{0,1\}^{n \times m}$ bilden die Klassen $C_0(M_0)$ und $C_1(M_1)$ genau dann ein (k,n)-Schema $C = (C_0, C_1)$ mit Schwellwert d, Kontrast α und m Subpixeln, wenn die Klassen $\widetilde{C_0}(M_0)$ und $\widetilde{C_1}(M_1)$ ein (k,n)-Schema $\widetilde{C} = (\widetilde{C_0}, \widetilde{C_1})$ mit den selben Parametern d, α und m bilden.

Beweis: Die Mengen $C_0(M_0)$ und $\widetilde{C_0}(M_0)$ bzw. $C_1(M_1)$ und $\widetilde{C_1}(M_1)$ enthalten die selben Matrizen, lediglich in unterschiedlichen Anzahlen. Da sich die Matrizen selbst nicht unterscheiden, sind die Parameter α, d und m bei beiden Klassen gleich. Somit ist lediglich zu zeigen, dass $C_0(M_0)$ und $C_1(M_1)$ genau dann die Sicherheitsbedingung erfüllen, wenn $\widetilde{C_0}(M_0)$ und $\widetilde{C_1}(M_1)$ die Sicherheitsbedingung erfüllen.

Sei r die Anzahl verschiedener Spalten aus M_0 und s die Anzahl verschiedener Spalten aus M_1. Weiter sei $m_{0,i}$ die Anzahl des Auftretens der Spalte i in M_0 und $m_{1,j}$ die Anzahl des Auftretens der Spalte j in M_1.
Es gibt genau $m_{0,1}! \cdot \ldots \cdot m_{0,r}!$ verschiedene Spaltenpermutationen von M_0, welche die selbe Matrix erzeugen bzw. $m_{1,1}! \cdot \ldots \cdot m_{1,s}!$ für M_1. Demnach muss

$$|C_0(M_0)| = \frac{m!}{m_{0,1}! \cdot \ldots \cdot m_{0,r}!}$$

und

$$|C_1(M_1)| = \frac{m!}{m_{1,1}! \cdot \ldots \cdot m_{1,s}!}$$

gelten.
Sei n_0 die Anzahl des Vorkommens einer beliebigen Matrix aus $C_0(\ell_1, \ldots, \ell_q)$ und n_1 die Anzahl des Vorkommens der gleichen Matrix in $C_1(\ell_1, \ldots, \ell_q)$ mit $\{\ell_1, \ldots, \ell_q\} \subset \{1, \ldots, n\}$ und $q \in \{1, \ldots, k-1\}$. Dann ist die relative Häufigkeit der Matrix in $C_0(\ell_1, \ldots, \ell_q)$ gleich

$$\frac{n_0}{\frac{m!}{m_{0,1}! \cdot \ldots \cdot m_{0,r}!}}$$

und in $C_1(\ell_1, \ldots, \ell_q)$ gleich

$$\frac{n_1}{\frac{m!}{m_{1,1}! \cdot \ldots \cdot m_{1,s}!}}.$$

Sei $\widetilde{n_0}$ die Anzahl des Vorkommens dieser Matrix in $\widetilde{C_0}(\ell_1, \ldots, \ell_q)$ und $\widetilde{n_1}$ die Anzahl des Vorkommens der Matrix in $\widetilde{C_1}(\ell_1, \ldots, \ell_q)$. Dann gilt

$$\widetilde{n_0} = n_0 \cdot m_{0,1}! \cdot \ldots \cdot m_{0,r}!$$

und

$$\widetilde{n_1} = n_1 \cdot m_{1,1}! \cdot \ldots \cdot m_{1,s}!.$$

Zusammen erhält man

$$\begin{aligned}
&\frac{\widetilde{n_0}}{|\widetilde{C_0}(M_0)|} = \frac{\widetilde{n_1}}{|\widetilde{C_1}(M_1)|} \\
\iff &\frac{n_0 \cdot m_{0,1}! \cdot \ldots \cdot m_{0,r}!}{m!} = \frac{n_1 \cdot m_{1,1}! \cdot \ldots \cdot m_{1,s}!}{m!} \\
\iff &\frac{n_0}{\frac{m!}{m_{0,1}! \cdot \ldots \cdot m_{0,r}!}} = \frac{n_1}{\frac{m!}{m_{1,1}! \cdot \ldots \cdot m_{1,s}!}} \\
\iff &\frac{n_0}{|C_0(M_0)|} = \frac{n_1}{|C_1(M_1)|},
\end{aligned}$$

was bedeutet, dass die betrachtete Matrix in $\widetilde{C_0}(\ell_1, \ldots, \ell_q)$ und $\widetilde{C_1}(\ell_1, \ldots, \ell_q)$ genau dann die selbe relative Häufigkeit hat, wenn sie in $C_0(\ell_1, \ldots, \ell_q)$ und $C_1(\ell_1, \ldots, \ell_q)$ die selbe relative Häufigkeit hat. Da dies für alle Matrizen gilt, die durch die Auswahl von $q \in \{1, \ldots, k-1\}$ beliebigen Zeilen entstehen, erfüllen $C_0(M_0)$ und $C_1(M_1)$ genau dann die Sicherheitsbedingung, wenn $\widetilde{C_0}(M_0)$ und $\widetilde{C_1}(M_1)$ die Sicherheitsbedingung erfüllen. □

Durch Lemma 2.2 ist es nun möglich, die Klassen $\widetilde{C_0}(M_0)$ und $\widetilde{C_1}(M_1)$ durch die Klassen $C_0(M_0)$ und $C_1(M_1)$ zu ersetzen. Das (k, n)-Schema bleibt mit seinen Parametern erhalten. Somit können $C_0(M_0)$ und $C_1(M_1)$ als Mengen betrachtet werden, die paarweise verschiedene Matrizen enthalten.

Lemma 2.3:
Aus einem (k, n)-Schema $C = (C_0, C_1)$ mit Schwellwert d, Kontrast α und m Subpixeln lässt sich ein (k, n)-Schema $C' = (C'_0, C'_1)$ mit den selben Parametern d, α und m konstruieren, so dass C'_0 und C'_1 gleichmächtig sind.

Beweis: Sei r das kleinste gemeinsame Vielfache von $|C_0|$ und $|C_1|$. Dann lassen sich die zwei Matrizenklassen C'_0 und C'_1 konstruieren durch

$$C'_0 = \left\{ \text{jede Matrix aus } C_0 \text{ genau } \frac{r}{|C_0|} \text{ mal} \right\}$$

und

$$C_1' = \left\{\text{jede Matrix aus } C_1 \text{ genau } \frac{r}{|C_1|} \text{ mal}\right\}.$$

Somit haben beide Klassen die selbe Mächtigkeit, denn es gilt

$$|C_0'| = |C_0| \cdot \frac{r}{|C_0|} = r \quad \text{und} \quad |C_1'| = |C_1| \cdot \frac{r}{|C_1|} = r.$$

Da die Matrizen ohne Veränderungen beibehalten wurden, sind die Parameter d, α und m ebenfalls unverändert. Damit C_0' und C_1' auch ein gültiges (k, n)-Schema darstellen, muss noch die Sicherheitsbedingung erfüllt werden.
Sei $\{i_1, \ldots, i_q\} \subset \{1, \ldots, n\}$ eine beliebige Teilmenge mit $q \in \{1, \ldots, k-1\}$, n_0 die Anzahl des Vorkommens einer beliebigen Submatrix aus $C_0(i_1, \ldots, i_q)$ und n_1 die Anzahl des Vorkommens der selben Submatrix in $C_1(i_1, \ldots, i_q)$. Analog dazu werden n_0' und n_1' festgelegt. Für die relative Häufigkeit der betrachteten Submatrix in C_0' und C_1' ergibt sich dann

$$\frac{n_0'}{|C_0'|} = \frac{n_0 \cdot \frac{r}{|C_0|}}{|C_0| \cdot \frac{r}{|C_0|}} = \frac{n_0}{|C_0|}$$

und

$$\frac{n_1'}{|C_1'|} = \frac{n_1 \cdot \frac{r}{|C_1|}}{|C_1| \cdot \frac{r}{|C_1|}} = \frac{n_1}{|C_1|}.$$

Da C_0 und C_1 die Sicherheitsbedingung erfüllen, gilt

$$\frac{n_0'}{|C_0'|} = \frac{n_0 \cdot \frac{r}{|C_0|}}{|C_0| \cdot \frac{r}{|C_0|}} = \frac{n_0}{|C_0|} = \frac{n_1}{|C_1|} = \frac{n_1 \cdot \frac{r}{|C_1|}}{|C_1| \cdot \frac{r}{|C_1|}} = \frac{n_1'}{|C_1'|}.$$

Demnach erfüllen C_0' und C_1' ebenfalls die Sicherheitsbedingung. □

2.4 Ein Beispiel nach Naor und Shamir

In ihrer Arbeit [17] haben Naor und Shamir nicht nur die mathematischen Grundlagen für die Visuelle Kryptographie definiert, vielmehr haben sie auch erste Konstruktionen von (k, n)-Schemata angegeben. Im Folgenden soll das $(2, n)$-Schema vorgestellt werden.

Konstruktion eines $(2, n)$-Schemas

Die Matrizenklassen
$C_0 = \{$alle Matrizen, die aus Spaltenpermutationen der Matrix M_0 entstehen$\}$ und
$C_1 = \{$alle Matrizen, die aus Spaltenpermutationen der Matrix M_1 entstehen$\}$, wobei

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

gilt, definieren ein $(2, n)$-Schema mit den Parametern $n = m, d = 2$ und $\alpha = \frac{1}{m}$.
Die Klasse C_0 enthält alle 0/1-Matrizen der Größe $n \times m$, die genau eine Spalte bestehend aus n Einsen enthalten. Alle anderen Spalten bestehen nur aus Nullen. Die Klasse C_1 hingegen enthält alle 0/1-Matrizen der Größe $n \times m$, bei der in jeder Spalte und jeder Zeile genau eine Eins vorkommt.
Um nachzuweisen, dass diese Konstruktion ein gültiges $(2, n)$-Schema ist, müssen die drei Bedingungen der Definition 2.4 gezeigt werden.

Nachweis der Kontrasteigenschaften:

Durch die komponentenweise Disjunktion zweier beliebiger Zeilen v, w einer Matrix M aus C_0 hat der Ergebnisvektor ein Hamming-Gewicht von 1. Es gilt also $H(v \vee w) = 1$ mit $v \neq w, M \in C_0$.
Wird die selbe Operation auf einer Matrix aus C_1 ausgeführt, liefert dies ein Hamming-Gewicht von 2.
Angewandt auf die Kontrasteigenschaften muss also $1 \leq d - \alpha \cdot m$ und $2 \geq d$ gelten. Daraus folgt, dass $d = 2$ ist. Für $1 = d - \alpha \cdot m$ folgt für den Kontrast $\alpha = \frac{1}{m}$. Die Kontrasteigenschaften sind also für $d = 2$ und $\alpha = \frac{1}{m}$ erfüllt.

Nachweis der Sicherheitsbedingung:

Da hier $k = 2$ gilt, müssen nur die relativen Häufigkeiten einer festen Zeile i, also einer $1 \times m$-Matrix, betrachtet werden. Da die beiden Klassen C_0 und C_1 durch Spaltenpermutationen einer Ausgangsmatrix gebildet wurden, kann Lemma 2.2 angewandt werden. Somit kann davon ausgegangen werden, dass alle Matrizen in C_0 bzw. C_1 paarweise verschieden sind. Für ein beliebiges i kommt die i'te Zeile einer beliebigen Matrix genau einmal in C_0 vor. Somit liegt ihre relative Häufigkeit bei $\frac{1}{n}$, da C_0 genau n verschiedene Elemente enthält. Die selbe Zeile kommt in C_1 hingegen $(n-1)!$ mal vor. Da C_1 genau $n!$ verschiedene Elemente enthält, ergibt sich für die betrachtete Zeile i auch hier eine relative Häufigkeit von $\frac{(n-1)!}{n!} = \frac{1}{n}$. Da die relativen Häufigkeiten für beliebige Zeilen aus Matrizen beider Klassen identisch sind, ist die Sicherheitsbedingung erfüllt.

Somit ist gezeigt, dass die angegebene Konstruktion ein gültiges $(2, n)$-Schema ist. Für große Werte für n ist dieses Schema jedoch ungeeignet, da der Kontrast sehr klein ist. Mit anderen Matrizenklassen lassen sich jedoch $(2, n)$-Schemata konstruieren, die einen höheren Kontrast garantieren. Diese werden im folgenden Kapitel betrachtet.
Naor und Shamir haben in [17] desweiteren ein $(3, 3)$-Schema angegeben, auf dessen Basis ein allgemeines (k, k)-Schema definiert wird. Auch für ein allgemeines (k, n)-Schema geben sie eine Lösung an, jedoch sollen diese Schemata hier nicht näher betrachtet werden.

3 Optimaler Kontrast und Lineare Programmierung

Ein (k, n)-Schema soll einen möglichst hohen Kontrast haben. Dazu ist es wichtig zu wissen, wie groß der maximal erzielbare, auch *optimale*, Kontrast ist. Natürlich möchte man dann auch die Matrizenklassen kennen, mit denen der optimale Kontrast erreichbar ist.
Hofmeister, Krause und Simon haben diese Fragen in [20] untersucht. Im Folgenden sollen ihre Ergebnisse dargestellt werden. Dabei wird der optimale Kontrast für $(2, n)$-Schemata allgemein bestimmt. Im Anschluss wird gezeigt, wie kontrastoptimale $(2, n)$-Schemata konstruiert werden können. Abschließend wird ein Zusammenhang zwischen (k, n)-Schemata und Linearen Programmen aufgezeigt, mit denen der optimale Kontrast berechnet werden kann.

3.1 Der optimale Kontrast aller $(2, n)$-Schemata

Für die allgemeine Herleitung des optimalen Kontrastes für $(2, n)$-Schemata werden einige Begriffe und Lemmata benötigt, die im folgenden Abschnitt angegeben werden.

Definition 3.1 - Hamming-Abstand:
Seien $v = (v_1, \ldots, v_n) \in \{0, 1\}^n$ und $w = (w_1, \ldots, w_n) \in \{0, 1\}^n, n \in \mathbb{N}$, zwei Vektoren. Dann heißt

$$d(v, w) := |\{i | v_i \neq w_i\}|$$

Hamming-Abstand von v und w (Anzahl an Stellen, an denen sich v und w unterscheiden).

Der Hamming-Abstand stellt somit eine Verallgemeinerung des Hamming-Gewichts dar. Wird der Hamming-Abstand der Vektoren $v \in \{0, 1\}^n$ und $O = (0, \ldots, 0)$ bestimmt, entspricht dies gerade dem Hamming-Gewicht von v, also $H(v) = d(v, O)$. Desweiteren besitzt der Hamming-Abstand die Eigenschaft der Symmetrie, also $d(v, w) = d(w, v)$ für alle $v, w \in \{0, 1\}^n$.

Lemma 3.1:
Seien $v, w \in \{0,1\}^n, n \in \mathbb{N}$, zwei beliebige Vektoren. Dann gilt

$$d(v,w) = (H(v \vee w) - H(v)) + (H(v \vee w) - H(w)) = 2 \cdot H(v \vee w) - (H(v) + H(w)).$$

Beweis: Da durch die Veroderung von v und w ein Vektor entsteht, der höchstens noch mehr Einsen enthält als v bzw. w, gilt offenbar $H(v \vee w) \geq H(v)$ bzw. $H(v \vee w) \geq H(w)$. Durch $H(v \vee w) - H(v)$ wird somit die Hamming-Distanz $d(v \vee w, v)$ bestimmt. Analog gilt dies für w.
Unterscheiden sich v und $v \vee w$ an einer Stelle, ist dies nur möglich, wenn v an dieser Stelle eine 0 hat, $v \vee w$ hingegen eine 1, da eine 1 in v auch eine 1 in $v \vee w$ bedingt. Das wiederum impliziert, dass w an dieser Stelle eine 1 hat. Somit unterscheiden sich v und w ebenfalls an dieser Stelle. Diese Argumentation ist auch für w und $v \vee w$ durchführbar. Unterscheiden sich v und w an einer Stelle nicht, gibt es auch keinen Unterschied zwischen v und $v \vee w$ bzw. w und $v \vee w$. Daraus folgt, dass alle die Hamming-Distanz beeinflussenden Stellen verschieden sind. Daher können die Hamming-Distanzen $d(v \vee w, v)$ und $d(v \vee w, w)$ addiert werden und ergeben die Distanz zwischen v und w. Es gilt also

$$d(v,w) = d(v \vee w, v) + d(v \vee w, w) = (H(v \vee w) - H(v)) + (H(v \vee w) - H(w)),$$

was zu beweisen war. □

Notation:
Für eine Matrix M bezeichnet im Folgenden die Schreibweise $\boldsymbol{v \in M}$ die Auswahl einer Zeile v aus einer Matrix M.

Definition 3.2 - Abstand einer Matrix:
Sei M eine $n \times m$-Matrix mit Einträgen aus $\{0,1\}$. Dann heißt

$$d(M) := \min_{\substack{v,w \in M \\ v \neq w}} \{d(v,w)\}$$

Abstand der Matrix M.

Es werden also alle Hamming-Abstände zweier verschiedener Zeilen der Matrix M betrachtet und der kleinste Wert stellt den Abstand der Matrix M dar. Da sich zwei Zeilen in höchstens m Stellen unterscheiden können, gilt $0 \leq d(M) \leq m$.

Definition 3.3 - Kontrast einer Matrix:
Sei M eine $n \times m$-Matrix mit Einträgen aus $\{0,1\}$. Dann heißt

$$\alpha(M) := \frac{1}{m} \cdot \left(\min_{\substack{v,w \in M \\ v \neq w}} H(v \vee w) - \max_{v \in M} H(v) \right)$$

Kontrast der Matrix M.

Sowohl $H(v \vee w)$ als auch $H(v)$ sind Zahlen aus $\{0, \ldots, m\}$. Daher ist $\alpha(M)$ also eine rationale Zahl mit dem Wertebereich des offenen Intervalls $[-1, 1)$.

Definition 3.4 - balancierte Matrix:
Eine $n \times m$-Matrix M mit Einträgen aus $\{0, 1\}$ heißt *balanciert*, wenn für alle Zeilen v, w aus M gilt $H(v) = H(w)$ (alle Zeilen haben die selbe Anzahl an Einsen).

Lemma 3.2:
Sei M eine $n \times m$-Matrix mit Einträgen aus $\{0, 1\}$. Dann gilt

$$\alpha(M) \leq \frac{d(M)}{2m}$$

mit Gleichheit für balancierte Matrizen M.

Beweis: Seien v, w, v^*, w^* Zeilen der Matrix M. Für v^* und w^* gelte dabei im Besonderen: $d(v^*, w^*) = d(M)$ und ohne Einschränkung $H(v^*) \leq H(w^*)$.
Daraus folgt, dass $H(v^*) + H(w^*) \leq 2 \cdot H(w^*)$ ist. Mit der aus Lemma 3.1 gezeigten Beziehung $d(v, w) = 2 \cdot H(v \vee w) - (H(v) + H(w))$ gilt somit

$$d(M) = d(v^*, w^*) \geq 2 \cdot (H(v^* \vee w^*) - H(w^*)). \tag{3.1}$$

Der Kontrast lässt sich durch

$$\begin{aligned}
\alpha(M) &= \frac{1}{m} \cdot \left(\min_{\substack{v,w \in M \\ v \neq w}} H(v \vee w) - \max_{v \in M} H(v) \right) \\
&\leq \frac{1}{m} \cdot (H(v^* \vee w^*) - H(w^*)) && (3.2) \\
&\leq \frac{1}{m} \cdot \frac{d(M)}{2} = \frac{d(M)}{2m} && (3.3)
\end{aligned}$$

nach oben abschätzen. Die Abschätzung (3.2) gilt, da $H(v^* \vee w^*)$ höchstens größer ist, als das minimale Hamming-Gewicht zweier veroderter Matrizenzeilen und $H(w^*)$ nicht größer sein kann als das maximale Hamming-Gewicht einer Zeile der Matrix M. Durch Einsetzen von (3.1) in (3.2) erhält man (3.3).

In balancierten Matrizen M hat jede Zeile nach Definition dieselbe Anzahl an Einsen. Das Hamming-Gewicht zweier veroderter Zeilen wird daher genau dann minimal, wenn zwei Zeilen miteinander verodert werden, die minimalen Abstand haben, also

$$\min_{\substack{v,w \in M \\ v \neq w}} H(v \vee w) = H(v^* \vee w^*) \text{ mit } d(v^*, w^*) = d(M).$$

Für den Kontrast gilt daher

$$\begin{aligned}\alpha(M) &= \frac{1}{m} \cdot \left(\min_{\substack{v,w \in M \\ v \neq w}} H(v \vee w) - \max_{v \in M} H(v) \right) \\ &= \frac{1}{m} \cdot (H(v^* \vee w^*) - H(w^*)) \\ &= \frac{1}{m} \cdot \frac{d(M)}{2} = \frac{d(M)}{2m}\end{aligned}$$

für balancierte Matrizen. □

An dieser Stelle sei darauf hingewiesen, dass es auch nicht-balancierte Matrizen geben kann, für die $\alpha(M) = \frac{d(M)}{2m}$ gelten kann, wie folgendes Beispiel zeigt:

Beispiel 3.1.
Sei

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

Da die ersten beiden Zeilen jeweils 2 *Einsen haben, die dritte Zeile hingegen nur eine* 1*, ist die Matrix* M *offensichtlich nicht balanciert. Der Kontrast nach Definition 3.3 ist*

$$\alpha(M) = \frac{1}{4}(3 - 2) = \frac{1}{4},$$

da gilt

$$m = 4, \qquad \min_{\substack{v,w \in M \\ v \neq w}} H(v \vee w) = 3 \qquad \textit{und} \qquad \max_{v \in M}(M) = 2.$$

Außerdem ist

$$\frac{d(M)}{2m} = \frac{2}{2 \cdot 4} = \frac{1}{4}$$

und somit

$$\alpha(M) = \frac{d(M)}{2m},$$

obwohl M *nicht balanciert ist.*

Lemma 3.3:
Sei $C = (C_0, C_1)$ ein $(2, n)$-Schema mit m Subpixeln. Dann gilt

$$\alpha(C) \leq \min_{M \in C_1} \frac{d(M)}{2m}.$$

Beweis: Wird die Definition 3.3 des Kontrastes einer Matrix auf $(2,n)$-Schemata erweitert, erhält man

$$\begin{aligned}\alpha(C) &= \frac{1}{m} \cdot \left(\min_{M \in C_1} \min_{\substack{v,w \in M \\ v \neq w}} H(v \vee w) - \max_{M \in C_0} \max_{\substack{v,w \in M \\ v \neq w}} H(v \vee w) \right) \\ &\leq \frac{1}{m} \cdot \left(\min_{M \in C_1} \min_{\substack{v,w \in M \\ v \neq w}} H(v \vee w) - \max_{M \in C_0} \max_{v \in M} H(v) \right). \end{aligned} \tag{3.4}$$

Aus der Sicherheitsbedingung eines $(2,n)$-Schemas folgt

$$\max_{M \in C_0} \max_{v \in M} H(v) = \max_{M \in C_1} \max_{v \in M} H(v).$$

Eingesetzt in (3.4) folgt damit

$$\begin{aligned}\alpha(C) &\leq \frac{1}{m} \cdot \left(\min_{M \in C_1} \min_{\substack{v,w \in M \\ v \neq w}} H(v \vee w) - \max_{M \in C_1} \max_{v \in M} H(v) \right) \\ &\leq \frac{1}{m} \cdot \min_{M \in C_1} \left(\min_{\substack{v,w \in M \\ v \neq w}} H(v \vee w) - \max_{v \in M} H(v) \right) \\ &= \min_{M \in C_1} \alpha(M) \qquad (3.5) \\ &\leq \min_{M \in C_1} \frac{d(M)}{2m}. \qquad (3.6)\end{aligned}$$

Die Gleichheit bei (3.5) folgt aus der Definition 3.3 des Kontrastes, die Abschätzung (3.6) aus Lemma 3.2. □

Lemma 3.4:
Für alle balancierten Matrizen M der Größe $n \times m$ mit Einträgen aus $\{0,1\}$ lässt sich ein $(2,n)$-Schema $C(M)$ konstruieren, welches den Kontrast $\alpha(C) = \frac{d(M)}{2m}$ hat.

Beweis: Der Kontrast $\alpha(M)$ einer balancierten Matrix ist nach Lemma 3.2 gleich $\frac{d(M)}{2m}$. Mit $z_1, \ldots, z_n$ seien die Zeilenvektoren der Matrix M bezeichnet, also

$$M = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}.$$

Das $(2,n)$-Schema $C = C(M) = (C_0, C_1)$ basierend auf der Matrix M wird folgendermaßen konstruiert:

Für $i = 1, \ldots, n$ wird die Matrix M_i, die n Kopien des Zeilenvektors z_i übereinander enthält, in C_0 eingefügt:

$$C_0 = \left\{ \begin{pmatrix} z_1 \\ \vdots \\ z_1 \end{pmatrix}, \ldots, \begin{pmatrix} z_n \\ \vdots \\ z_n \end{pmatrix} \right\}.$$

Für $i = 1, \ldots, n$ wird die Matrix $\pi^i(M)$, die durch i-fache zyklische Zeilenrotationen entsteht, in C_1 eingefügt:

$$C_1 = \left\{ \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{pmatrix}, \begin{pmatrix} z_n \\ z_1 \\ \vdots \\ z_{n-1} \end{pmatrix}, \ldots, \begin{pmatrix} z_2 \\ \vdots \\ z_n \\ z_1 \end{pmatrix} \right\}.$$

Nun ist zu zeigen, dass dieses Schema den Kontrast $\alpha(C) = \frac{d(M)}{2m}$ hat und die Sicherheitsbedingung erfüllt.
Nach Definition 2.4 gilt für den Kontrast

$$\alpha(C) = \frac{1}{m} \cdot \left(\underbrace{\min_{\pi^i(M) \in C_1} \min_{\substack{v,w \in \pi^i(M) \\ v \neq w}} H(v \vee w)}_{A} - \underbrace{\max_{M_i \in C_0} \max_{\substack{v,w \in M_i \\ v \neq w}} H(v \vee w)}_{B} \right).$$

Aus der Konstruktion von C_0 und C_1 folgt

$$\begin{aligned} A &= \min_{\substack{v,w \in M \\ v \neq w}} H(v \vee w) \\ B &= \max_{v \in M} H(v). \end{aligned}$$

Daher ergibt sich für den Kontrast

$$\begin{aligned} \alpha(C) &= \frac{1}{m} \cdot \left(\min_{\substack{v,w \in M \\ v \neq w}} H(v \vee w) - \max_{v \in M} H(v) \right) \\ &= \alpha(M) \\ &= \frac{d(M)}{2m}. \end{aligned}$$

Sicherheitsbedingung: Wir wählen eine beliebige Zeile $i \in \{1, \ldots, n\}$ aus allen Matrizen von C_0 bzw. C_1. Dadurch erhalten wir jeden Vektor $z_j, j = 1, \ldots, n$, als Submatrix jeweils genau einmal. Es treten also die selben Submatrizen mit den selben Häufigkeiten in C_0 und C_1 auf. Somit ist die Sicherheitsbedingung des $(2, n)$-Schemas erfüllt. □

Lemma 3.5:
Sei $G = (V, E)$ ein bipartiter Graph. Dann existieren höchstens $\frac{|V|^2}{4}$ Kanten in G.

Beweis: Da G bipartit ist, kann die Knotenmenge V in zwei disjunkte Teilmengen V_1 und V_2 aufgeteilt werden, so dass keine Kante des Graphen zwischen zwei Knoten einer Teilmenge verläuft, wobei $V = V_1 \cup V_2$ gilt. Sei $|V| = n$ und $|V_1| = k$. Dann gilt $|V_2| = (n-k)$. Da keine Kanten innerhalb einer Teilmenge verlaufen, existieren höchstens $k(n-k)$ Kanten in G. Um dies für festes n zu maximieren, wird die erste Ableitung nach k gleich 0 gesetzt:

$$\begin{aligned} & (k(n-k))' = (kn - k^2)' = -2k + n \\ \Longrightarrow \quad & -2k + n = 0 \\ \Longleftrightarrow \quad & -2k = -n \\ \Longleftrightarrow \quad & k = \frac{-n}{-2} = \frac{n}{2}. \end{aligned}$$

Da die zweite Ableitung nach k gleich $-2 < 0$ ist, liegt ein Maximum an der Stelle $k = \frac{n}{2}$ vor. Somit hat ein bipartiter Graph auf n Knoten höchstens $\frac{n}{2}(n - \frac{n}{2}) = \frac{n^2}{4}$ Kanten.
Für eine ungerade Knotenanzahl n gilt

$$\lceil \tfrac{n}{2} \rceil (n - \lceil \tfrac{n}{2} \rceil) = \lfloor \tfrac{n}{2} \rfloor (n - \lfloor \tfrac{n}{2} \rfloor) = \lceil \tfrac{n}{2} \rceil \cdot \lfloor \tfrac{n}{2} \rfloor \leq \tfrac{n}{2}(n - \tfrac{n}{2}) = \tfrac{n^2}{4}$$

und somit gilt für alle bipartiten Graphen auf n Knoten $|E| \leq \frac{n^2}{4}$. □

Lemma 3.6 (Plotkin-Schranke):
Sei M eine $n \times m$-Matrix mit Einträgen aus $\{0, 1\}$. Dann gilt

$$d(M) \leq \frac{n}{2(n-1)} \cdot m.$$

Beweis: Wir erstellen aus der Matrix M einen Multigraphen $G = (V, E)$ mit $n = |V|$ Knoten, bei dem jeder Knoten eine Zeile der Matrix repräsentiert. Wenn Knoten v die Zeile s repräsentiert und Knoten w die Zeile t, dann verlaufen $d(s, t)$ Kanten zwischen v und w. Zwischen zwei beliebigen Knoten verlaufen somit mindestens $d(M)$ Kanten. Jeder Kante wird eine Farbe $i \in \{1, \ldots, m\}$ zugewiesen, wenn $s_i \neq t_i$ gilt, also ein Unterschied in der i'ten Spalte der Zeilen s und t vorliegt.
Im gesamten Graphen verlaufen $|E| \geq \binom{n}{2} \cdot d(M)$ Kanten, da für jedes Knotenpaar mindestens $d(M)$ Kanten existieren.
Jeder Kante in G wurde durch die Konstruktion genau eine Farbe zugewiesen. Da $i \in \{1, \ldots, m\}$ gilt, muss es eine Farbe geben, in der mindestens $\binom{n}{2} \cdot \frac{d(M)}{m}$ Kanten gefärbt sind. Für den Graphen $G_i = (V, E_i)$, der aus allen Knoten und den mit der Farbe i

gefärbten Kanten besteht, lassen sich nun zwei Knotenmengen definieren:

$$V_1 = \{v \in V | s_i = 0, \text{ wobei } s \text{ die durch } v \text{ repräsentierte Zeile der Matrix ist}\}$$
$$V_2 = \{v \in V | s_i = 1, \text{ wobei } s \text{ die durch } v \text{ repräsentierte Zeile der Matrix ist}\}.$$

Offensichtlich sind beide Knotenmengen disjunkt und es gilt $V_1 \cup V_2 = V$. Werden zwei Knoten aus der selben Teilmenge V_1 bzw. V_2 betrachtet, so ist der Eintrag der entsprechenden Matrizenzeilen an der Position i identisch, also verläuft keine Kante zwischen diesen Knoten in G_i. Somit ist G_i ein bipartiter Graph.
Durch die Wahl von i und Lemma 3.5 folgt

$$\binom{n}{2} \cdot \frac{d(M)}{m} \leq |E_i| \leq \frac{n^2}{4} \Longrightarrow d(M) \leq \frac{n^2}{4} \cdot \binom{n}{2}^{-1} \cdot m = \frac{n}{2(n-1)} \cdot m,$$

was zu beweisen war. □

Satz 3.1:
Sei $C = (C_0, C_1)$ ein $(2, n)$-Schema mit m Subpixeln. Dann gilt

$$\alpha(C) \leq \frac{n}{4(n-1)}.$$

Beweis: Aus Lemma 3.3 und der Plotkin-Schranke Lemma 3.6 folgt

$$\begin{aligned}\alpha(C) &\leq \min_{M \in C_1} \frac{d(M)}{2m} \\ &\leq \frac{n}{2(n-1)} \cdot m \cdot \frac{1}{2m} \\ &= \frac{n}{4(n-1)}.\end{aligned}$$

□

Wir kennen nun den maximalen Kontrast eines $(2, n)$-Schemas und wissen, dass dieser mit Hilfe von balancierten Matrizen erreichbar ist. Im folgenden Abschnitt soll daher gezeigt werden, wie $(2, n)$-Schemata mit optimalem Kontrast für $n = 2^\ell$, $\ell \in \mathbb{N}$, konstruiert werden können.

3.1.1 Kontrastoptimale $(2, n)$-Schemata mit Hadamard-Matrizen

Nach Lemma 3.4 erhalten wir ein $(2, n)$-Schema mit optimalem Kontrast, wenn für eine balancierte Matrix der Quotient $\frac{d(M)}{2m}$ maximal wird. Sogenannte *Hadamard-Matrizen* erfüllen diese Bedingung, was in diesem Abschnitt gezeigt werden soll.

Definition 3.5 - Hadamard-Matrix:
Die rekursiv gebildeten, quadratischen Matrizen $H_n \in \{0,1\}^{n\times n}$ mit $n = 2^\ell$ und $\ell \in \mathbb{N} \cup \{0\}$ der Form $H_1 = (1)$ und

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & \overline{H_n} \end{pmatrix}$$

werden als *Hadamard-Matrizen* bezeichnet. Die Matrix $\overline{H_n}$ ergibt sich dabei aus H_n durch die Invertierung aller Nullen und Einsen.

Die ersten vier nach dieser Vorschrift gebildeten Matrizen sind demnach

$$H_1 = (1)$$

$$H_2 = \begin{pmatrix} H_1 & H_1 \\ H_1 & \overline{H_1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$H_4 = \begin{pmatrix} H_2 & H_2 \\ H_2 & \overline{H_2} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$H_8 = \begin{pmatrix} H_4 & H_4 \\ H_4 & \overline{H_4} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Durch die besondere Struktur der Hadamard-Matrizen ergeben sich spezielle Eigenschaften, die für die Konstruktion von optimalen $(2, n)$-Schemata hilfreich sind.

Lemma 3.7:
Sei $n = 2^\ell$ und $\ell \in \mathbb{N} \cup \{0\}$. Dann besteht sowohl die erste Zeile, als auch die erste Spalte einer Hadamard-Matrix H_n nur aus Einsen.

Beweis: Diese Tatsache folgt direkt aus der Konstruktion der Hadamard-Matrizen. □

Lemma 3.8:
Sei $n = 2^\ell$ und $\ell \in \mathbb{N}$. Dann hat, mit Ausnahme der ersten Spalte und ersten Zeile, jede Zeile und jede Spalte ein Hamming-Gewicht von $\frac{n}{2}$.

Beweis: Induktion über ℓ:
Induktionsanfang:

$$\ell = 1 \Longrightarrow n = 2 \Longrightarrow H_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Die zweite Zeile hat ein Hamming-Gewicht von 1, ebenso die zweite Spalte. Daher gilt $1 = \frac{n}{2} = \frac{2}{2}$.
Induktionsvoraussetzung:
Für $n = 2^\ell$ hat H_n in jeder Spalte und jeder Zeile ein Hamming-Gewicht von $\frac{n}{2}$, bis auf die erste Zeile und erste Spalte.
Induktionsschritt: $\ell \longrightarrow \ell + 1$
Die Zeilen und Spalten $2, \ldots, n$ der Matrix H_{2n} haben nach Induktionsvoraussetzung ein Hamming-Gewicht von $2 \cdot \frac{n}{2} = n = \frac{2n}{2}$.
Die Zeilen und Spalten $2, \ldots, n$ der Matrix $\overline{H_n}$ haben ebenfalls ein Hamming-Gewicht von $\frac{n}{2}$, da die $\frac{n}{2}$ Nullen von H_n nun Einsen sind und umgekehrt. Somit haben auch die Zeilen und Spalten $n+2, \ldots, 2n$ der Matrix H_{2n} ein Hamming-Gewicht von $2 \cdot \frac{n}{2} = n = \frac{2n}{2}$.
Die Zeile und Spalte $n + 1$ besteht an den ersten n Positionen nur aus Einsen, gefolgt von n Nullen. Somit ergibt sich auch hier ein Hamming-Gewicht von n. Insgesamt haben also alle Zeilen und Spalten, mit Ausnahme der jeweils ersten, ein Hamming-Gewicht von $n = \frac{2n}{2}$. □

Lemma 3.9:
Sei $n = 2^\ell$ und $\ell \in \mathbb{N}$. Dann ist der Hamming-Abstand zweier beliebiger verschiedener Zeilen von H_n gleich $\frac{n}{2}$ und somit gilt $d(H_n) = \frac{n}{2}$.

Beweis: Induktion über ℓ:
Induktionsanfang:

$$\ell = 1 \Longrightarrow n = 2 \Longrightarrow H_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Der Hamming-Abstand der beiden Zeilen aus H_2 ist $1 = \frac{2}{2} = \frac{n}{2}$.
Induktionsvoraussetzung: Für $n = 2^\ell$ gilt $d(H_n) = \frac{n}{2}$.
Induktionsschritt: $\ell \longrightarrow \ell + 1$
Es ist jetzt zu zeigen, dass $d(H_{2n}) = n$ gilt. Die Definition 3.5 der Hadamard-Matrizen legt die Struktur von H_{2n} fest als

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & \overline{H_n} \end{pmatrix} = \begin{pmatrix} M_1 \\ M_2 \end{pmatrix}.$$

Zunächst betrachten wir zwei beliebige verschiedene Zeilen v und w aus der Submatrix M_1. Nach Induktionsvoraussetzung haben beide Zeilen einen Hamming-Abstand von n und somit gilt hier

$$d(M_1) = d(H_n) + d(H_n) = 2 \cdot \frac{n}{2} = n.$$

Zwei beliebige verschiedene Zeilen der Matrix $\overline{H_n}$ haben wie die Matrix H_n einen Hamming-Abstand von $\frac{n}{2}$, da sich der Hamming-Abstand beim Invertieren der Matrixeinträge nicht ändert. Somit gilt auch für zwei beliebige verschiedene Zeilen v und w aus M_2

$$d(M_2) = d(H_n) + d(\overline{H_n}) = 2 \cdot \frac{n}{2} = n.$$

Wird v aus M_1 und w aus M_2 gewählt, sind zwei Fälle zu unterscheiden. Mit v_1 bzw. w_1 seien die ersten n Stellen der Vektoren v bzw. w bezeichnet, mit v_2 bzw. w_2 die entsprechend letzten n Stellen.
Für den Fall $(v_1, v_2) = (w_1, \overline{w_2})$ ergibt sich der Hamming-Abstand

$$d(v, w) = d(v_1, w_1) + d(v_2, w_2) = 0 + n = n.$$

Für jede andere Auswahl von v und w gilt

$$d(v, w) = d(v_1, w_1) + d(v_2, w_2) = \frac{n}{2} + \left(n - \frac{n}{2}\right) = n,$$

denn die beiden Zeilen v_2 und $\overline{w_2}$ kommen in H_n mit einem Hamming-Abstand von $\frac{n}{2}$ vor. □

Somit verfügen wir über alle nötigen Informationen, um mit Hilfe von Hadamard-Matrizen kontrastoptimale $(2, n)$-Schemata zu bilden.

Lemma 3.10:
Für $n = 2^\ell, \ell \in \mathbb{N}$, lassen sich $n \times (2n-2)$-Matrizen M_n konstruieren, für die $d(M_n) = n$ gilt.

Beweis: Wir definieren A_n als die Matrix, die aus H_n durch Streichen der ersten Spalte entsteht. Dadurch hat A_n eine Größe von $n \times (n-1)$. Desweiteren definieren wir $M_n = \left[A_n \overline{A_n}\right]$ als die $n \times (2n-2)$-Matrix, die durch Konkatenation von A_n und $\overline{A_n}$ entsteht. Die Matrix A_n ist konstruktionsbedingt eine balancierte Matrix und hat einen Hamming-Abstand von $\frac{n}{2}$, da das Löschen der ersten Zeile aus H_n keinen Einfluss auf den Hamming-Abstand hat. Daraus folgt, dass der Hamming-Abstand der Matrix M_n gleich n ist und somit gilt $d(M_n) = n$. □

Lemma 3.11:
Mit Hilfe der Matrix M_n aus Lemma 3.10 lässt sich ein $(2, n)$-Schema $C(M_n) = (C_0, C_1)$ konstruieren, welches den Kontrast $\alpha = \frac{n}{4 \cdot (n-1)}$ und $(2n-2)$ Subpixel hat.

Beweis: Durch Anwendung von Lemma 3.4 auf die Matrix M_n lässt sich ein $(2, n)$-Schema konstruieren, da M_n balanciert ist. Dieses Schema hat den Kontrast

$$\alpha = \frac{d(M_n)}{2m} = \frac{n}{2 \cdot (2n-2)} = \frac{n}{4 \cdot (n-1)}.$$

Dies ist nach Satz 3.1 optimal. □

Für $k = 2$ ist nun ein Verfahren bekannt, mit dem kontrastoptimale Schemata konstruiert werden können. Jedoch wissen wir noch nicht, wie Schemata konstruiert werden können, bei denen $k \geq 3$ gilt. Hofmeister, Krause und Simon konnten in [20] zeigen, dass Lineare Programme verwendet werden können, um den optimalen Kontrast eines (k, n)-Schemas zu bestimmen, unabhängig davon, wie k und n gewählt werden. Deshalb sollen im folgenden Abschnitt die Linearen Programme genauer betrachtet werden.

3.2 Der optimale Kontrast für allgemeine (k, n)-Schemata

Hofmeister, Krause und Simon benutzen in [20] Lineare Programme für die Berechnung des optimalen Kontrastes eines (k, n)-Schemas. Der Zielfunktionswert stellt den optimalen Kontrast dar. Darüber hinaus lassen sich durch die Linearen Programme (k, n)-Schemata mit den entsprechenden Kontrastwerten konstruieren. Dabei wird jedoch eine besondere Form von Matrizen genutzt, die *total symmetrischen Matrizen*.
Nachfolgend werden die benötigten Definitionen und Lemmata betrachtet, welche die Voraussetzung für die Anwendbarkeit der Linearen Programme bilden. Anschließend wird gezeigt, wie (k, n)-Schemata entsprechend der Linearen Programme konstruiert werden können.

3.2.1 Grundlagen zur Herleitung der Linearen Programme

Definition 3.6:
Sei M eine $n \times m$-Matrix mit Einträgen aus $\{0, 1\}$. Dann heißt M *total symmetrisch*, falls für je zwei Spaltenvektoren $v, w \in \{0, 1\}^n$ mit $H(v) = H(w)$ die Häufigkeiten $f(v)$ und $f(w)$ in M identisch sind. Man definiert $f_j := f(v)$ mit $H(v) = j$, für $j \in \{0, \ldots, n\}$.

Anders ausgedrückt heißt das, eine beliebige Spalte v mit $H(v) = j$ Einsen muss genau so häufig in M vorkommen, wie alle anderen Spalten mit j Einsen, um eine total symmetrische Matrix zu bilden. Somit müssen alle möglichen Vektoren mit j Einsen in M vorhanden sein, sobald eine Spalte j Einsen hat. Damit ergibt sich für die Anzahl Spalten mit genau j Einsen nun $f_j \cdot \binom{n}{j}$. Insgesamt hat die Matrix also $m = \sum_{j=0}^{n} f_j \cdot \binom{n}{j}$ Spalten.

Lemma 3.12:
Sei M eine $n \times m$-Matrix mit Einträgen aus $\{0,1\}$ und $\sigma_j, j = 1, \ldots, n!$, die $n!$ Zeilenpermutationen der Matrix M. Dann ist die $n \times (n! \cdot m)$-Matrix

$$M^* = [\sigma_1(M)|\sigma_2(M)|\ldots|\sigma_{n!}(M)]$$

total symmetrisch. Dabei entsteht die Matrix M^* durch Nebeneinanderlegen der Matrizen, die durch die Zeilenpermutationen σ_j bestimmt werden.

Beweis: Ein Spaltenvektor v aus der Matrix M mit i Einsen bleibt genau dann erhalten, wenn eine Zeilenpermutation nur die Zeilen untereinander permutiert, welche nur Einsen bzw. Nullen enthalten. Von den $n!$ Zeilenpermutationen erzeugen $i! \cdot (n-i)!$ wieder den Vektor v. Jede andere Möglichkeit die Einsen anzuordnen tritt auch $i! \cdot (n-i)!$ mal auf. Somit erzeugt man durch die Zeilenpermutationen jeden Spaltenvektor mit i Einsen gleich häufig. Deshalb ist die konstruierte Matrix M^* total symmetrisch. □

Satz 3.2:
Sei M eine total symmetrische $n \times m$-Matrix mit Einträgen aus $\{0,1\}$. Desweiteren seien I und I' mit $I, I' \subseteq \{1, \ldots, n\}, |I| = |I'| = \ell$, zwei Mengen von Zeilenindizes der Kardinalität ℓ. Dann gilt:

1. Die durch I bestimmte $\ell \times m$-Submatrix M_I ist total symmetrisch.
2. Der Parameter $C_j^\ell(M)$ gibt an, wie oft ein fester Spaltenvektor der Länge ℓ mit j Einsen in der Submatrix M_I vorkommt, also $C_j^\ell(M) := f_j(M_I) = f_j(M_{I'})$ für jedes $j = 0, \ldots, \ell$.
3. Es gilt $C_j^\ell(M) = \sum_{i=j}^{n-\ell+j} f_i(M) \cdot \binom{n-\ell}{i-j}$.

Beweis: Wir wählen ein beliebiges j, $0 \leq j \leq \ell$, und einen beliebigen Spaltenvektor v aus $\{0,1\}$ der Länge ℓ mit Hamming-Gewicht $H(v) = j$. Die absolute Häufigkeit des Vektors v in M_I entspricht der Häufigkeit der Vektoren $\hat{v}$ in M der Länge n, die v an den Indizes aus der Menge I enthalten. Für das Hamming-Gewicht von v gilt $j = H(v) \leq H(\hat{v}) \leq n - (\ell - j)$.
Betrachten wir alle Vektoren $\hat{v}$ mit $H(\hat{v}) = j + i$ und $i = 0, \ldots, n - \ell$, dann gibt es $\binom{n-\ell}{i}$ Vektoren $\hat{v}$ für jedes i, die v enthalten. Dies entspricht genau der Anzahl an Möglichkeiten die i Einsen auf $n - \ell$ Positionen zu verteilen. Da M total symmetrisch ist und $H(\hat{v}) = j + i$ ist, kommt $\hat{v}$ genau $f_{j+i}(M)$ mal in M vor. Somit ist die absolute Häufigkeit von v

$$H_v(M_I) = \sum_{i=0}^{n-\ell} f_{j+i}(M) \cdot \binom{n-\ell}{i} = \sum_{i=j}^{n-\ell+j} f_i(M) \cdot \binom{n-\ell}{i-j}.$$

Da lediglich das Hamming-Gewicht von v und nicht v selbst Einfluss auf die Häufigkeit hat, treten alle Vektoren mit Hamming-Gewicht $H(v) = j$ gleich häufig in M_I auf. Somit ist die Matrix M_I total symmetrisch und Teil 1 des Lemmas ist gezeigt.
Die konkret gewählte Zeilenindexmenge I spielt keine Rolle, sondern nur deren Kardinalität. Somit gilt für $|I| = |I'| = \ell$ die Gleichung $f_j(M_I) = f_j(M_{I'})$. Bezeichnen wir nun diesen Wert mit $C_j^\ell(M)$, ist dieser gleich $\sum_{i=j}^{n-\ell+j} f_i(M) \cdot \binom{n-\ell}{i-j}$, wie oben bereits gezeigt wurde. Somit sind auch die Teile 2 und 3 des Lemmas gezeigt. □

Lemma 3.13:
Sei M eine total symmetrische $n \times m$-Matrix. Dann ist M balanciert.

Beweis: Zu zeigen ist, dass alle Zeilen der Matrix M die selbe Anzahl an Einsen haben, also das Hamming-Gewicht aller Zeilen identisch ist. Dazu wählen wir zwei beliebige Zeilen v_i und v_j und definieren zwei Zeilenindexmengen $I := \{i\}$ und $I' := \{j\}$. Betrachten wir nun v_i bzw. v_j als $1 \times m$-Matrizen, so sind sie nach Definition 3.6 total symmetrisch und es gilt $f_1(M_I) = H(v_i)$ und $f_1(M_{I'}) = H(v_j)$. Nach Satz 3.2 gilt $f_1(M_I) = f_1(M_{I'})$ und somit $H(v_i) = H(v_j)$. Somit haben zwei beliebige Zeilen das gleiche Hamming-Gewicht. □

Lemma 3.14:
Sei M eine total symmetrische $n \times m$-Matrix und $\ell \in \{1, \ldots, n\}$. Dann gilt

$$m = \sum_{j=0}^{\ell} C_j^\ell(M) \cdot \binom{\ell}{j}.$$

Beweis: Jede Spalte einer $\ell \times m$-Submatrix von M hat ein Hamming-Gewicht zwischen 0 und ℓ. Insgesamt lassen sich somit $\binom{\ell}{j}$ Vektoren der Länge ℓ mit Hamming-Gewicht j angeben. Nach Satz 3.2 ist jeder dieser Vektoren $C_j^\ell(M)$ mal in der $\ell \times m$-Submatrix vorhanden. Somit gibt es $C_j^\ell(M) \cdot \binom{\ell}{j}$ Vektoren mit Hamming-Gewicht j in der Submatrix. Aufsummiert über alle Werte von j ergibt das genau die Anzahl an Spalten, da jede Spalte ein Hamming-Gewicht zwischen 0 und ℓ haben muss. Also gilt

$$m = \sum_{j=0}^{\ell} C_j^\ell(M) \cdot \binom{\ell}{j},$$

wie behauptet. □

Definition 3.7:
Ein (k, n)-Schema $C = (C_0, C_1)$ heißt *total symmetrisches Schema*, wenn es durch Spaltenpermutationen zweier total symmetrischer Matrizen M_0 und M_1 gebildet wurde, also

$$C_0 = \{\text{alle Matrizen, die aus Spaltenpermutationen der Matrix } M_0 \text{ entstehen}\}$$
$$C_1 = \{\text{alle Matrizen, die aus Spaltenpermutationen der Matrix } M_1 \text{ entstehen}\}.$$

Lemma 3.15:
Zu jedem (k, n)-Schema $C = (C_0, C_1)$ mit Kontrast $\alpha(C) > 0$ gibt es ein total symmetrisches (k, n)-Schema $C' = (C'_0, C'_1)$ mit Kontrast $\alpha(C') \geq \alpha(C)$.

Beweis: Zuerst konstruieren wir das total symmetrische Schema C' aus dem Schema C und bestimmen anschließend den Kontrast des neuen Schemas.
Wegen Lemma 2.3 können wir davon ausgehen, dass C_0 und C_1 gleich mächtig sind. Es gilt demnach $|C_0| = |C_1| = r$. Somit lassen sich die Matrizen der Klassen C_0 und C_1 aufzählen als $C_0 = \{M_{0,1}, \ldots, M_{0,r}\}$ und $C_1 = \{M_{1,1}, \ldots, M_{1,r}\}$. Aus diesen Matrizen konstruieren wir nun zwei neue Matrizen $N_0 = [M_{0,1}M_{0,2} \ldots M_{0,r}]$ und $N_1 = [M_{1,1}M_{1,2} \ldots M_{1,r}]$ der Größe $n \times (r \cdot m)$ durch Hintereinanderreihung. Dabei ist m die Anzahl Subpixel des Schemas C. Aus diesen beiden Matrizen können nun nach Lemma 3.12 zwei total symmetrische Matrizen gebildet werden, welche mit N_0^* und N_1^* bezeichnet werden und eine Größe von $n \times (n! \cdot r \cdot m)$ haben. Die Matrizen N_0^* und N_1^* können nach Definition 3.7 dazu genutzt werden, ein total symmetrisches Schema zu konstruieren. Somit ergibt sich

$$C'_0 = \{\text{alle Matrizen, die aus Spaltenpermutationen der Matrix } N_0^* \text{ entstehen}\}$$
$$C'_1 = \{\text{alle Matrizen, die aus Spaltenpermutationen der Matrix } N_1^* \text{ entstehen}\}.$$

Jetzt muss noch der Kontrast des Schemas C' bestimmt werden.
Für das Schema C wissen wir nach Definition 2.4, dass die Kontrastbedingung erfüllt ist. Daher gilt $H(v) \leq d - \alpha(C) \cdot m$ für einen Vektor v, der aus der Veroderung von k paarweise verschiedenen Zeilen einer Matrix $M_{0,i}$ entsteht. Dabei ist d der Schwellwert des Schemas C und $i \in \{1, \ldots, r\}$. Für Matrizen aus C_1 gilt $H(v) \geq d$.
Werden aus der Matrix N_0 (bzw. N_1) k paarweise verschiedene Zeilen zum Vektor w verodert, folgt $H(w) \leq r \cdot (d - \alpha(C) \cdot m)$ (bzw. $H(w) \geq r \cdot d$).
Analog folgt für k paarweise verschiedene zum Vektor u veroderte Zeilen der Matrix N_0^* (bzw. N_1^*) $H(u) \leq n! \cdot r \cdot (d - \alpha(C) \cdot m)$ (bzw. $H(u) \geq n! \cdot r \cdot d$). Für den Kontrast des Schemas C' folgt somit

$$\alpha(C') \geq \frac{n! \cdot r \cdot (d - (d - \alpha(C) \cdot m))}{n! \cdot r \cdot m} = \frac{d - (d - \alpha(C) \cdot m)}{m} = \alpha(C).$$

□

Lemma 3.16:
Für zwei total symmetrische Matrizen $M_0, M_1 \in \{0,1\}^{n\times m}$, mit $n, m \geq 2$, und $k \in \{2,\ldots,n\}$ kann man genau dann ein (k,n)-Schema $C = (C_0, C_1)$ mit dem Kontrast

$$\alpha := \frac{C_0^k(M_0) - C_0^k(M_1)}{m} > 0$$

konstruieren, wenn gilt

$$C_j^{k-1}(M_0) = C_j^{k-1}(M_1) \qquad \forall j = 0,\ldots,k-1. \tag{3.7}$$

Beweis:
$\Longrightarrow$: Da $C = (C_0, C_1)$ ein gültiges (k,n)-Schema mit Kontrast α ist, wird die Sicherheitsbedingung aus Definition 2.4 erfüllt. Nach Lemma 2.1 haben die Submatrizen, die durch Auswahl von $(k-1)$ beliebigen Zeilen aus M_0 und M_1 entstehen, dieselben Spalten mit den selben Häufigkeiten. Demnach gilt

$$C_j^{k-1}(M_0) = C_j^{k-1}(M_1) \qquad \forall j = 0,\ldots,k-1.$$

$\Longleftarrow$: Nach Satz 3.2 gibt der Parameter $C_j^{k-1}(M_0)$ bzw. $C_j^{k-1}(M_1)$ an, wie oft ein fester Vektor der Länge $(k-1)$ mit j Einsen als Spalte in einer Submatrix vorkommt, die durch Auswahl von $(k-1)$ beliebigen Zeilen aus M_0 bzw. M_1 entsteht. Wenn $C_j^{k-1}(M_0) = C_j^{k-1}(M_1)$ für alle $j = 0,\ldots,k-1$ gilt, dann haben die Submatrizen, welche durch die Auswahl von $(k-1)$ beliebigen Zeilen aus M_0 bzw. M_1 entstehen, die selben Spalten mit den selben Häufigkeiten. Lediglich die Reihenfolge der Spalten innerhalb der Submatrizen ist unterschiedlich. Somit ist nach Lemma 2.1 die Sicherheitsbedingung erfüllt.
Der Parameter $C_0^k(M_0)$ bzw. $C_0^k(M_1)$ gibt an, wie oft der Nullvektor als Spalte in einer Submatrix vorhanden ist, die durch Auswahl von k beliebigen Zeilen aus M_0 bzw. M_1 entsteht. Die Anzahl an Spalten der Submatrizen mit mindestens einer Eins ist somit gleich $m - C_0^k(M_0)$ bzw. $m - C_0^k(M_1)$. Aus Definition 2.4 folgt damit

$$\begin{aligned}\alpha &= \frac{\big(m - C_0^k(M_1)\big) - \big(m - C_0^k(M_0)\big)}{m} \\ &= \frac{C_0^k(M_0) - C_0^k(M_1)}{m}.\end{aligned}$$

□

Durch Lemma 3.15 reicht es also aus, sich bei der Suche nach Schemata mit optimalem Kontrast auf total symmetrische Schemata zu beschränken. Genauer gesagt reicht es aus, total symmetrische Matrizen zu finden, welche den optimalen Kontrast liefern. Dazu können Lineare Programme genutzt werden.

3.2.2 Herleitung der Linearen Programme

Um mit Hilfe von total symmetrischen Matrizen gültige (k,n)-Schemata zu finden, müssen die drei Bedingungen in Definition 2.4 eines (k,n)-Schemas erfüllt werden. Die im letzten Abschnitt gezeigten Lemmata helfen dabei, das Problem mathematisch zu beschreiben.
Zum einen soll der Kontrast möglichst groß sein. Wir haben in Lemma 3.16 gezeigt, dass der Kontrast bei total symmetrischen Schemata gleich $\frac{C_0^k(M_0)-C_0^k(M_1)}{m}$ ist. Dieser Wert soll also maximiert werden. Zum anderen muss, damit die Sicherheitsbedingung erfüllt ist, gleichzeitig $C_\ell^{k-1}(M_0) = C_\ell^{k-1}(M_1)$ für alle $\ell = 0,\dots,k-1$ gelten.
Nach Anwendung des Satzes 3.2 erhalten wir daher folgendes Optimierungsproblem:

Zielfunktion: $\sum_{j=0}^{n-k} \binom{n-k}{j} \cdot (f_j(M_0) - f_j(M_1)) \longrightarrow$ maximieren

Nebenbedingungen: $\sum_{j=\ell}^{n-(k-1)+\ell} \binom{n-(k-1)}{j-\ell} \cdot (f_j(M_0) - f_j(M_1)) = 0 \qquad \forall \ell = 0,\dots,k-1.$

Sind bei festem k und n die Werte $f_i(M_0)$ und $f_i(M_1)$ für $i = 0,\dots,n$ bekannt, legen sie die Matrizen M_0 und M_1 fest. Definiert man $x_j := \frac{\binom{n}{j}\cdot f_j(M_0)}{m}$ und $y_j := \frac{\binom{n}{j}\cdot f_j(M_1)}{m}$ für alle $j = 0,\dots,n$, stellen die einzelnen Komponenten der Vektoren x und y die relativen Häufigkeiten der Vektoren mit Hamming-Gewicht j in M_0 und M_1 dar. Somit gilt $x_j, y_j \geq 0, j = 0,\dots n$ und $\sum_{j=0}^{n} x_j = \sum_{j=0}^{n} y_j = 1$. Daraus ergibt sich das Lineare Programm $L(k,n)$.

Definition 3.8:
Das Lineare Programm $L(k,n)$ mit $n \geq 2$ und $k \in \{2,\dots,n\}$ wird für die Variablen $((x_0,\dots,x_n),(y_0,\dots,y_n))$, 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. $x_j, y_j \geq 0, \qquad j = 0,\dots,n$
2. $\sum_{j=0}^{n} x_j = \sum_{j=0}^{n} y_j = 1$
3. $\sum_{j=\ell}^{n-k+\ell+1} \binom{n-k+1}{j-\ell} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) = 0, \qquad \ell = 0,\dots,k-1.$

Durch das folgende Lemma lässt sich zeigen, dass die Menge der total symmetrischen (k,n)-Schemata der Lösungsmenge des Linearen Programms $L(k,n)$ entspricht. Es lässt

sich also einem total symmetrischen Schema eine Lösung des Linearen Programms zuordnen und umgekehrt.

Lemma 3.17:

1. Sei $C = (C_0, C_1)$ ein total symmetrisches (k, n)-Schema, welches durch die Matrizen M_0 und M_1 erzeugt wurde. Dann ist das Lineare Programm $L(k, n)$ erfüllt durch $x_j := f_j(M_0) \cdot \binom{n}{j} \cdot m^{-1}$ und $y_j := f_j(M_1) \cdot \binom{n}{j} \cdot m^{-1}, j = 0, \ldots, n$. Darüber hinaus liefern x und y den Kontrast des Schemas C, der dem Zielfunktionswert entspricht.

2. Seien die zwei Vektoren $(x, y) = ((x_0, \ldots, x_n), (y_0, \ldots, y_n))$ eine Lösung des Linearen Programms $L(k, n)$ mit einem Zielfunktionswert größer als Null. Dann gibt es ein total symmetrisches (k, n)-Schema C, bei dem der Kontrast $\alpha(C)$ dem Zielfunktionswert entspricht.

Beweis:

1. Wir kennen das total symmetrische Schema C und somit auch die Werte $x_j = f_j(M_0 \cdot \binom{n}{j} \cdot m^{-1})$ und $y_j = f_j(M_1 \cdot \binom{n}{j} \cdot m^{-1})$ für $j = 0, \ldots, n$. Damit lassen sich die Nebenbedingungen des Linearen Programms überprüfen:

   (1) Offensichtlich sind alle Werte x_j und y_j nichtnegativ.

   (2) Der Wert $f_j(M) \cdot \binom{n}{j}$ entspricht gerade der Anzahl an Vektoren v einer $n \times m$-Matrix M mit Hamming-Gewicht $H(v) = j$ für alle $j = 0, \ldots, n$. Also gilt $m = \sum_{j=0}^{n} f_j(M) \cdot \binom{n}{j}$, woraus

$$\sum_{j=0}^{n} x_j = \sum_{j=0}^{n} f_j(M_0) \cdot \binom{n}{j} \cdot m^{-1} = 1 = \sum_{j=0}^{n} f_j(M_1) \cdot \binom{n}{j} \cdot m^{-1} = \sum_{j=0}^{n} y_j$$

   folgt. Damit ist die zweite Nebenbedingung erfüllt.
   (3) Die dritte Nebenbedingung ist auch erfüllt, da für alle $\ell = 0, \ldots, k-1$ gilt

$$\sum_{j=\ell}^{n-k+\ell+1} \binom{n-k+1}{j-\ell} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j)$$
$$= \sum_{j=\ell}^{n-k+\ell+1} \binom{n-k+1}{j-\ell} \cdot \binom{n}{j}^{-1} \cdot \left(f_j(M_0) \cdot \binom{n}{j} \cdot m^{-1} - f_j(M_1) \cdot \binom{n}{j} \cdot m^{-1} \right)$$

$$
\begin{aligned}
&= m^{-1} \cdot \sum_{j=\ell}^{n-k+\ell+1} \binom{n-k+1}{j-\ell} \cdot (f_j(M_0) - f_j(M_1)) \\
&= m^{-1} \cdot \left(\sum_{j=\ell}^{n-k+\ell+1} \binom{n-k+1}{j-\ell} \cdot f_j(M_0) - \sum_{j=\ell}^{n-k+\ell+1} \binom{n-k+1}{j-\ell} \cdot f_j(M_1) \right) \\
&= m^{-1} \cdot (C_\ell^{k-1}(M_0) - C_\ell^{k-1}(M_1)) && \text{nach Satz 3.2} \\
&= 0 && \text{nach Lemma 3.16.}
\end{aligned}
$$

Somit kann der Zielfunktionswert bestimmt werden:

$$
\begin{aligned}
&\sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) \\
&= \sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot \left(f_j(M_0) \cdot \binom{n}{j} \cdot m^{-1} - f_j(M_1) \cdot \binom{n}{j} \cdot m^{-1} \right) \\
&= \left(\sum_{j=0}^{n-k} \binom{n-k}{j} \cdot (f_j(M_0) - f_j(M_1)) \right) \cdot m^{-1} \\
&= \left(\sum_{j=0}^{n-k} f_j(M_0) \cdot \binom{n-k}{j} - \sum_{j=0}^{n-k} f_j(M_1) \cdot \binom{n-k}{j} \right) \cdot m^{-1} \\
&= (C_0^k(M_0) - C_0^k(M_1)) \cdot m^{-1} && \text{nach Satz 3.2} \\
&= \alpha(C) && \text{nach Lemma 3.16.}
\end{aligned}
$$

2. Stellen die beiden Vektoren x und y eine Lösung des Linearen Programms $L(k,n)$ dar, lassen sich die Komponenten als $x_j = \frac{A_j \cdot \binom{n}{j}}{m}$ und $y_j = \frac{B_j \cdot \binom{n}{j}}{m}$ darstellen, da sie rationale Zahlen sind. Dies folgt aus den Nebenbedingungen (1) und (2). Die Werte A_j, B_j und m sind dabei natürliche Zahlen. Durch diese Zahlen können nun zwei total symmetrische Matrizen M_0 und M_1 konstruiert werden:
   Die Matrix M_0 enthält jede Spalte mit Hamming-Gewicht j genau A_j mal, also insgesamt $A_j \cdot \binom{n}{j}$ Spalten mit Hamming-Gewicht j,
   Die Matrix M_1 enthält jede Spalte mit Hamming-Gewicht j genau B_j mal, also insgesamt $B_j \cdot \binom{n}{j}$ Spalten mit Hamming-Gewicht j.
   Aus M_0 und M_1 wird nun das total symmetrische Schema, wie in der Definition 3.7 angegeben, gebildet.
   Für dieses Schema ist die Sicherheitsbedingung erfüllt, da die Nebenbedingung (3) von $L(k,n)$ bedingt, dass $C_j^{k-1}(M_0) = C_j^{k-1}(M_1), j = 0, \ldots, k-1$, gilt (Lemma 3.16). Für den Zielfunktionswert von $L(k,n)$ ergibt sich

$$
\sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j)
$$

$$
\begin{aligned}
&= \sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot \binom{n}{j} \cdot (A_j - B_j) \cdot m^{-1} \\
&= m^{-1} \cdot \left(\left(\sum_{j=0}^{n-k} \binom{n-k}{j} \cdot A_j \right) - \left(\sum_{j=0}^{n-k} \binom{n-k}{j} \cdot B_j \right) \right) \\
&= m^{-1} \cdot \left(C_0^k(M_0) - C_0^k(M_1) \right) && \text{nach Satz 3.2} \\
&= \alpha(C) && \text{nach Lemma 3.16.}
\end{aligned}
$$

□

Die Nebenbedingungen (1) und (2) des Linearen Programms $L(k,n)$ stellen sicher, dass die relativen Häufigkeiten zulässige Werte sind. Nebenbedingung (3) hingegen stellt die Sicherheitsbedingung eines (k,n)-Schemas dar. Lemma 3.17 besagt darüber hinaus, dass der Wert einer optimalen Lösung des Linearen Programms $L(k,n)$ dem maximal erzielbaren Kontrast eines (k,n)-Schemas entspricht. Denn würde ein (k,n)-Schema mit einem Kontrast größer als dem optimalen Zielfunktionswert von $L(k,n)$ existieren, dann gäbe es nach Lemma 3.17 Teil 1 einen größeren als den optimalen Zielfunktionswert. Da dies offensichtlich ein Widerspruch ist, muss der maximal erzielbare Kontrast eines (k,n)-Schemas dem optimalen Zielfunktionswert von $L(k,n)$ entsprechen.

Lemma 3.18:
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 $x_j \geq y_j$.
Fall 1: $y_j = 1$

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. Dies stellt jedoch einen Widerspruch zur Voraussetzung dar. Somit muss $y_j < 1$ gelten.

Fall 2: $0 < y_j < 1$

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 als $x''_i := \frac{x'_i}{s}$ und $y''_i := \frac{y'_i}{s}$ für alle $i = 0, \ldots, n$. 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 dies 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 $j = 0, \ldots, n$. □

3.2.3 Lösungen für spezielle Lineare Programme

In diesem Abschnitt werden für die Linearen Programme $L(2, n), L(3, n), L(k-1, k)$ und $L(k, k)$ die optimalen Lösungen bestimmt. Diese stellen, wie im vorigen Abschnitt gezeigt wurde, die maximal erreichbaren Kontraste der jeweils entsprechenden (k, n)-Schemata dar.

Das Lineare Programm $L(2, n)$

Für das Lineare Programm $L(k, n)$ aus Definition 3.8 ergibt sich mit $k = 2$:
Zielfunktion:

$$\begin{aligned}
L(2,n) &= \sum_{j=0}^{n-2} \binom{n-2}{j} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) \\
&= \sum_{j=0}^{n-2} \frac{(n-2)!}{j! \cdot (n-2-j)!} \cdot \frac{j! \cdot (n-j)!}{n!} \cdot (x_j - y_j) \\
&= \sum_{j=0}^{n} \frac{(n-j) \cdot (n-j-1)}{n \cdot (n-1)} \cdot (x_j - y_j) \\
&= \sum_{j=0}^{n} \frac{n^2 - 2 \cdot n \cdot j - n + j + j^2}{n \cdot (n-1)} \cdot (x_j - y_j)
\end{aligned}$$

$$
\begin{aligned}
&= \underbrace{\sum_{j=0}^{n} \frac{n^2}{n\cdot(n-1)} \cdot (x_j - y_j)}_{=0 \text{ (nach Nebenbedingung (2))}} - \underbrace{\sum_{j=0}^{n} \frac{2\cdot n\cdot j}{n\cdot(n-1)} \cdot (x_j - y_j)}_{=0 \text{ (nach Nebenbedingung (3b))}} \\
&\quad - \underbrace{\sum_{j=0}^{n} \frac{n-j}{n\cdot(n-1)} \cdot (x_j - y_j)}_{=0 \text{ (nach Nebenbedingung (3a))}} + \sum_{j=0}^{n} \frac{j^2}{n\cdot(n-1)} \cdot (x_j - y_j) \\
&= \sum_{j=0}^{n} \frac{j^2}{n\cdot(n-1)} \cdot (x_j - y_j) \longrightarrow \text{maximiere} \qquad (3.8)
\end{aligned}
$$

mit den Nebenbedingungen

1. $x_j, y_j \geq 0 \qquad j = 0, \ldots, n$
2. $\sum\limits_{j=0}^{n} x_j = \sum\limits_{j=0}^{n} y_j = 1$
3. a) $\ell = 0$: $\quad \sum\limits_{j=0}^{n-1} \binom{n-1}{j} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) = 0$

   $\iff \quad \sum\limits_{j=0}^{n} (n-j) \cdot (x_j - y_j) = 0$

   b) $\ell = 1$: $\quad \sum\limits_{j=1}^{n} \binom{n-1}{j-1} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) = 0$

   $\iff \quad \sum\limits_{j=0}^{n} j \cdot (x_j - y_j) = 0.$

An dieser Stelle ist eine Fallunterscheidung bezüglich der Parität von n nötig. Betrachten wir zunächst den Fall, n ist eine gerade Zahl.
Die Zielfunktion 3.8 lässt sich umformen zu

$$
\begin{aligned}
&\sum_{j=0}^{n} \frac{j^2}{n\cdot(n-1)} \cdot (x_j - y_j) \\
&= \sum_{j=0}^{n} \frac{j^2}{n\cdot(n-1)} \cdot (x_j - y_j) + \sum_{j=0}^{n} \frac{(\frac{n}{2})^2}{n\cdot(n-1)} \cdot (x_j - y_j) - \sum_{j=0}^{n} \frac{j\cdot n}{n\cdot(n-1)} \cdot (x_j - y_j) \\
&= \sum_{j=0}^{n} \frac{(j-\frac{n}{2})^2}{n\cdot(n-1)} \cdot (x_j - y_j) \\
&= \underbrace{\sum_{j=0}^{n} \frac{(j-\frac{n}{2})^2}{n\cdot(n-1)} \cdot x_j}_{A} - \underbrace{\sum_{j=0}^{n} \frac{(j-\frac{n}{2})^2}{n\cdot(n-1)} \cdot y_j}_{B} \longrightarrow \text{maximiere.} \qquad (3.9)
\end{aligned}
$$

Unter der Annahme, dass Teil A konstant ist, muss Teil B minimiert werden, damit die Zielfunktion einen maximalen Wert annehmen kann. Der minimale Wert für B ist 0, da kein y_j negativ sein kann. Mit der folgenden Belegung der $y_j, j = 0, \ldots, n$, ist es möglich

den Wert für Teil B auf 0 zu bringen:

$$y_j = \begin{cases} 1 & \text{falls } j = \frac{n}{2} \\ 0 & \text{sonst.} \end{cases}$$

Durch Lemma 3.18 wissen wir, dass $x_{\frac{n}{2}}$ gleich 0 sein muss. Gleichzeitig müssen die Nebenbedingungen erfüllt werden, um eine zulässige Lösung zu erhalten. Aus den Nebenbedingungen $3a$ und $3b$ wird ersichtlich, dass die beiden jeweils größten Summanden aus Teil A mit in den Funktionswert zu gleichen Teilen einfließen müssen. Somit ergibt sich für den Vektor x die Belegung

$$x_j = \begin{cases} \frac{1}{2} & \text{falls } j = 0 \text{ oder } j = n \\ 0 & \text{sonst.} \end{cases}$$

Die so konstruierte Lösung bezeichnen wir mit (x^*, y^*), also gilt

$$(x^*, y^*) = \left((x_0^*, x_1^*, \ldots, x_n^*), (y_0^*, y_1^*, \ldots, y_n^*)\right) = \left(\left(\frac{1}{2}, 0, \ldots, 0, \frac{1}{2}\right), (0, \ldots, 0, 1, 0, \ldots, 0)\right),$$

was eine zulässige Lösung ist, da alle Nebenbedingungen erfüllt werden.
Setzen wir die Lösung (x^*, y^*) in die Zielfunktion 3.8 ein, ergibt sich

$$\begin{aligned} &\sum_{j=0}^{n} \frac{j^2}{n \cdot (n-1)} \cdot (x_j - y_j) \\ &= \frac{0^2}{n \cdot (n-1)} \cdot \frac{1}{2} + \frac{(\frac{n}{2})^2}{n \cdot (n-1)} \cdot (-1) + \frac{n^2}{n \cdot (n-1)} \cdot \frac{1}{2} \\ &= -\frac{1}{4} \cdot \frac{n^2}{n \cdot (n-1)} + \frac{1}{2} \cdot \frac{n^2}{n \cdot (n-1)} \\ &= \frac{n}{4 \cdot (n-1)} \end{aligned} \tag{3.10}$$

als Zielfunktionswert.
Die Lösung (x^*, y^*) stellt damit eine optimale Lösung dar, denn für jede beliebige zulässige Belegung der Variablen $((x_0, \ldots, x_n), (y_0, \ldots, y_n))$ ergibt sich als Zielfunktionswert maximal

$$\sum_{j=0}^{n} \frac{(j - \frac{n}{2}) \cdot (j - \frac{n}{2})}{n \cdot (n-1)} \cdot x_j - \sum_{j=0}^{n} \frac{(j - \frac{n}{2}) \cdot (j - \frac{n}{2})}{n \cdot (n-1)} \cdot y_j \qquad \text{nach 3.9}$$

$$\leq \sum_{j=0}^{n} \frac{\frac{n^2}{4}}{n \cdot (n-1)} \cdot x_j = \frac{\frac{n^2}{4}}{n \cdot (n-1)} \cdot \sum_{j=0}^{n} x_j = \frac{n}{4 \cdot (n-1)},$$

was genau dem Funktionswert entspricht, der durch die Lösung (x^*, y^*) erreicht wird. Dies entspricht auch dem in Satz 3.1 bestimmten Wert.
Mit dem folgenden Lemma wird gezeigt, dass die Lösung (x^*, y^*) auch eindeutig ist.

Lemma 3.19:
Die einzige Lösung des Linearen Programms $L(2,n)$, die den optimalen Zielfunktionswert von $\frac{n}{4\cdot(n-1)}$, für n gerade, liefert, ist (x^*, y^*).

Beweis: Die Zielfunktion des Linearen Programms $L(2,n)$ lässt sich für gerade n und beliebige zulässige Variablen (x,y) nach 3.9 umformen zu

$$\sum_{j=0}^{n} \frac{(j-\frac{n}{2})^2}{n\cdot(n-1)} \cdot x_j - \sum_{j=0}^{n} \frac{(j-\frac{n}{2})^2}{n\cdot(n-1)} \cdot y_j$$

$$= \frac{1}{n\cdot(n-1)} \cdot \left(\underbrace{\sum_{j=0}^{n} \left(j-\frac{n}{2}\right)^2 \cdot x_j}_{A} - \underbrace{\sum_{j=0}^{n} \left(j-\frac{n}{2}\right)^2 \cdot y_j}_{B} \right) \longrightarrow \text{ maximiere.}$$

Der Summand $(j-\frac{n}{2})^2$ aus Teil A nimmt lediglich für $j=0$ und $j=n$ den Wert $\frac{n^2}{4}$ an, welcher maximal ist. Da die Summe der Variablen x_j gleich Eins sein muss, wird Teil A nur dann maximal, wenn $x_0 + x_n = 1$ gilt. Jede andere Belegung der Variablen würde dazu führen, dass der maximale Wert von Teil A kleiner ist als $\frac{n^2}{4}$. Somit muss $x_0 + x_n = 1$ und $x_j = 0, j = 1, \ldots, n-1$, gelten.
Der maximal erreichbare Zielfunktionswert von $\frac{n}{4\cdot(n-1)}$ kann nur erreicht werden, wenn $A - B = \frac{n^2}{4}$ ist. Somit muss Teil B gleich 0 sein. Dies ist unter Berücksichtigung der Nebenbedingungen nur möglich, wenn $y_{\frac{n}{2}} = 1$ und $y_j = 0, j \neq \frac{n}{2}$, gilt, da bei jeder anderen Belegung der Variablen ein Summand entstehen würde, der vom Teil A subtrahiert werden müsste. Dann könnte jedoch die Zielfunktion nicht mehr den maximalen Wert annehmen.
Somit lässt sich die Belegung für x_0 und x_n bestimmen:

$0 \cdot x_0 + 1 \cdot x_1 + \ldots + n \cdot x_n = 0 \cdot y_0 + 1 \cdot y_1 + \ldots + n \cdot y_n$ nach Nebenbedingung 3*b*

$\Longrightarrow 0 \cdot x_0 + n \cdot x_n = \frac{n}{2} \cdot y_{\frac{n}{2}} = \frac{n}{2} \cdot 1$

$\Longrightarrow x_n = \frac{1}{2}$

$\Longrightarrow x_0 = \frac{1}{2}.$

Da diese Lösung die selbe ist wie (x^*, y^*), ist gezeigt, dass (x^*, y^*) die einzige Lösung ist, für die das Lineare Programm $L(2,n)$ den maximalen Zielfunktionswert annimmt. □

Nun betrachten wir den Fall, dass n eine ungerade Zahl ist.
Hier lässt sich die Zielfunktion 3.8 umformen zu

$$\begin{aligned}
&\sum_{j=0}^{n} \frac{j^2}{n\cdot(n-1)} \cdot (x_j - y_j) \\
&= \sum_{j=0}^{n} \frac{j^2}{n\cdot(n-1)} \cdot (x_j - y_j) + \sum_{j=0}^{n} \frac{\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil}{n\cdot(n-1)} \cdot (x_j - y_j) - \sum_{j=0}^{n} \frac{j\cdot n}{n\cdot(n-1)} \cdot (x_j - y_j) \\
&= \sum_{j=0}^{n} \frac{(j - \lfloor \frac{n}{2} \rfloor)\cdot(j - \lceil \frac{n}{2} \rceil)}{n\cdot(n-1)} \cdot (x_j - y_j) \longrightarrow \text{maximiere.} \qquad (3.11)
\end{aligned}$$

Der Zielfunktionswert kann somit nur ein Maximum von

$$\begin{aligned}
\sum_{j=0}^{n} \frac{\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil}{n\cdot(n-1)} \cdot x_j &= \frac{\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil}{n\cdot(n-1)} \cdot \sum_{j=0}^{n} x_j = \frac{\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil}{n\cdot(n-1)} \\
&= \frac{\frac{n-1}{2} \cdot \frac{n+1}{2}}{n\cdot(n-1)} = \frac{(n-1)\cdot(n+1)}{4\cdot n\cdot(n-1)} \\
&= \frac{n - \frac{1}{n}}{4\cdot(n-1)} < \frac{n}{4\cdot(n-1)}
\end{aligned}$$

erreichen. Durch den bekannten Maximalwert kann nun eine optimale Lösung bestimmt werden.
Für eine beliebige zulässige Belegung der Variablen hat die Zielfunktion 3.11 die Form

$$\frac{1}{n\cdot(n-1)} \cdot \left(\underbrace{\sum_{j=0}^{n} \left(j - \left\lfloor \frac{n}{2} \right\rfloor\right) \cdot \left(j - \left\lceil \frac{n}{2} \right\rceil\right) \cdot x_j}_{A} - \underbrace{\sum_{j=0}^{n} \left(j - \left\lfloor \frac{n}{2} \right\rfloor\right) \cdot \left(j - \left\lceil \frac{n}{2} \right\rceil\right) \cdot y_j}_{B} \right).$$

Der Term $(j - \lfloor \frac{n}{2} \rfloor) \cdot (j - \lceil \frac{n}{2} \rceil)$ aus Teil A nimmt nur für $j = 0$ und $j = n$ den Wert $\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil$ an, welcher maximal ist. Daraus folgt, dass $x_0 + x_n = 1$ gelten muss, da bei jeder anderen Belegung der Variablen der Zielfunktionswert kleiner wäre. Durch die Nebenbedingungen folgt $x_j = 0, j = 1, \ldots, n-1$.
Der maximal erreichbare Zielfunktionswert $\frac{n+1}{4n}$ kann nur erreicht werden, wenn $A - B = \lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil$ gilt. Somit muss $B = 0$ gelten. Da der Term $(j - \lfloor \frac{n}{2} \rfloor) \cdot (j - \lceil \frac{n}{2} \rceil)$ aus Teil B nur für $j = \lfloor \frac{n}{2} \rfloor$ und $j = \lceil \frac{n}{2} \rceil$ gleich 0 ist, muss $y_j = 0, j \neq \lfloor \frac{n}{2} \rfloor$ und $j \neq \lceil \frac{n}{2} \rceil$, sowie $y_{\lfloor \frac{n}{2} \rfloor} + y_{\lceil \frac{n}{2} \rceil} = 1$ gelten.
Damit die gewählte Belegung auch zulässig ist, müssen alle Nebenbedingungen erfüllt werden, was für die ersten beiden offensichtlich gilt. Aus den Nebenbedingungen $3a$ und $3b$ folgt

$$\begin{aligned}
&n\cdot x_0 + \left(n - \left\lfloor \frac{n}{2} \right\rfloor\right) \cdot \left(-y_{\lfloor \frac{n}{2} \rfloor}\right) + \left(n - \left\lceil \frac{n}{2} \right\rceil\right) \cdot \left(-y_{\lceil \frac{n}{2} \rceil}\right) = 0 \\
&\iff n\cdot x_0 - \left\lceil \frac{n}{2} \right\rceil \cdot y_{\lfloor \frac{n}{2} \rfloor} - \left\lfloor \frac{n}{2} \right\rfloor \cdot y_{\lceil \frac{n}{2} \rceil} = 0
\end{aligned}$$

sowie

$$\begin{aligned}&\left\lfloor\frac{n}{2}\right\rfloor\cdot\left(-y_{\lfloor\frac{n}{2}\rfloor}\right)+\left\lceil\frac{n}{2}\right\rceil\cdot\left(-y_{\lceil\frac{n}{2}\rceil}\right)+n\cdot x_n=0\\ \Longleftrightarrow\ &n\cdot x_n-\left\lfloor\frac{n}{2}\right\rfloor\cdot y_{\lfloor\frac{n}{2}\rfloor}-\left\lceil\frac{n}{2}\right\rceil\cdot y_{\lceil\frac{n}{2}\rceil}=0.\end{aligned}$$

Die vier Gleichungen

$$\begin{aligned}&x_0+x_n=1\\ &y_{\lfloor\frac{n}{2}\rfloor}+y_{\lceil\frac{n}{2}\rceil}=1\\ &n\cdot x_0-\left\lceil\frac{n}{2}\right\rceil\cdot y_{\lfloor\frac{n}{2}\rfloor}-\left\lfloor\frac{n}{2}\right\rfloor\cdot y_{\lceil\frac{n}{2}\rceil}=0\\ &n\cdot x_n-\left\lfloor\frac{n}{2}\right\rfloor\cdot y_{\lfloor\frac{n}{2}\rfloor}-\left\lceil\frac{n}{2}\right\rceil\cdot y_{\lceil\frac{n}{2}\rceil}=0\end{aligned}$$

lassen sich jedoch nicht eindeutig lösen. Die Matrixform $A\cdot X=b$ des Linearen Gleichungssystems ist

$$\begin{pmatrix}1&1&0&0\\0&0&1&1\\n&0&-\left\lceil\frac{n}{2}\right\rceil&-\left\lfloor\frac{n}{2}\right\rfloor\\0&n&-\left\lfloor\frac{n}{2}\right\rfloor&-\left\lceil\frac{n}{2}\right\rceil\end{pmatrix}\cdot\begin{pmatrix}x_0\\x_n\\y_{\lfloor\frac{n}{2}\rfloor}\\y_{\lceil\frac{n}{2}\rceil}\end{pmatrix}=\begin{pmatrix}1\\1\\0\\0\end{pmatrix},$$

wobei A die 4×4-Koeffizientenmatrix, X der Vektor der 4 Variablen und b der Ergebnisvektor ist. Aus der Linearen Algebra ist bekannt, dass ein Lineares Gleichungssystem der Form $A\cdot X=b$ genau dann lösbar ist, wenn $\mathrm{Rang}(A)=\mathrm{Rang}(A|b)$ gilt. Ist der Rang der (erweiterten) Koeffizientenmatrix gleich der Anzahl der Variablen, dann hat das Lineare Gleichungssystem genau eine Lösung. Für das vorliegende Gleichungssystem gilt jedoch $\mathrm{Rang}(A)=3<4$. Das gegebene System ist demnach nicht eindeutig lösbar. Eine mögliche Lösung ist $x_0=x_n=y_{\lfloor\frac{n}{2}\rfloor}=y_{\lceil\frac{n}{2}\rceil}=\frac{1}{2}$. Die Belegung der Variablen

$$\begin{aligned}x_j&=\begin{cases}\frac{1}{2}&\text{falls } j=0 \text{ oder } j=n\\0&\text{sonst,}\end{cases}\\ y_j&=\begin{cases}\frac{1}{2}&\text{falls } j=\lfloor\frac{n}{2}\rfloor \text{ oder } j=\lceil\frac{n}{2}\rceil\\0&\text{sonst}\end{cases}\end{aligned}$$

mit dem Zielfunktionswert

$$\begin{aligned}&\sum_{j=0}^{n}\frac{j^2}{n\cdot(n-1)}\cdot(x_j-y_j)\\ &=\frac{0^2}{n\cdot(n-1)}\cdot\frac{1}{2}+\frac{\lfloor\frac{n}{2}\rfloor^2}{n\cdot(n-1)}\cdot(-\frac{1}{2})+\frac{\lceil\frac{n}{2}\rceil^2}{n\cdot(n-1)}\cdot(-\frac{1}{2})+\frac{n^2}{n\cdot(n-1)}\cdot\frac{1}{2}\\ &=\frac{n+1}{4n}\end{aligned}$$

ist eine optimale Lösung des Linearen Programms $L(2,n)$ für ungerades n.

$(2, n)$-Schemata nach $L(2, n)$

Im vorigen Abschnitt haben wir gezeigt, dass der maximal erreichbare Kontrast für $(2, n)$-Schemata bei

$$\alpha = \begin{cases} \frac{n}{4\cdot(n-1)} & \text{falls } n \text{ gerade} \\ \\ \frac{n+1}{4n} & \text{falls } n \text{ ungerade} \end{cases}$$

liegt. Desweiteren konnten wir jeweils eine Belegung der Variablen angeben, die den optimalen Kontrast liefert. Nach Lemma 3.17 ist es damit möglich, jeweils ein total symmetrisches Schema anzugeben, das den optimalen Kontrast besitzt.
Zuerst konstruieren wir das $(2, n)$-Schema für n gerade.
Die einzige Lösung des Linearen Programms $L(2, n)$, die den optimalen Kontrast liefert, ist

$$x_j = \begin{cases} \frac{1}{2} & \text{falls } j = 0 \text{ oder } j = n \\ 0 & \text{sonst} \end{cases}$$
$$y_j = \begin{cases} 1 & \text{falls } j = \frac{n}{2} \\ 0 & \text{sonst.} \end{cases}$$

Durch den Beweis von Lemma 3.17 wissen wir, dass x_j und y_j die relativen Häufigkeiten der Spaltenvektoren mit genau j Einsen repräsentieren. Somit lassen sich x_j und y_j darstellen als

$$x_j = \frac{A_j \cdot \binom{n}{j}}{m} \text{ und } y_j = \frac{B_j \cdot \binom{n}{j}}{m}$$

mit $A_j, B_j, m \in \mathbb{N} \cup \{0\}$ und $m \geq 2, j = 0, \ldots, n$. Dabei müssen die Werte für A_j, B_j und m entsprechend gewählt werden. Mit diesen Angaben lassen sich nun die zwei total symmetrischen Matrizen M_0 und M_1 aus $\{0, 1\}^{n\times m}$ angeben, die benötigt werden, um ein total symmetrisches Schema zu konstruieren.
Für die Matrix M_0 müssen dabei die beiden Gleichungen

$$x_0 = \frac{f_0(M_0) \cdot \binom{n}{0}}{m} \qquad \text{und}$$
$$x_n = \frac{f_n(M_0) \cdot \binom{n}{n}}{m}$$

gelten. Das heißt, jeder $\{0, 1\}^n$-Vektor mit j Einsen muss genau A_j mal in der Matrix M_0 vorhanden sein.
In der Matrix M_1 müssen alle $\{0, 1\}^n$-Vektoren mit j Einsen genau B_j mal vorhanden sein. Daher muss hier

$$y_{\frac{n}{2}} = \frac{f_{\frac{n}{2}}(M_1) \cdot \binom{n}{\frac{n}{2}}}{m}$$

gelten. Wählen wir die Häufigkeiten f_j als

$$f_j(M_0) = \begin{cases} \frac{m}{2\cdot\binom{n}{j}} & \text{falls } j = 0 \text{ oder } j = n \\ 0 & \text{sonst} \end{cases}$$
$$f_j(M_1) = \begin{cases} \frac{m}{\binom{n}{j}} & \text{falls } j = \frac{n}{2} \\ 0 & \text{sonst,} \end{cases}$$

dann sind alle Gleichungen erfüllt. Die Werte der Häufigkeiten $f_0(M_0), f_n(M_0)$ und $f_{\frac{n}{2}}(M_1)$ müssen jedoch ganzzahlig sein. Deshalb wählen wir $m = \binom{n}{\frac{n}{2}}$ als kleinstes gemeinsames Vielfache der Nenner.
Die Matrizen M_0 und M_1 sind somit festgelegt durch

$$f_0(M_0) = \frac{1}{2} \cdot \binom{n}{\frac{n}{2}},$$
$$f_n(M_0) = \frac{1}{2} \cdot \binom{n}{\frac{n}{2}} \qquad \text{und}$$
$$f_{\frac{n}{2}}(M_1) = 1.$$

Somit besteht M_0 aus $\frac{m}{2}$ Nullspalten und $\frac{m}{2}$ Einsspalten, in M_1 hingegen hat jede Spalte genau $\frac{n}{2}$ Einsen:

$$M_0 = \begin{pmatrix} 0 & \cdots & 0 & 1 & \ldots & 1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & \ldots & 1 \end{pmatrix}, \quad M_1 = \begin{pmatrix} \frac{n}{2} \text{ Einsen pro Spalte} \end{pmatrix}.$$

Mit diesen Matrizen lässt sich nun ein total symmetrisches $(2, n)$-Schema $C = (C_0, C_1)$ konstruieren, welches den Kontrast $\frac{n}{4\cdot(n-1)}$ hat:

$$C_0 = \{M_0 \text{ und alle Spaltenpermutationen von } M_0\} \qquad \text{und}$$
$$C_1 = \{M_1 \text{ und alle Spaltenpermutationen von } M_1\}.$$

Nun konstruieren wir das $(2, n)$-Schema für n ungerade.
Im vorigen Abschnitt haben wir gezeigt, dass es für ungerade n mehrere Belegungen der Variablen gibt, die einen maximalen Kontrast erzielen. Im Folgenden soll die Schemakonstruktion für die Lösung

$$x_j = \begin{cases} \frac{1}{2} & \text{falls } j = 0 \text{ oder } j = n \\ 0 & \text{sonst,} \end{cases}$$
$$y_j = \begin{cases} \frac{1}{2} & \text{falls } j = \lfloor \frac{n}{2} \rfloor \text{ oder } j = \lceil \frac{n}{2} \rceil \\ 0 & \text{sonst} \end{cases}$$

exemplarisch betrachtet werden.
Die Variablen x_j und y_j repräsentieren auch hier die relativen Häufigkeiten der Spaltenvektoren mit genau j Einsen, nach Lemma 3.17. Somit lassen sie sich darstellen als

$$x_j = \frac{A_j \cdot \binom{n}{j}}{m} \text{ und } y_j = \frac{B_j \cdot \binom{n}{j}}{m}$$

mit $A_j, B_j, m \in \mathbb{N} \cup \{0\}$ und $m \geq 2, j = 0, \ldots, n$. Dabei müssen die Werte für A_j, B_j und m entsprechend gewählt werden. Jetzt lassen sich die zwei total symmetrischen Matrizen $M_0, M_1 \in \{0,1\}^{n \times m}$ angeben, die benötigt werden, um ein total symmetrisches Schema zu konstruieren.
Die Matrix M_0 muss jeden $\{0,1\}^n$-Vektor mit j Einsen genau A_j mal enthalten, M_1 hingegen genau B_j mal. Daher müssen die Gleichungen

$$\begin{aligned}
x_0 &= \frac{f_0(M_0) \cdot \binom{n}{0}}{m} \\
x_n &= \frac{f_n(M_0) \cdot \binom{n}{n}}{m} \\
y_{\lfloor \frac{n}{2} \rfloor} &= \frac{f_{\lfloor \frac{n}{2} \rfloor}(M_1) \cdot \binom{n}{\lfloor \frac{n}{2} \rfloor}}{m} \\
y_{\lceil \frac{n}{2} \rceil} &= \frac{f_{\lceil \frac{n}{2} \rceil}(M_1) \cdot \binom{n}{\lceil \frac{n}{2} \rceil}}{m}
\end{aligned}$$

erfüllt werden. Somit können wir die Häufigkeiten wählen als

$$f_j(M_0) = \begin{cases} \frac{m}{2 \cdot \binom{n}{j}} & \text{falls } j = 0 \text{ oder } j = n \\ 0 & \text{sonst} \end{cases}$$

$$f_j(M_1) = \begin{cases} \frac{m}{2 \cdot \binom{n}{j}} & \text{falls } j = \lfloor \frac{n}{2} \rfloor \text{ oder } j = \lceil \frac{n}{2} \rceil \\ 0 & \text{sonst.} \end{cases}$$

Auch hier wählen wir $m = 2 \cdot \binom{n}{\lfloor \frac{n}{2} \rfloor} = 2 \cdot \binom{n}{\lceil \frac{n}{2} \rceil}$ als kleinstes gemeinsames Vielfache der Nenner.
Die Matrizen M_0 und M_1 sind somit durch

$$\begin{aligned}
f_0(M_0) &= \binom{n}{\lceil \frac{n}{2} \rceil}, \\
f_n(M_0) &= \binom{n}{\lceil \frac{n}{2} \rceil}, \\
f_{\lfloor \frac{n}{2} \rfloor}(M_1) &= 1, \\
f_{\lceil \frac{n}{2} \rceil}(M_1) &= 1
\end{aligned}$$

eindeutig bestimmt. Die Matrix M_0 besteht demnach aus $\frac{m}{2}$ Nullspalten und $\frac{m}{2}$ Einsspalten, in M_1 hingegen ist jede Spalte mit $\lfloor \frac{n}{2} \rfloor$ Einsen und jede Spalte mit $\lceil \frac{n}{2} \rceil$ Einsen genau einmal vorhanden.
Mit diesen Matrizen lässt sich nun ein total symmetrisches $(2, n)$-Schema $C = (C_0, C_1)$ konstruieren, welches den Kontrast $\frac{n+1}{4n}$ hat:

$$C_0 = \{M_0 \text{ und alle Spaltenpermutationen von } M_0\} \qquad \text{und}$$
$$C_1 = \{M_1 \text{ und alle Spaltenpermutationen von } M_1\}.$$

Das Lineare Programm $L(3, n)$

Das Lineare Programm $L(k, n)$ vereinfacht sich für $k = 3$ zu:
Zielfunktion:

$$\begin{aligned}
&\sum_{j=0}^{n-3} \binom{n-3}{j} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) \\
=&\sum_{j=0}^{n-3} \frac{(n-3)!}{j! \cdot (n-3-j)!} \cdot \frac{j! \cdot (n-j)!}{n!} \cdot (x_j - y_j) \\
=&\sum_{j=0}^{n} \frac{(n-j) \cdot (n-j-1) \cdot (n-j-2)}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j - y_j) \\
=&\underbrace{\sum_{j=0}^{n} \frac{n \cdot (n-j) \cdot (n-j-1)}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j - y_j)}_{=0 \text{ (nach Nebenbedingung } (3a))} - \sum_{j=0}^{n} \frac{j \cdot (n-j) \cdot (n-j-1)}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j - y_j) \\
&\underbrace{- \sum_{j=0}^{n} \frac{2 \cdot (n-j) \cdot (n-j-1)}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j - y_j)}_{=0 \text{ (nach Nebenbedingung } (3a))} \\
=&- \sum_{j=0}^{n} \frac{j \cdot (n-j) \cdot (n-j-1)}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j - y_j) \\
=&\underbrace{- \sum_{j=0}^{n} \frac{n \cdot j \cdot (n-j)}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j - y_j)}_{=0 \text{ (nach Nebenbedingung } (3b))} + \sum_{j=0}^{n} \frac{j^2 \cdot (n-j)}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j - y_j) \\
&\underbrace{+ \sum_{j=0}^{n} \frac{j \cdot (n-j)}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j - y_j)}_{=0 \text{ (nach Nebenbedingung } (3b))} \\
=&\sum_{j=0}^{n} \frac{j^2 \cdot (n-j)}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j - y_j) \longrightarrow \text{ maximiere}
\end{aligned} \tag{3.12}$$

mit den 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. a) $\ell = 0$:

$$\sum_{j=0}^{n-2} \binom{n-2}{j} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) = 0$$

$$\iff \sum_{j=0}^{n} (n-j) \cdot (n-j-1) \cdot (x_j - y_j) = 0$$

$$\iff \sum_{j=0}^{n} \big((n-1) \cdot (n-j) - j \cdot (n-j)\big) \cdot (x_j - y_j) = 0$$

$$\iff \sum_{j=0}^{n} (n-1) \cdot (n-j) \cdot (x_j - y_j) - \underbrace{\sum_{j=0}^{n} j \cdot (n-j) \cdot (x_j - y_j)}_{=0 \text{ (nach Nebenbedingung (3}b\text{))}} = 0$$

$$\iff \sum_{j=0}^{n} (n-1) \cdot (n-j) \cdot (x_j - y_j) = 0$$

$$\iff \sum_{j=0}^{n} (n-j) \cdot (x_j - y_j) = 0$$

b) $\ell = 1$:

$$\sum_{j=1}^{n-1} \binom{n-2}{j-1} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) = 0$$

$$\iff \sum_{j=0}^{n} j \cdot (n-j) \cdot (x_j - y_j) = 0$$

c) $\ell = 2$:

$$\sum_{j=2}^{n} \binom{n-2}{j-2} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) = 0$$

$$\iff \sum_{j=0}^{n} j \cdot (j-1) \cdot (x_j - y_j) = 0.$$

Lemma 3.20:
Falls n durch 4 teilbar ist, haben die Zielfunktionen

$$\sum_{j=0}^{n} \frac{j^2 \cdot (n-j)}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j - y_j) \qquad \text{und} \tag{3.13}$$

$$\sum_{j=0}^{n} \frac{(n-j) \cdot (j - \frac{n}{4}) \cdot (j - \frac{n}{4})}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j - y_j) \tag{3.14}$$

den selben Wert, für alle zulässigen Lösungen $(x_0, \ldots, x_n, y_0, \ldots, y_n)$.

Beweis:

$$
\begin{aligned}
&\sum_{j=0}^{n} \frac{(n-j)\cdot(j-\frac{n}{4})\cdot(j-\frac{n}{4})}{n\cdot(n-1)\cdot(n-2)}\cdot(x_j-y_j)\\
=&\sum_{j=0}^{n} \frac{n\cdot j^2-j^3-\frac{1}{2}\cdot n^2\cdot j+\frac{1}{2}\cdot n\cdot j^2+\frac{1}{16}\cdot n^3-\frac{1}{16}\cdot n^2\cdot j}{n\cdot(n-1)\cdot(n-2)}\cdot(x_j-y_j)\\
=&\sum_{j=0}^{n} \frac{(n\cdot j^2-j^3)+\frac{1}{2}\cdot n\cdot j\cdot(j-n)-\frac{1}{16}\cdot n^2\cdot(j-n)}{n\cdot(n-1)\cdot(n-2)}\cdot(x_j-y_j)\\
=&\sum_{j=0}^{n} \frac{n\cdot j^2-j^3}{n\cdot(n-1)\cdot(n-2)}\cdot(x_j-y_j)+\underbrace{\sum_{j=0}^{n} \frac{\frac{n}{2}\cdot j\cdot(j-n)}{n\cdot(n-1)\cdot(n-2)}\cdot(x_j-y_j)}_{=0 \text{ (nach Nebenbedingung } (3b))}\\
&\underbrace{-\sum_{j=0}^{n} \frac{\frac{n^2}{16}\cdot(j-n)}{n\cdot(n-1)\cdot(n-2)}\cdot(x_j-y_j)}_{=0 \text{ (nach Nebenbedingung } (3a))}\\
=&\sum_{j=0}^{n} \frac{j^2\cdot(n-j)}{n\cdot(n-1)\cdot(n-2)}\cdot(x_j-y_j),
\end{aligned}
$$

wie behauptet. □

Für durch 4 teilbare n ist es daher ausreichend für die Zielfunktion 3.14 eine zulässige Belegung zu finden, die den maximal möglichen Kontrast liefert.
Analog zu den $(2,n)$-Schemata aus dem vorigen Abschnitt (siehe Zielfunktion 3.9) soll nun

$$
\underbrace{\sum_{j=0}^{n} \frac{(n-j)\cdot(j-\frac{n}{4})\cdot(j-\frac{n}{4})}{n\cdot(n-1)\cdot(n-2)}\cdot x_j}_{A}-\underbrace{\sum_{j=0}^{n} \frac{(n-j)\cdot(j-\frac{n}{4})\cdot(j-\frac{n}{4})}{n\cdot(n-1)\cdot(n-2)}\cdot y_j}_{B} \tag{3.15}
$$

maximiert werden. Unter der Annahme, dass Teil A konstant ist, muss Teil B minimiert werden. Nur so kann die Zielfunktion einen maximalen Wert annehmen. Der minimale Wert für Teil B ist 0, welcher bei einer zulässigen Belegung der Variablen $y_j, j=0,\ldots,n$, nur dann erreicht wird, wenn

$$
y_j \;=\; \begin{cases} \frac{2}{3} & \text{falls } j=\frac{n}{4} \\ \frac{1}{3} & \text{falls } j=n \\ 0 & \text{sonst} \end{cases}
$$

gewählt wird. Damit folgt aus Lemma 3.18 für $x_{\frac{n}{4}}$ und x_n der Wert 0. Um eine zulässige Lösung zu erhalten, müssen alle Nebenbedingungen erfüllt sein. Die Nebenbedingung $3b$

hat nach Einsetzen von allen y_j die Form

$$\begin{aligned}
&0 \cdot x_0 + 1 \cdot (n-1) \cdot (x_1 - 0) + \ldots + \left(\frac{n}{4} - 1\right) \cdot \left(n - \left(\frac{n}{4} - 1\right)\right) \cdot \left(x_{\frac{n}{4}-1} - 0\right) \\
&+ \frac{n}{4} \cdot \left(n - \frac{n}{4}\right) \cdot \left(x_{\frac{n}{4}} - \frac{2}{3}\right) + \left(\frac{n}{4} + 1\right) \cdot \left(n - \left(\frac{n}{4} + 1\right)\right) \cdot \left(x_{\frac{n}{4}+1} - 0\right) + \ldots \\
&+ \frac{3n}{4} \cdot \left(n - \frac{3n}{4}\right) \cdot \left(x_{\frac{3n}{4}} - 0\right) + \ldots + n \cdot (n-n) \cdot \left(x_n - \frac{1}{3}\right) = 0. \qquad (3.16)
\end{aligned}$$

Eine zulässige Belegung der Variablen $x_j, j = 0, \ldots, n$, ist somit

$$x_j \quad = \quad \begin{cases} \frac{1}{3} & \text{falls } j = 0 \\ \frac{2}{3} & \text{falls } j = \frac{3n}{4} \\ 0 & \text{sonst.} \end{cases}$$

Die gewählte Belegung der Variablen $(x_0, \ldots, x_n, y_0, \ldots, y_n)$ erfüllt alle Nebenbedingungen und ist somit zulässig. Sie wird im Folgenden mit (x^*, y^*) bezeichnet. Als Zielfunktionswert ergibt sich

$$\begin{aligned}
&\sum_{j=0}^{n} \frac{j^2 \cdot (n-j)}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j^* - y_j^*) \\
&= 0 \cdot \frac{1}{3} + \frac{(\frac{n}{4})^2 \cdot (n - \frac{n}{4})}{n \cdot (n-1) \cdot (n-2)} \cdot \left(-\frac{2}{3}\right) + \frac{(\frac{3n}{4})^2 \cdot (n - \frac{3n}{4})}{n \cdot (n-1) \cdot (n-2)} \cdot \left(\frac{2}{3}\right) + 0 \cdot \left(-\frac{1}{3}\right) \\
&= -\frac{n^2}{2 \cdot 16 \cdot (n-1) \cdot (n-2)} + \frac{3 \cdot n^2}{2 \cdot 16 \cdot (n-1) \cdot (n-2)} \\
&= \frac{n^2}{16 \cdot (n-1) \cdot (n-2)}.
\end{aligned}$$

Nun bestimmen wir den maximal erzielbaren Kontrast aller $(3, n)$-Schemata, für durch 4 teilbare n.
Als obere Schranke für den Kontrast einer beliebigen zulässigen Lösung für $L(3, n)$ erhalten wir

$$\begin{aligned}
&\sum_{j=0}^{n} \frac{(n-j) \cdot (j - \frac{n}{4}) \cdot (j - \frac{n}{4})}{n \cdot (n-1) \cdot (n-2)} \cdot (x_j - y_j) \leq \sum_{j=0}^{n} \frac{(n-j) \cdot (j - \frac{n}{4}) \cdot (j - \frac{n}{4})}{n \cdot (n-1) \cdot (n-2)} \cdot x_j \\
&\leq \sum_{j=0}^{n} \frac{\frac{n^3}{16}}{n \cdot (n-1) \cdot (n-2)} \cdot x_j = \frac{\frac{n^3}{16}}{n \cdot (n-1) \cdot (n-2)} \cdot \sum_{j=0}^{n} x_j = \frac{n^2}{16 \cdot (n-1) \cdot (n-2)},
\end{aligned}$$

was dem Zielfunktionswert entspricht, den wir mit der Lösung (x^*, y^*) erhalten haben. Somit ist diese Lösung optimal.

Lemma 3.21:
Die Lösung (x^*, y^*) ist die einzige Lösung, die den maximalen Zielfunktionswert des Linearen Programms $L(3, n)$ liefert, falls n eine durch 4 teilbare Zahl ist.

Beweis: Die Zielfunktion

$$\frac{1}{n \cdot (n-1) \cdot (n-2)} \cdot \left(\underbrace{\sum_{j=0}^{n} (n-j) \cdot (j - \frac{n}{4}) \cdot (j - \frac{n}{4}) \cdot x_j}_{A} \right.$$
$$\left. - \underbrace{\sum_{j=0}^{n} (n-j) \cdot (j - \frac{n}{4}) \cdot (j - \frac{n}{4}) \cdot y_j}_{B} \right)$$

nimmt im Teil A nur dann den maximalen Wert von $\frac{n^3}{16}$ an, wenn $j = 0$ oder $j = \frac{3n}{4}$ ist. Somit muss $x_0 + x_{\frac{3n}{4}} = 1$ gelten, da der Wert von Teil A sonst kleiner ist. Aus der zweiten Nebenbedingung folgt dann $x_j = 0$ für alle anderen Werte von j.
Wäre der Teil B größer als 0, müsste dieser Betrag vom Teil A subtrahiert werden. Dies würde bedeuten, dass die Zielfunktion nicht mehr den maximalen Wert annehmen kann. Deshalb muss Teil B gleich 0 sein. Da dies lediglich für $j = \frac{n}{4}$ und $j = n$ gilt, muss unter Berücksichtigung der Nebenbedingungen $y_{\frac{n}{4}} + y_n = 1$ gelten. Alle anderen Variablen y_j sind demnach gleich 0.
Um eine zulässige Lösung zu erhalten, müssen die Nebenbedingungen erfüllt sein. Aus den Nebenbedingungen $3a$ und $3b$ entstehen die Gleichungen

$$n \cdot x_0 + \left(n - \frac{n}{4}\right) \cdot (-y_{\frac{n}{4}}) + \left(n - \frac{3n}{4}\right) \cdot x_{\frac{3n}{4}} = 0$$
$$\iff 4 \cdot x_0 - 3 \cdot y_{\frac{n}{4}} + x_{\frac{3n}{4}} = 0$$

und

$$\frac{n}{4} \cdot \left(n - \frac{n}{4}\right) \cdot (-y_{\frac{n}{4}}) + \frac{3n}{4} \cdot \left(n - \frac{3n}{4}\right) \cdot x_{\frac{3n}{4}} = 0$$
$$\iff x_{\frac{3n}{4}} - y_{\frac{n}{4}} = 0.$$

Insgesamt erhalten wir somit vier Gleichungen mit vier Unbekannten:

$$\begin{cases} x_0 + x_{\frac{3n}{4}} = 1 \\ y_{\frac{n}{4}} + y_n = 1 \\ 4 \cdot x_0 - 3 \cdot y_{\frac{n}{4}} + x_{\frac{3n}{4}} = 0 \\ x_{\frac{3n}{4}} - y_{\frac{n}{4}} = 0. \end{cases}$$

Dieses Gleichungssystem ist eindeutig lösbar. Die Werte der Variablen sind

$$x_0 = \frac{1}{3}, \qquad x_{\frac{3n}{4}} = \frac{2}{3}, \qquad y_{\frac{n}{4}} = \frac{2}{3}, \qquad y_n = \frac{1}{3},$$

welche den Werten der Lösung (x^*, y^*) entsprechen. Diese Lösung liefert, wie bereits gezeigt wurde, den maximal möglichen Kontrast von

$$\frac{n^2}{16 \cdot (n-1) \cdot (n-2)}.$$

Daher ist die Lösung (x^*, y^*) die einzige optimale Lösung des Linearen Programms $L(3, n)$ für durch 4 teilbare n. □

$(3, n)$-Schemata nach $L(3, n)$

Um aus der Lösung für durch 4 teilbare n des Linearen Programms $L(3, n)$ mit

$$x_j = \begin{cases} \frac{1}{3} & \text{falls } j = 0 \\ \frac{2}{3} & \text{falls } j = \frac{3n}{4} \\ 0 & \text{sonst.} \end{cases}$$

$$y_j = \begin{cases} \frac{2}{3} & \text{falls } j = \frac{n}{4} \\ \frac{1}{3} & \text{falls } j = n \\ 0 & \text{sonst} \end{cases}$$

das entsprechende total symmetrische $(3, n)$-Schema zu konstruieren, können wir Lemma 3.17 anwenden. Somit lassen sich die Variablen x_j und y_j darstellen als

$$x_j = \frac{A_j \cdot \binom{n}{j}}{m} \text{ und } y_j = \frac{B_j \cdot \binom{n}{j}}{m}$$

mit $A_j, B_j, m \in \mathbb{N} \cup \{0\}$ und $m \geq 2, j = 0, \ldots, n$. Die Werte für A_j, B_j und m müssen dabei geeignet gewählt werden.

Jetzt lassen sich die zwei total symmetrischen Matrizen $M_0, M_1 \in \{0,1\}^{n\times m}$ bestimmen, die benötigt werden, um ein total symmetrisches Schema zu konstruieren.
Die Matrix M_0 muss dabei jeden $\{0,1\}^n$-Vektor mit j Einsen genau A_j mal enthalten. Daher müssen die beiden Gleichungen

$$x_0 = \frac{f_0(M_0)\cdot\binom{n}{0}}{m}$$
$$x_{\frac{3n}{4}} = \frac{f_{\frac{3n}{4}}(M_0)\cdot\binom{n}{\frac{3n}{4}}}{m}$$

erfüllt werden.
Entsprechend muss die Matrix M_1 alle $\{0,1\}^n$-Vektoren mit j Einsen genau B_j mal enthalten. Für M_1 müssen also die Gleichungen

$$y_{\frac{n}{4}} = \frac{f_{\frac{n}{4}}(M_1)\cdot\binom{n}{\frac{n}{4}}}{m}$$
$$y_n = \frac{f_n(M_1)\cdot\binom{n}{n}}{m}$$

gelten. Die Wahl der Häufigkeiten als

$$f_j(M_0) = \begin{cases} \frac{m}{3\cdot\binom{n}{0}} & \text{falls } j = 0 \\ \frac{m}{\frac{3}{2}\cdot\binom{n}{\frac{3n}{4}}} & \text{falls } j = \frac{3n}{4} \\ 0 & \text{sonst,} \end{cases}$$

$$f_j(M_1) = \begin{cases} \frac{m}{\frac{3}{2}\cdot\binom{n}{\frac{n}{4}}} & \text{falls } j = \frac{n}{4} \\ \frac{m}{3\cdot\binom{n}{n}} & \text{falls } j = n \\ 0 & \text{sonst} \end{cases}$$

erfüllt alle vier Gleichungen. Mit m als kleinstem gemeinsamen Vielfachen der Nenner ergibt sich

$$\begin{aligned} m &= \frac{3}{2}\cdot\binom{n}{\frac{n}{4}} = \frac{3}{2}\cdot\binom{n}{\frac{3n}{4}} \\ f_0(M_0) &= \frac{1}{2}\cdot\binom{n}{\frac{n}{4}} \\ f_{\frac{3n}{4}}(M_0) &= 1 \\ f_{\frac{n}{4}}(M_1) &= 1 \\ f_n(M_1) &= \frac{1}{2}\cdot\binom{n}{\frac{n}{4}}. \end{aligned}$$

Die Matrix M_0 enthält demnach $\frac{1}{2} \cdot \binom{n}{\frac{n}{4}}$ Nullspalten und jeden Spaltenvektor mit $\frac{3n}{4}$ Einsen genau einmal. Die Matrix M_1 hingegen enthält $\frac{1}{2} \cdot \binom{n}{\frac{n}{4}}$ Einsspalten und jeden Spaltenvektor mit $\frac{n}{4}$ Einsen genau einmal.
Mit diesen beiden Matrizen ist es nun möglich, das total symmetrische $(3, n)$-Schema $C = (C_0, C_1)$, für durch 4 teilbare n, zu konstruieren, welches den maximalen Kontrast hat:

$$C_0 = \{M_0 \text{ und alle Spaltenpermutationen von } M_0\} \qquad \text{und}$$
$$C_1 = \{M_1 \text{ und alle Spaltenpermutationen von } M_1\}.$$

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

Das lineare Programm $L(k-1, k)$ ist:
Zielfunktion:

$$\begin{aligned} L(k-1,k) &= \sum_{j=0}^{k-k+1} \binom{k-k+1}{j} \cdot \binom{k}{j}^{-1} \cdot (x_j - y_j) \\ &= (x_0 - y_0) + \frac{1}{k}(x_1 - y_1) \longrightarrow \text{maximieren} \end{aligned} \tag{3.17}$$

mit den Nebenbedingungen:

1. $x_j, y_j \geq 0 \qquad \ell = 0, \ldots, k$
2. $\sum_{j=0}^{k} x_j = \sum_{j=0}^{k} y_j = 1$
3. $\ell = 0, \ldots, k-2 : \quad \sum_{j=\ell}^{k-k+1+\ell+1} \binom{k-k+1+1}{j-\ell} \cdot \binom{k}{j}^{-1} \cdot (x_j - y_j) = 0$
   $\iff \quad \frac{(x_\ell - y_\ell)}{\binom{k}{\ell}} + 2\frac{(x_{\ell+1} - y_{\ell+1})}{\binom{k}{\ell+1}} + \frac{(x_{\ell+2} - y_{\ell+2})}{\binom{k}{\ell+2}} = 0.$

Fasst man ein Paar $(x_i - y_i)$ zusammen zu einem z_i, also $z_i := x_i - y_i$, so erhält man das folgende Lineare Programm $L(k-1, k)_z$:
Zielfunktion:

$$L(k-1,k)_z = z_0 + \frac{z_1}{k} \longrightarrow \text{maximieren} \tag{3.18}$$

mit den Nebenbedingungen:

1. $-1 \leq z_\ell \leq 1 \qquad \ell = 0, \ldots, k$
2. $\sum_{j=0}^{k}(x_j - y_j) = \sum_{j=0}^{k} z_j = 0$
3. $\ell = 0, \ldots, k-2 : \qquad \binom{k}{\ell}^{-1} z_\ell + 2\binom{k}{\ell+1}^{-1} z_{\ell+1} + \binom{k}{\ell+2}^{-1} z_{\ell+2} = 0.$

Durch diese Transformation fehlt in der zweiten Nebenbedingung jedoch die Eigenschaft,

dass alle x_i (bzw. y_i) aufsummiert 1 ergeben. Daher müssen zwei weitere Nebenbedingungen zu $L(k-1,k)_z$ hinzugefügt werden:

$$2a) \quad \sum_{\substack{i=0 \\ z_i>0}}^{k} z_i = 1$$
$$2b) \quad \sum_{\substack{i=0 \\ z_i<0}}^{k} z_i = -1.$$

Eine optimale Lösung des Linearen Programms $L(k-1,k)_z$ kann leicht in eine optimale Lösung des Linearen Programms $L(k-1,k)$ überführt werden. Nach Lemma 3.18 ist in einer optimalen Lösung für $L(k-1,k)$ mindestens einer der beiden Werte x_i oder y_i gleich 0. Somit entspricht ein positiver z_i-Wert gerade dem x_i-Wert und y_i ist 0. Analog für den negativen Fall. Sollte $z_i = 0$ gelten, folgt $x_i = y_i = 0$.
Durch Umformen der dritten Nebenbedingung lassen sich alle $z_\ell, \ell \in \{2,\dots,k\}$, in Abhängigkeit von z_0 und z_1 darstellen, wie das folgende Lemma zeigt.

Lemma 3.22:
Die Variablen $z_\ell, \ell \in \{2,\dots,k\}$, des Linearen Programms $L(k-1,k)_z$ lassen sich darstellen als

$$z_\ell = (-1)^{\ell-1}\left(\frac{1}{k}z_1 + (\ell-1)\left(z_0 + \frac{1}{k}z_1\right)\right)\binom{k}{\ell}. \tag{3.19}$$

Beweis: Beweis per Induktion über ℓ:
Induktionsanfang:
Aus der dritten Nebenbedingung folgt für z_2:

$$\begin{aligned}
&\binom{k}{0}^{-1} z_0 + 2\binom{k}{1}^{-1} z_1 + \binom{k}{2}^{-1} z_2 = 0 \\
\iff \quad & z_0 + 2\frac{z_1}{k} + \binom{k}{2}^{-1} z_2 = 0 \\
\iff \quad & \binom{k}{2}^{-1} z_2 = -z_0 - 2\frac{z_1}{k} \\
\iff \quad & z_2 = \left(-z_0 - 2\frac{z_1}{k}\right)\binom{k}{2} \\
\iff \quad & z_2 = -\left(z_0 + 2\frac{z_1}{k}\right)\binom{k}{2} \qquad (3.20) \\
& \quad = (-1)^{2-1}\left(\frac{z_1}{k} + (2-1)\left(z_0 + \frac{z_1}{k}\right)\right)\binom{k}{2}
\end{aligned}$$

und damit für z_3:

$$\begin{aligned}
& \binom{k}{1}^{-1} z_1 + 2\binom{k}{2}^{-1} z_2 + \binom{k}{3}^{-1} z_3 = 0 \\
\iff & \frac{z_1}{k} - 2\binom{k}{2}^{-1} \left(z_0 + 2\frac{z_1}{k}\right)\binom{k}{2} + \binom{k}{3}^{-1} z_3 = 0 && \text{nach 3.20} \\
\iff & \frac{z_1}{k} - \left(2z_0 + 4\frac{z_1}{k}\right) + \binom{k}{3}^{-1} z_3 = 0 \\
\iff & -2z_0 - 3\frac{z_1}{k} + \binom{k}{3}^{-1} z_3 = 0 \\
\iff & \binom{k}{3}^{-1} z_3 = 2z_0 + 3\frac{z_1}{k} \\
\iff & z_3 = \left(2z_0 + 3\frac{z_1}{k}\right)\binom{k}{3} \\
& \quad = (-1)^{3-1}\left(\frac{z_1}{k} + 2\left(z_0 + \frac{z_1}{k}\right)\right)\binom{k}{3}
\end{aligned}$$

Induktionsvoraussetzung:
Für alle $\ell \in \{2, \ldots, g\}, g < k$, gilt

$$z_\ell = (-1)^{\ell-1}\left(\frac{1}{k}z_1 + (\ell-1)\left(z_0 + \frac{1}{k}z_1\right)\right)\binom{k}{\ell}.$$

Induktionsschritt: $\ell = g + 1$:

$$\begin{aligned}
& \binom{k}{g-1}^{-1} z_{g-1} + 2\binom{k}{g}^{-1} z_g + \binom{k}{g+1}^{-1} z_{g+1} = 0 \\
\iff & \binom{k}{g-1}^{-1} (-1)^{g-2}\left(\frac{1}{k}z_1 + (g-2)\left(z_0 + \frac{1}{k}z_1\right)\right)\binom{k}{g-1} \\
& + 2\binom{k}{g}^{-1} (-1)^{g-1}\left(\frac{1}{k}z_1 + (g-1)\left(z_0 + \frac{1}{k}z_1\right)\right)\binom{k}{g} \\
& + \binom{k}{g+1}^{-1} z_{g+1} = 0 && \text{nach Induktionsvoraussetzung} \\
\iff & (-1)^{g-2}\left(\frac{1}{k}z_1 + (g-2)\left(z_0 + \frac{1}{k}z_1\right)\right) \\
& + 2(-1)^{g-1}\left(\frac{1}{k}z_1 + (g-1)\left(z_0 + \frac{1}{k}z_1\right)\right) \\
& + \binom{k}{g+1}^{-1} z_{g+1} = 0
\end{aligned}$$

An dieser Stelle ist eine Fallunterscheidung notwendig, da g gerade oder ungerade sein kann.

Fall I: g gerade:

$$
\begin{aligned}
& (-1)^{g-2}\left(\frac{1}{k}z_1+(g-2)\left(z_0+\frac{1}{k}z_1\right)\right)+2(-1)^{g-1}\left(\frac{1}{k}z_1+(g-1)\left(z_0+\frac{1}{k}z_1\right)\right)\\
& +\binom{k}{g+1}^{-1}z_{g+1}=0\\
\iff\quad & \left(\frac{1}{k}z_1+(g-2)\left(z_0+\frac{1}{k}z_1\right)\right)-2\left(\frac{1}{k}z_1+(g-1)\left(z_0+\frac{1}{k}z_1\right)\right)\\
& +\binom{k}{g+1}^{-1}z_{g+1}=0\\
\iff\quad & -\frac{1}{k}z_1-g\left(z_0+\frac{1}{k}z_1\right)+\binom{k}{g+1}^{-1}z_{g+1}=0\\
\iff\quad & z_{g+1}=\left(\frac{1}{k}z_1+g\left(z_0+\frac{1}{k}z_1\right)\right)\binom{k}{g+1}\\
& \quad =(-1)^{g+1-1}\left(\frac{1}{k}z_1+(g+1-1)\left(z_0+\frac{1}{k}z_1\right)\right)\binom{k}{g+1} \qquad \text{da } g \text{ gerade}
\end{aligned}
$$

Fall II: g ungerade:

$$
\begin{aligned}
& (-1)^{g-2}\left(\frac{1}{k}z_1+(g-2)\left(z_0+\frac{1}{k}z_1\right)\right)+2(-1)^{g-1}\left(\frac{1}{k}z_1+(g-1)\left(z_0+\frac{1}{k}z_1\right)\right)\\
& +\binom{k}{g+1}^{-1}z_{g+1}=0\\
\iff\quad & -\left(\frac{1}{k}z_1+(g-2)\left(z_0+\frac{1}{k}z_1\right)\right)+2\left(\frac{1}{k}z_1+(g-1)\left(z_0+\frac{1}{k}z_1\right)\right)\\
& +\binom{k}{g+1}^{-1}z_{g+1}=0\\
\iff\quad & \frac{1}{k}z_1+g\left(z_0+\frac{1}{k}z_1\right)+\binom{k}{g+1}^{-1}z_{g+1}=0\\
\iff\quad & z_{g+1}=-\left(\frac{1}{k}z_1+g\left(z_0+\frac{1}{k}z_1\right)\right)\binom{k}{g+1}\\
& \quad =(-1)^{g+1-1}\left(\frac{1}{k}z_1+(g+1-1)\left(z_0+\frac{1}{k}z_1\right)\right)\binom{k}{g+1} \qquad \text{da } g \text{ ungerade}
\end{aligned}
$$

Damit ist gezeigt, dass sich alle $z_\ell, \ell \in \{2,\dots,k\}$, in Abhängigkeit von z_0 und z_1 darstellen lassen, wie behauptet. □

Um die dritte Nebenbedingung zu erfüllen, müssen somit nach Lemma 3.22 alle z_ℓ-Werte entsprechend der Formel (3.19) bestimmt werden. Gleichzeitig wird dadurch die

Nebenbedingung 2 erfüllt, denn es gilt

$$
\begin{aligned}
&\sum_{j=0}^{k} z_j \\
&\quad = z_0 + z_1 + \sum_{j=2}^{k} z_j \\
&\quad = z_0 + z_1 + \sum_{j=2}^{k} (-1)^{j-1} \left(\frac{1}{k} z_1 + (j-1) \left(z_0 + \frac{1}{k} z_1 \right) \right) \binom{k}{j} \qquad \text{nach Lemma 3.22} \\
&\quad = z_0 + z_1 + \sum_{j=2}^{k} (-1)^{j-1} \binom{k}{j} \frac{z_1}{k} + \sum_{j=2}^{k} (-1)^{j-1} \binom{k}{j} (j-1) \left(z_0 + \frac{z_1}{k} \right) \\
&\quad = z_0 + z_1 + \frac{z_1}{k} \sum_{j=2}^{k} (-1)^{j-1} \binom{k}{j} + \left(z_0 + \frac{z_1}{k} \right) \sum_{j=2}^{k} (-1)^{j-1} \binom{k}{j} (j-1) \\
&\quad = z_0 + z_1 + \frac{z_1}{k} (1-k) + \left(z_0 + \frac{z_1}{k} \right) (-1) \\
&\quad = z_0 + z_1 + \frac{z_1}{k} - z_1 - z_0 - \frac{z_1}{k} \\
&\quad = 0.
\end{aligned}
$$

Im Folgenden wird versucht, den optimalen Zielfunktionswert und somit den maximalen Kontrast eines $(k-1,k)$-Schemas für k gerade zu bestimmen. Dabei sind die 4 Fälle

Fall 1: $z_0 > 0 \quad z_1 \geq 0$
Fall 2: $z_0 \leq 0 \quad z_1 > 0$
Fall 3: $z_0 > 0 \quad z_1 < 0$
Fall 4: $z_0 < 0 \quad z_1 < 0$

zu unterscheiden. Da der optimale Zielfunktionswert stets positiv ist, kann Fall 4 vernachlässigt werden, denn eine Lösung des Linearen Programms $L(k-1,k)_z$ mit negativen z_0 und z_1 würde einen negativen Zielfunktionswert liefern.
Betrachten wir zunächst Fall 1.
Da, nach Annahme, z_0 und z_1 positive Werte sind, ist ein z_ℓ-Wert genau dann negativ, wenn ℓ eine gerade Zahl ist. Dies geht unmittelbar aus Formel (3.19) hervor. Aus der Nebenbedingung $2a$ wissen wir, dass die Summe der positiven z_ℓ-Werte gleich 1 sein muss. Somit können wir alle positiven z_ℓ aufsummieren und damit z_0 in Abhängigkeit von z_1 darstellen. Anschließend liefert die erste Nebenbedingung eine obere Schranke für den maximal erzielbaren Kontrast.
Aus Nebenbedingung $2a$ folgt

$$\sum_{\substack{j=0 \\ z_j>0}}^{k} z_j = 1$$

$$
\begin{aligned}
\iff \quad & z_0 + z_1 + \sum_{\substack{j=2 \\ z_j>0}}^{k} z_j = 1 \\
\iff \quad & z_0 + z_1 + \sum_{\substack{j=3 \\ j \text{ ungerade}}}^{k} \left(\frac{1}{k} z_1 + (j-1)\left(z_0 + \frac{1}{k} z_1\right)\right)\binom{k}{j} = 1 \\
\iff \quad & z_0 + z_1 + \frac{z_1}{k} \sum_{\substack{j=3 \\ j \text{ ungerade}}}^{k} \binom{k}{j} + z_0 \sum_{\substack{j=3 \\ j \text{ ungerade}}}^{k} j\binom{k}{j} + \frac{z_1}{k} \sum_{\substack{j=3 \\ j \text{ ungerade}}}^{k} j\binom{k}{j} \\
& \quad - z_0 \sum_{\substack{j=3 \\ j \text{ ungerade}}}^{k} \binom{k}{j} - \frac{z_1}{k} \sum_{\substack{j=3 \\ j \text{ ungerade}}}^{k} \binom{k}{j} = 1 \\
\iff \quad & z_0 + z_1 + z_0 \frac{1}{4}\left(2^k - 4\right) k + z_1 \frac{1}{4}\left(2^k - 4\right) - z_0\left(2^{k-1} - k\right) = 1 \\
\iff \quad & z_0\left(1 + \frac{1}{4}\left(2^k - 4\right) k - 2^{k-1} + k\right) + z_1\left(1 + \frac{1}{4}\left(2^k - 4\right)\right) = 1 \\
\iff \quad & z_0\left(2^{k-2}\left(k-2\right) + 1\right) + z_1 2^{k-2} = 1 \\
\iff \quad & z_0 = \frac{4 - 2^k z_1}{2^k k - 2^{k+1} + 4} \qquad (3.21)
\end{aligned}
$$

und damit für Formel (3.19)

$$
z_\ell = (-1)^{\ell-1}\left(\frac{1}{k} z_1 + (\ell - 1)\left(\frac{4 - 2^k z_1}{2^k k - 2^{k+1} + 4} + \frac{1}{k} z_1\right)\right)\binom{k}{\ell}.
$$

Aus Nebenbedingung 1 ist bekannt, dass $-1 \leq z_\ell \leq 1$ gelten muss. Für gerades k folgt damit

$$
\begin{aligned}
& -1 \leq z_{\frac{k}{2}} \\
\iff \quad & -1 \leq \frac{2(k + z_1 - 2)}{2^k(k-2) + 4}\binom{k}{\frac{k}{2}} \\
\iff \quad & -(2^k(k-2) + 4) \leq 2\binom{k}{\frac{k}{2}}(k + z_1 - 2) \\
\iff \quad & -\frac{(2^k(k-2) + 4)}{2}\binom{k}{\frac{k}{2}}^{-1} \leq (k + z_1 - 2) \\
\iff \quad & -\frac{(2^k(k-2) + 4)}{2}\binom{k}{\frac{k}{2}}^{-1} - k + 2 \leq z_1 \qquad (3.22)
\end{aligned}
$$

und

$$\begin{aligned}
& & z_{\frac{k}{2}} \leq & 1 \\
\iff & & \frac{2(k+z_1-2)}{2^k(k-2)+4}\binom{k}{\frac{k}{2}} \leq & 1 \\
\iff & & 2\binom{k}{\frac{k}{2}}(k+z_1-2) \leq & 2^k(k-2)+4 \\
\iff & & (k+z_1-2) \leq & \frac{2^k(k-2)+4}{2}\binom{k}{\frac{k}{2}}^{-1} \\
\iff & & z_1 \leq & \frac{2^k(k-2)+4}{2}\binom{k}{\frac{k}{2}}^{-1} - k + 2. \qquad (3.23)
\end{aligned}$$

Die Zielfunktion $L(k-1,k)_z$ hat nach Einsetzen von z_0 die Form

$$L(k-1,k)_z = \frac{4-2^k z_1}{2^k k - 2^{k+1}+4} + \frac{z_1}{k} \qquad \text{nach (3.21)}$$

und ist für festes k monoton fallend in z_1. Demnach muss z_1 möglichst klein gewählt werden, um den Zielfunktionswert zu maximieren. Aus (3.22) und (3.23) folgt dabei, dass $z_1 = 0$ gelten muss, da sowohl z_0 als auch z_1 nach Annahme nicht negativ sind. Folglich ist der maximale Zielfunktionswert für den Fall 1

$$\alpha_{max} \leq \frac{4}{2^k k - 2^{k+1}+4}.$$

Für den Fall 2 verfährt man analog zu obigem Verfahren. Da der Term $z_0 + \frac{z_1}{k}$ aus Formel (3.19) gerade dem Zielfunktionswert entspricht, kann man davon ausgehen, dass dieser Wert positiv ist. Somit ist auch im Fall 2 die Summe über die z_ℓ mit ungeradem Index zu bilden. Als Ergebnis erhält man

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

was eingesetzt in die Zielfunktion

$$L(k-1,k)_z = -\frac{z_1}{2k^2}$$

liefert. Da aber auch im Fall 2 davon ausgegangen wird, dass z_1 nicht negativ ist, resultiert hieraus ein negativer Zielfunktionswert. Daher kann Fall 2 bei einer optimalen Lösung nicht eintreten.
Betrachten wir nun den Fall 3, also $z_0 > 0, z_1 < 0$.
In diesem Fall ist das oben beschriebene Vorgehen nicht möglich, da $\frac{z_1}{k}$ so klein sein könnte, dass der gesamte Term $\frac{z_1}{k} + (\ell-1)(z_0 + \frac{z_1}{k})$ aus Formel (3.19) für einige ℓ negativ sein könnte. Dadurch ist unklar, welche z_ℓ positiv sind. Betrachtet man jedoch einige konkrete $(k-1,k)$-Schemata für gerade k, beispielsweise $k = 4, 6, 8, 10, 12$, stellt man fest, dass in einer optimalen Belegung jeweils $z_{\frac{k}{2}} = 0$ gilt. Daraus kann man die Vermutung ableiten, dass auch im Allgemeinen $z_{\frac{k}{2}} = 0$ gelten muss.

Lemma 3.23:
Die folgenden drei Aussagen sind äquivalent:

1. Für eine optimale Belegung der Variablen des Linearen Programms $L(k-1,k)_z$ gilt für gerade k: $z_{\frac{k}{2}} = 0$.

2. Es existiert genau eine Belegung der Variablen des Linearen Programms $L(k-1,k)_z$ für gerade k, die den optimalen Zielfunktionswert liefert.

3. Die optimale Belegung der Variablen des Linearen Programms $L(k-1,k)_z$ für gerade k ist:

$$z_0 = 2\binom{k}{\frac{k}{2}}^{-1} \qquad z_1 = (4-2k)\binom{k}{\frac{k}{2}}^{-1}$$
$$z_\ell = (-1)^{\ell-1}\left(\frac{1}{k}z_1 + (\ell-1)(z_0 + \frac{1}{k}z_1)\right)\binom{k}{\ell} \qquad \ell \in \{2,\ldots,k\}.$$

Beweis: Die Korrektheit der drei Aussagen aus Lemma 3.23 wird durch einen Ringschluss gezeigt, also $1 \Longrightarrow 2 \Longrightarrow 3 \Longrightarrow 1$.
$\underline{1 \Longrightarrow 2:}$
Nach Annahme gilt $z_{\frac{k}{2}} = 0$. Somit folgt aus Formel (3.19)

$$\begin{aligned}
& z_{\frac{k}{2}} = 0 \\
& \quad = (-1)^{\frac{k}{2}-1}\left(\frac{1}{k}z_1 + \left(\frac{k}{2}-1\right)\left(z_0 + \frac{1}{k}z_1\right)\right)\binom{k}{\frac{k}{2}} \\
\Longleftrightarrow \quad & 0 = \frac{1}{k}z_1 + \left(\frac{k}{2}-1\right)\left(z_0 + \frac{1}{k}z_1\right) \\
\Longleftrightarrow \quad & 0 = \frac{z_1}{2} + \left(\frac{k}{2}-1\right)z_0 \\
\Longleftrightarrow \quad & -\frac{z_1}{2} = \frac{k-2}{2}z_0 \\
\Longleftrightarrow \quad & -z_1 = (k-2)z_0 \\
\Longleftrightarrow \quad & -\frac{z_1}{k-2} = z_0. \qquad (3.24)
\end{aligned}$$

Dies können wir nun in Formel (3.19) einsetzen und erhalten

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

$$
\begin{aligned}
&= (-1)^{\ell-1}\left(\frac{1}{k}z_1 + (\ell-1)\left(-\frac{z_1 2}{k(k-2)}\right)\right)\binom{k}{\ell}\\
&= (-1)^{\ell-1}\left(\frac{z_1(k-2)}{k(k-2)} - \frac{z_1 2(\ell-1)}{k(k-2)}\right)\binom{k}{\ell}\\
&= (-1)^{\ell-1}\left(\frac{z_1(k-2-2(\ell-1))}{k(k-2)}\right)\binom{k}{\ell}\\
&= (-1)^{\ell-1} z_1 \frac{(k-2\ell)}{k(k-2)}\binom{k}{\ell}. \qquad (3.25)
\end{aligned}
$$

Wir gehen davon aus, dass z_1 negativ ist. Das heißt, z_ℓ ist für $\ell < \frac{k}{2}$ genau dann positiv, wenn ℓ eine gerade Zahl ist. Analog ist z_ℓ für $\ell > \frac{k}{2}$ genau dann positiv, wenn ℓ eine ungerade Zahl ist. Folglich kann nun die Summe der positiven z_ℓ bestimmt werden, wodurch eine lineare Funktion in Abhängigkeit von z_1 entsteht. Da diese den Wert 1 annehmen muss, um die zweite Nebenbedingung zu erfüllen, ist z_1 eindeutig festgelegt. Somit ist die Belegung der Variablen ebenfalls eindeutig.

$\underline{2 \Longrightarrow 3:}$
Um zu zeigen, dass die zweite Aussage von Lemma 3.23 die dritte Aussage impliziert, wird gezeigt, dass $2 \Longrightarrow 1$ gilt und anschließend $1 \Longrightarrow 3$.
Sei $(z_0, z_1, \ldots, z_k)$ eine optimale Belegung des Linearen Programms $L(k-1,k)_z$ für gerades k. Dann ist auch $(z'_0, z'_1, \ldots, z'_k)$ mit $z'_\ell = -z_{k-\ell}$ eine optimale Belegung, denn es gilt nach Formel (3.19)

$$
\begin{aligned}
z'_0 + \frac{z'_1}{k} &= -z_k - \frac{z_{k-1}}{k}\\
&= -(-1)^{k-1}\left(\frac{1}{k}z_1 + (k-1)\left(z_0 + \frac{1}{k}z_1\right)\right)\binom{k}{k}\\
&\quad - \frac{1}{k}(-1)^{k-2}\left(\frac{1}{k}z_1 + (k-2)\left(z_0 + \frac{1}{k}z_1\right)\right)\binom{k}{k-1}\\
&= \left(\frac{1}{k}z_1 + (k-1)\left(z_0 + \frac{1}{k}z_1\right)\right) - \left(\frac{1}{k}z_1 + (k-2)\left(z_0 + \frac{1}{k}z_1\right)\right)\\
&= (k-1-k+2)\left(z_0 + \frac{1}{k}z_1\right)\\
&= z_0 + \frac{1}{k}z_1
\end{aligned}
$$

und alle Nebenbedingungen werden erfüllt, da sie bereits durch die optimale Belegung $(z_0, z_1, \ldots, z_k)$ erfüllt wurden. Damit die Belegung eindeutig ist, muss $z_\ell = -z_{k-\ell}$ gelten:

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

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

Es muss also die selbe Beziehung gelten, wie bereits Formel 3.24 ausdrückt. Somit ist $2 \implies 1$ gezeigt. Um auch $1 \implies 3$ zu zeigen, bestimmen wir, wie bereits im ersten Teil des Beweises skizziert, die Summe der positiven z_ℓ und erhalten so einen eindeutigen Wert für z_1.
Für $\ell < \frac{k}{2}$ sind die z_ℓ positiv, bei denen ℓ eine gerade Zahl ist. Für $\ell > \frac{k}{2}$ sind hingegen die z_ℓ positiv, bei denen ℓ eine ungerade Zahl ist. Durch die Beziehung $z_\ell = -z_{k-\ell}$ ist die Summe der positiven z_ℓ für $\ell > \frac{k}{2}$ vom Betrag gleich 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. Dies vereinfacht die Summenberechnung:

$$
\begin{aligned}
&\sum_{\substack{j=0 \\ z_j>0}}^{k} z_j \\
&\qquad = z_0 - z_1 - \sum_{\substack{j=3 \\ j \text{ ungerade}}}^{k/2} z_j + \sum_{\substack{j=2 \\ j \text{ gerade}}}^{k/2} z_j \\
&\qquad = z_0 - z_1 - \sum_{\substack{j=3 \\ j \text{ ungerade}}}^{k/2} \left(\frac{1}{k}z_1 + (j-1)\left(z_0 + \frac{1}{k}z_1\right)\right)\binom{k}{j} \\
&\qquad\quad - \sum_{\substack{j=2 \\ j \text{ gerade}}}^{k/2} \left(\frac{1}{k}z_1 + (j-1)\left(z_0 + \frac{1}{k}z_1\right)\right)\binom{k}{j} \qquad \text{nach (3.19)} \\
&\qquad = -\frac{z_1}{k-2} - z_1 - \sum_{\substack{j=3 \\ j \text{ ungerade}}}^{k/2} \left(\frac{1}{k}z_1 + (j-1)\left(-\frac{z_1}{k-2} + \frac{1}{k}z_1\right)\right)\binom{k}{j} \\
&\qquad\quad - \sum_{\substack{j=2 \\ j \text{ gerade}}}^{k/2} \left(\frac{1}{k}z_1 + (j-1)\left(-\frac{z_1}{k-2} + \frac{1}{k}z_1\right)\right)\binom{k}{j}
\end{aligned}
$$

$$
\begin{aligned}
&= -\frac{z_1}{k-2} - z_1 - \sum_{\substack{j=3\\ j \text{ ungerade}}}^{k/2} z_1 \left(\frac{j}{k} - \frac{j-1}{k-2}\right)\binom{k}{j} \\
&\quad - \sum_{\substack{j=2\\ j \text{ gerade}}}^{k/2} z_1 \left(\frac{j}{k} - \frac{j-1}{k-2}\right)\binom{k}{j} \\
&= -\frac{z_1}{k-2} - z_1 - \sum_{\substack{i=3\\ i \text{ ungerade}}}^{k/2} z_1 \frac{k-2i}{k(k-2)}\binom{k}{i} - \sum_{\substack{i=2\\ i \text{ gerade}}}^{k/2} z_1 \frac{k-2i}{k(k-2)}\binom{k}{i} \\
&= z_1 \left(-\frac{1}{k-2} - 1 - \sum_{i=2}^{k/2} \frac{k-2i}{k(k-2)}\binom{k}{i}\right) \\
&= z_1 \left(-\frac{1}{k-2} - 1 - \frac{k\binom{k}{\frac{k}{2}+1} + 2\binom{k}{\frac{k}{2}+1} - 2k^2 + 2k}{2k(k-2)}\right) \\
&= z_1 \left(-\frac{(k+2)\binom{k}{\frac{k}{2}+1}}{2k(k-2)}\right) = 1 \\
\iff \qquad z_1 &= -\frac{2k(k-2)}{(k+2)\binom{k}{\frac{k}{2}+1}} = (4-2k)\binom{k}{\frac{k}{2}}^{-1}. \qquad (3.26)
\end{aligned}
$$

Aus (3.26) und (3.24) 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 ist sowohl $1 \Longrightarrow 3$ gezeigt, als auch $2 \Longrightarrow 3$.
$\underline{3 \Longrightarrow 1}$:

$$
\begin{aligned}
z_0 = 2\binom{k}{\frac{k}{2}}^{-1}, &\qquad z_1 = (4-2k)\binom{k}{\frac{k}{2}}^{-1} \\
\Longrightarrow \quad z_\ell &= (-1)^{\ell-1}\left(\frac{1}{k}(4-2k)\binom{k}{\frac{k}{2}}^{-1} + (\ell-1)\left(2\binom{k}{\frac{k}{2}}^{-1} + \frac{1}{k}(4-2k)\binom{k}{\frac{k}{2}}^{-1}\right)\right)\binom{k}{\ell} \\
\Longrightarrow z_{\frac{k}{2}} &= (-1)^{\frac{k}{2}-1}\left(\frac{1}{k}(4-2k)\binom{k}{\frac{k}{2}}^{-1} + \left(\frac{k}{2}-1\right)\left(2\binom{k}{\frac{k}{2}}^{-1} + \frac{1}{k}(4-2k)\binom{k}{\frac{k}{2}}^{-1}\right)\right)\binom{k}{\frac{k}{2}} \\
&= (-1)^{\frac{k}{2}-1}\left(\frac{1}{2}(4-2k)\binom{k}{\frac{k}{2}}^{-1} + \left(\frac{k}{2}-1\right)2\binom{k}{\frac{k}{2}}^{-1}\right)\binom{k}{\frac{k}{2}} \\
&= (-1)^{\frac{k}{2}-1}\left((2-k)\binom{k}{\frac{k}{2}}^{-1} + (k-2)\binom{k}{\frac{k}{2}}^{-1}\right)\binom{k}{\frac{k}{2}}
\end{aligned}
$$

$$= (-1)^{\frac{k}{2}-1}(0)\binom{k}{\frac{k}{2}} = 0$$

Somit ist die Äquivalenz aller drei Aussagen bewiesen. □

Die im Fall 1 für den Kontrast bestimmte obere Schranke von

$$\alpha_{max} \leq \frac{4}{2^k k - 2^{k+1} + 4}$$

ist kleiner als

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

Demnach muss für eine optimale Lösung $z_0 > 0, z_1 < 0$ gelten.
Es ist bisher allerdings unklar, wie eine der Aussagen aus Lemma 3.23 direkt gezeigt werden kann. Blundo, D'Arco, De Santis und Stinson konnten in [7] jedoch durch die Verwendung von *kanonischen Matrizen* den optimalen Kontrast eines $(k-1,k)$-Schemas bestimmen, welcher den Wert

$$\alpha = \frac{4}{k}\binom{k}{\frac{k}{2}}^{-1}$$

hat. Die *kanonischen Matrizen* sind ähnlich zu den total symmetrischen Matrizen konzipiert, erfüllen jedoch eine weitere Bedingung. Da mit der aus Lemma 3.23 angegebenen Belegung dieser Kontrast erreicht wird, ist die angegebene Belegung optimal und eindeutig.
Für ungerade k liegt der optimale Kontrast bei

$$\alpha = \frac{2}{k}\binom{k-1}{\frac{k-1}{2}}^{-1},$$

wie in [7] nachgewiesen wird. Damit sind die Kontrastwerte α eines $(k-1,k)$-Schemas $\alpha = \Theta(2^{-k}k^{-1/2})$, also kleiner als bei einem (k,k)-Schema.

Das Lineare Programm $L(k,k)$

Für den Fall $n = k$ haben Naor und Shamir in [17] gezeigt, dass der optimale Kontrast α eines (k,k)-Schemas (auch (n,n)-Schema genannt) gleich $2^{-(k-1)}$ ist. Mit Hilfe des Linearen Programms $L(k,k)$ ist es jedoch einfacher diesen Wert zu bestimmen, da lediglich der maximale Zielfunktionswert bestimmt werden muss.
Für $n = k$ vereinfacht sich das Lineare Programm $L(k,n)$ aus Definition 3.8 zu:
Zielfunktion:

$$L(k,k) = \sum_{j=0}^{k-k}\binom{k-k}{j}\cdot\binom{k}{j}^{-1}\cdot(x_j - y_j) = x_0 - y_0 \longrightarrow \text{maximiere} \tag{3.27}$$

mit den Nebenbedingungen

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

$$\iff \quad \frac{x_\ell - y_\ell}{\binom{k}{\ell}} + \frac{x_{\ell+1} - y_{\ell+1}}{\binom{k}{\ell+1}} = 0.$$

Nun bestimmen wir den maximalen Funktionswert, indem wir eine Belegung für die Variablen $(x_0, \ldots, x_n, y_0, \ldots, y_n)$ angeben, die den maximalen Funktionswert liefert.
Da der maximale Zielfunktionswert immer positiv ist, muss $x_0 > y_0$ gelten. Nach Lemma 3.18 folgt daraus $y_0 = 0$. Desweiteren gilt $x_1 = 0$ oder $y_1 = 0$ nach diesem Lemma. Zusammen mit der Nebenbedingung 3 folgt daraus für $\ell = 0$

$$\begin{aligned} &\frac{x_0 - y_0}{\binom{k}{0}} + \frac{x_1 - y_1}{\binom{k}{1}} = 0 \\ \iff &x_1 - y_1 = -\binom{k}{1} \cdot x_0 \\ \iff &x_1 = 0 \text{ und } y_1 = \binom{k}{1} \cdot x_0. \end{aligned}$$

Wäre hier $y_1 = 0$, würde gegen die erste Nebenbedingung verstoßen werden, da $x_1 < 0$ wäre.
Wird diese Argumentation mit Nebenbedingung 3 für alle ℓ fortgeführt, ergibt sich die Belegung

$$x_j = \begin{cases} 0 & \text{für } j \text{ ungerade} \\ \binom{k}{j} \cdot x_0 & \text{für } j \text{ gerade,} \end{cases}$$

$$y_j = \begin{cases} \binom{k}{j} \cdot x_0 & \text{für } j \text{ ungerade} \\ 0 & \text{für } j \text{ gerade.} \end{cases}$$

Die Belegung der Variablen hängt somit von dem für x_0 gewählten Wert ab. Die Nebenbedingungen 1 und 3 werden bereits in dieser allgemeinen Form erfüllt, lediglich die zweite Nebenbedingung muss noch erfüllt werden:

$$\begin{aligned} &\sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} x_j = 1 \\ \iff \quad &\sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j} \cdot x_0 = 1 \end{aligned}$$

$$\begin{aligned}
&\iff && x_0 \cdot \sum_{\substack{j=0 \\ j \text{ gerade}}}^{k} \binom{k}{j} = 1 \\
&\iff && x_0 \cdot 2^{k-1} = 1 \\
&\iff && x_0 = 2^{-(k-1)}.
\end{aligned}$$

Somit sind alle Nebenbedingungen erfüllt, wenn $x_0 = 2^{-(k-1)}$ ist. Die Zielfunktion hat damit einen maximalen Wert von $x_0 + y_0 = 2^{-(k-1)} + 0 = 2^{-(k-1)}$. Nach Lemma 3.17 ist dies somit auch der maximal erzielbare Kontrast aller (k, k)-Schemata. Dies entspricht auch dem Wert, den Naor und Shamir in [17] nachweisen konnten.
Die berechnete Belegung ist die einzige, welche den optimalen Zielfunktionswert liefert, da sie direkt aus den Nebenbedingungen folgt.

3.3 Schlussbemerkungen

In diesem Kapitel wurde gezeigt, wie sich mit Hilfe von Hadamard-Matrizen kontrastoptimale $(2, n)$-Schemata konstruieren lassen. Ein Nachteil dieser Matrizen ist jedoch, dass sie nur für $n = 2^\ell, \ell \in \mathbb{N}$, definiert sind. Das vorgestellte Lineare Programm $L(2, n)$ besitzt diese Einschränkung nicht und kann daher für alle Werte von n genutzt werden, um kontrastoptimale $(2, n)$-Schemata zu konstruieren. Allerdings ist die Pixelexpansion des Linearen Programms höher, falls n eine Zweierpotenz ist, als die der Hadamard-Matrizen. Mit den Linearen Programmen lässt sich somit immer ein $(2, n)$-Schema bestimmen, auch wenn es bezüglich der Pixelexpansion nicht optimal ist.

Die Lösungen der Linearen Programme sind nicht immer eindeutig, wie der Fall $L(2, n)$ für ungerade n zeigt. Es ist zwar möglich für jedes Paar (k, n) eine optimale Lösung zu finden, jedoch können auch andere Lösungen existieren, die ebenfalls einen optimalen Kontrast liefern.

Darüber hinaus bezieht sich das Lineare Programm nur auf total symmetrische Matrizen. Es wurde gezeigt, dass die Menge der total symmetrischen Schemata der Lösungsmenge des Linearen Programms $L(k, n)$ entspricht. Demnach existiert für eine feste Lösung des Linearen Programms auch genau ein total symmetrisches Schema. Somit gibt es bei uneindeutigen optimalen Lösungen auch mehrere kontrastoptimale total symmetrische Schemata. Bei eindeutigen Lösungen hingegen, ist das entsprechende total symmetrische Schema auch das einzige, welches den optimalen Kontast liefert. Es könnten lediglich nicht total symmetrische Schemata existieren, die ebenfalls den optimalen Kontrast für ein festes Paar (k, n) liefern, wie es beispielsweise bei den Hadamard-Matrizen der Fall ist.

Alles in allem haben die Linearen Programme jedoch einen großen Vorteil: es reicht aus, den maximalen Zielfunktionswert für ein Paar $(k, n), 2 \leq k \leq n$, zu bestimmen, um den maximal erreichbaren Kontrast für alle möglichen (k, n)-Schemata zu ermitteln.

Hofmeister, Krause und Simon haben in [20] eine Tabelle angegeben, die den optimalen Kontrast einiger (k, n)-Schemata aufzeigt. Aus ihr lässt sich die Vermutung ableiten, dass der optimale Zielfunktionswert des Linearen Programms $L(k, n)$ für n gegen unendlich bei $4^{-(k-1)}$ liegt. Mit Hilfe von Approximationsverfahren lässt sich diese theoretische Grenze auch beweisen, was in dieser Arbeit jedoch nicht behandelt wurde. Hierzu sei auf die Arbeit von Krause und Simon [15] verwiesen.

$k\backslash n$	2	3	4	5	6	7	8	$\cdots$	100	$\cdots$	∞
2	1/2	1/3	1/3	3/10	3/10	2/7	2/7	$\cdots$	25/99	$\cdots$	1/4
3		1/4	1/6	1/8	1/10	1/10	2/21	$\cdots$	625/9702	$\cdots$	1/16
4			1/8	1/15	1/18	3/70	3/80	$\cdots$	425/25608	$\cdots$	1/64

Tabelle 3.1: optimaler Kontrast der (k, n)-Schemata, bestimmt durch den optimalen Zielfunktionswert von $L(k, n)$ (siehe [20])

4 Aktuelle Entwicklungen

Aus dem ursprünglichen Modell der Visuellen Kryptographie, das Naor und Shamir in [17] angegeben haben, lassen sich viele Verallgemeinerungen und Erweiterungen ableiten. In diesem Kapitel werden ausgewählte Verfahren überblicksmäßig vorgestellt.

4.1 Visuelle Kryptographie mit General Access Structures

Die (k, n)-Schemata aus Definition 2.4 ermöglichen es, ein Bild in n Folien aufzuteilen, so dass immer mindestens k Folien für die Rekonstruktion des Bildes benötigt werden. Bekommen also n Personen jeweils eine Folie, müssen mindestens k Personen kooperieren, um das Geheimnis zu erhalten. Alle Personen sind demnach gleichberechtigt, in dem Sinne, dass sie alle einen ähnlich großen Informationsgehalt auf den Folien bekommen. Somit ist es nicht möglich, einer einzelnen Person zu erlauben, das Geheimnis durch Kooperation mit weniger als $k - 1$ anderen zu rekonstruieren. Solche Szenarien sind in der Realität aber durchaus denkbar, wie das folgende Beispiel veranschaulicht.

Beispiel 4.1.
Um ein Atomkraftwerk in Betrieb zu nehmen, muss ein Einschaltcode für die Steuerung eingegeben werden. Damit niemand eigenmächtig den Reaktor einschalten kann, wird der Einschaltcode mittels Visueller Kryptographie verschlüsselt. Erst wenn mindestens 4 *Ingenieure ihre Folien zusammenlegen, soll der Einschaltcode sichtbar werden. Ist jedoch der Sicherheitsbeauftragte der Energiegesellschaft anwesend, soll dessen Folie mit einer Folie der Ingenieure die Rekonstruktion des Codes ermöglichen, da in diesem Fall davon ausgegangen wird, dass alle Sicherheitsvorschriften eingehalten werden.*

Durch eine Erweiterung der Definition 2.4 ist es möglich, die Visuelle Kryptographie auch in solchen Szenarien nutzen zu können. Dazu werden *General Access Structures* genutzt. Diese Verallgemeinerung der ursprünglichen (k, n)-Schemata wird von Ateniese, Blundo, De Santis und Stinson in [12] erstmals beschrieben.

Definition 4.1 - General Access Structure (GAS):
Sei $\Gamma = \{1, \ldots, n\}$ die Menge der n Personen, die an der Visuellen Kryptographie teilnehmen sollen (die Personen werden also durchnummeriert). Dann ist das Paar $(\Gamma_{qual}, \Gamma_{forb})$ eine General Access Structure, wenn gilt:

1. Die Menge Γ_{qual} beinhaltet die Mengen von Personen, welche das Geheimnis rekonstruieren dürfen und es gilt $\Gamma_{qual} \subseteq \mathcal{P}(\Gamma)$. Eine Menge aus Γ_{qual} heißt *qualifizierte Menge*.
2. Die Menge Γ_{forb} beinhaltet die Mengen von Personen, welche das Geheimnis nicht rekonstruieren dürfen und es gilt $\Gamma_{forb} \subseteq \mathcal{P}(\Gamma)$. Eine Menge aus Γ_{forb} heißt *verbotene Menge*.
3. $\Gamma_{qual} \cap \Gamma_{forb} = \emptyset$.

Definition 4.2 - essentielle Teilnehmer:
Ein Teilnehmer $P \in \Gamma$ heißt *essentiell*, falls eine Menge $X \subseteq \Gamma$ existiert, für die

$$X \cup \{P\} \in \Gamma_{qual} \qquad \text{und} \qquad X \notin \Gamma_{qual}$$

gilt.

Ein nicht-essentieller Teilnehmer muss also nicht an der Rekonstruktion des Geheimnisses mitwirken. Somit können wir davon ausgehen, dass alle Teilnehmer essentiell sind.

Definition 4.3 - starke General Access Structure:
Eine General Access Structure $(\Gamma_{qual}, \Gamma_{forb})$ heißt *stark*, wenn die folgenden drei Eigenschaften gelten:

1. $\Gamma_{qual} \cup \Gamma_{forb} = \mathcal{P}(\Gamma)$
2. Die Menge Γ_{qual} ist monoton wachsend, das heißt eine Obermenge einer qualifizierten Menge ist auch wieder eine qualifizierte Menge.
3. Die Menge Γ_{forb} ist monoton fallend, das heißt jede Teilmenge einer verbotenen Menge ist auch wieder eine verbotene Menge.

Definition 4.4 - Basis einer starken GAS:
Sei $(\Gamma_{qual}, \Gamma_{forb})$ eine starke General Access Structure. Dann heißt

$$\Gamma_0 = \{A \in \Gamma_{qual} : A' \notin \Gamma_{qual} \text{ für alle } A' \subset A\}$$

Basis der starken General Access Structure $(\Gamma_{qual}, \Gamma_{forb})$. Die Basis ist somit die Menge der minimal qualifizierten Mengen.

Für eine starke GAS ist es daher ausreichend Γ_0 anzugeben, da hieraus alle qualifizierten Mengen gebildet werden können. Alle Mengen, die nicht aus Γ_0 gebildet werden können,

sind folglich verbotene Mengen.
Um nun die Visuelle Kryptographie mit den General Access Structures zu verbinden, dient die folgende Definition.

Definition 4.5 - $(\Gamma_{qual}, \Gamma_{forb}, m)$-Schema:
Sei $(\Gamma_{qual}, \Gamma_{forb})$ eine GAS über einer Menge Γ von n Teilnehmern.
Ein $(\Gamma_{qual}, \Gamma_{forb}, m)$-Schema der Visuellen Kryptographie besteht aus zwei Multimengen von Boolschen $n \times m$-Matrizen $\widetilde{C_0}$ und $\widetilde{C_1}$, für die ein Wert $\alpha(m)$ und eine Menge $\{(X, t_X)\}_{X \in \Gamma_{qual}}$ existieren, so dass die folgenden drei Bedingungen erfüllt sind:

1. Sei $X = \{i_1, \ldots, i_p\} \in \Gamma_{qual}$. Für jede Matrix $M \in \widetilde{C_0}$ gilt:
   Sei v der Vektor, der aus der komponentenweisen Disjunktion der p Zeilen $i_1, \ldots, i_p$ von M entsteht. Dann gilt: $H(v) \leq t_X - \alpha(m) \cdot m$.

2. Sei $X = \{i_1, \ldots, i_p\} \in \Gamma_{qual}$. Für jede Matrix $M \in \widetilde{C_1}$ gilt:
   Sei v der Vektor, der aus der komponentenweisen Disjunktion der p Zeilen $i_1, \ldots, i_p$ von M entsteht. Dann gilt: $H(v) \geq t_X$.

3. Sei $X = \{i_1, \ldots, i_p\} \in \Gamma_{forb}$. Die zwei Multimengen $\widetilde{D_0}$ und $\widetilde{D_1}$ von $p \times m$-Matrizen, welche aus $\widetilde{C_0}$ und $\widetilde{C_1}$ hervorgehen, indem man sich bei den enthaltenen Matrizen auf die Zeilen $i_1, \ldots, i_p$ beschränkt, enthalten die selben Matrizen mit den selben Häufigkeiten.

Analog zur Definition 2.4 bilden die ersten beiden Bedingungen die Kontrastbedingung, die dritte hingegen die Sicherheitsbedingung. Die Codierung erfolgt ebenso analog zu den bisherigen (k, n)-Schemata. Ein weißes (schwarzes) Pixel wird codiert, indem man zufällig eine Matrix M aus $\widetilde{C_0}$ ($\widetilde{C_1}$) wählt. Die Zeile i von M gibt dann die Subpixel-Anordnung auf der Folie des Teilnehmers i an.
Der Schwellwert d eines (k, n)-Schemas nach Definition 2.4 ist stets konstant. Durch die Verallgemeinerung zu einem $(\Gamma_{qual}, \Gamma_{forb}, m)$-Schema gibt es für jede qualifizierte Menge $X \in \Gamma_{qual}$ einen anderen Schwellwert t_X. Daraus ergibt sich die Menge $\{(X, t_X)\}_{X \in \Gamma qual}$.
Die (k, n)-Schemata nach Definition 2.4 ergeben sich als Spezialfall eines $(\Gamma_{qual}, \Gamma_{forb}, m)$-Schemas mit einer starken GAS, für die $\Gamma_0 = \{B \subseteq \mathcal{P}(\Gamma) : |B| = k\}$ gilt.
Für die Definition 4.5 ist die zugrunde liegende GAS nicht notwendigerweise eine starke GAS. Es ist jedoch leicht zu sehen, dass jede Teilmenge einer verbotenen Menge auch wieder eine verbotene Menge darstellt. Somit ist Γ_{forb} monoton fallend. Desweiteren kann keine Obermenge einer qualifizierten Menge eine verbotene Menge sein. Eine gegebene GAS $(\Gamma_{qual}, \Gamma_{forb})$ lässt sich somit leicht in eine starke GAS $(\Gamma'_{qual}, \Gamma'_{forb})$ einbetten. Dabei muss $\Gamma_{qual} \subseteq \Gamma'_{qual}$ und $\Gamma_{forb} \subseteq \Gamma'_{forb}$ gelten. Die einfachste Möglichkeit für diese Einbettung ist, $(\Gamma'_{qual}, \Gamma'_{forb})$ so zu wählen, dass Γ_0 die Basis dieser starken GAS darstellt, wobei Γ_0 die minimalen qualifizierten Mengen von Γ_{qual} enthält. Da also zu jeder GAS eine starke GAS angegeben werden kann, reicht es aus, nach $(\Gamma_{qual}, \Gamma_{forb}, m)$-Schemata

mit möglichst hohem Kontrast zu suchen, bei denen eine starke GAS zugrunde liegt. Ateniese, Blundo, De Santis und Stinson geben in [12] und [10] verschiedene Verfahren an, mit denen $(\Gamma_{qual}, \Gamma_{forb}, m)$-Schemata erzeugt werden können. Beispielsweise verwenden sie dafür *cumulative arrays*. Desweiteren zeigen sie, wie kleinere Schemata genutzt werden können, um ein größeres Schema zu konstruieren. Für detailiertere Informationen hierzu, sei auf die entsprechende Literatur [12] und [10] verwiesen.

4.2 Extended Visual Cryptography Schemes - EVCS

Bei der erweiterten Visuellen Kryptographie, kurz EVCS, soll bereits auf den einzelnen Folien ein Bild zu erkennen sein. Dies soll die Existenz einer verschlüsselten Nachricht verbergen. Die Idee dazu wird bereits von Naor und Shamir in [17] beschrieben, jedoch geben sie noch kein mathematisches Modell für entsprechende Schemata an. Aufbauend auf ihren Arbeiten [12] und [10] beschreiben Ateniese, Blundo, De Santis und Stinson in [11] ein allgemeines Konstruktionsprinzip für EVCS. Dabei verwenden sie General Access Structures.
Sei $(\Gamma_{qual}, \Gamma_{forb})$ eine GAS über einer Menge $\Gamma = \{1, \ldots, n\}$ von Teilnehmern. Dann soll auf jeder der n zu erzeugenden Folien ein sogenanntes Originalbild zu erkennen sein, das nichts über das geheime Bild verrät. Im Allgemeinen sind die n Originalbilder dabei paarweise verschieden. Insgesamt werden also $n+1$ Bilder benötigt. Legen die Teilnehmer einer qualifizierten Menge ihre Folien übereinander, soll wie üblich das geheime Bild zu erkennen sein. Da durch die Originalbilder bereits die Farben der Pixel vorgegeben sind, kann das geheime Bild nicht unabhängig von den Originalbildern codiert werden. Somit reichen die zwei Kollektionen $\widetilde{C_0}$ und $\widetilde{C_1}$ nicht mehr für die Codierung aus. Für jede mögliche Kombination von Pixelfarben wird daher eine eigene Kollektion genutzt.
Im Folgenden bezeichne w ein weißes Pixel, b hingegen ein schwarzes. Ein Pixel des geheimen Bildes mit Farbe $c \in \{b, w\}$ wird codiert, indem eine Matrix aus der Kollektion $C_c^{c_1,\ldots,c_n}$ gewählt wird, wobei c_i der Farbe des entsprechenden Pixels des Originalbildes von Teilnehmer i entspricht, mit $c_i \in \{b, w\}$ und $i = 1, \ldots, n$. Der tiefgestellte Index c gibt demnach die Farbe eines Pixels des geheimen Bildes an, die hochgestellten Indizes $c_1, \ldots, c_n$ stehen für die Pixelfarben auf den jeweiligen Originalbildern. Die gewählte Matrix legt wie bisher bei der Visuellen Kryptographie die Subpixel-Anordnung auf den Folien fest. Für alle möglichen Pixelfarbkombinationen der Teilnehmer ergeben sich somit insgesamt 2^n Kollektionenpaare $(C_w^{c_1,\ldots,c_n}, C_b^{c_1,\ldots,c_n})$. Ateniese, Blundo, De Santis und Stinson haben in [11] gezeigt, dass man zu jedem Schema der erweiterten Visuellen Kryptographie ein Schema konstruieren kann, in dem alle Matrizen die selbe Dimension und damit die selbe Pixelexpansion haben. Somit kann man davon ausgehen, dass alle Matrizen $n \times m$-Matrizen sind. Ein Schema der erweiterten Visuellen Kryptographie wird damit wie folgt definiert.

Definition 4.6 - $(\Gamma_{qual}, \Gamma_{forb}, m)$-EVCS:
Sei $(\Gamma_{qual}, \Gamma_{forb})$ eine GAS über einer Menge Γ von n Teilnehmern.

Ein $(\Gamma_{qual}, \Gamma_{forb}, m)$-Schema der erweiterten Visuellen Kryptographie besteht aus einer Familie von 2^n Paaren von Multimengen Boolscher $n \times m$-Matrizen $(C_w^{c_1,\ldots,c_n}, C_b^{c_1,\ldots,c_n})$, mit $c_1, \ldots, c_n \in \{b, w\}$, für die ein Wert $\alpha(m)$ und eine Menge $\{(X, t_X)\}_{X \in \Gamma_{qual}}$ existieren, so dass die folgenden vier Bedingungen erfüllt sind:

1. Sei $X = \{i_1, \ldots, i_p\} \in \Gamma_{qual}$ und $c_1, \ldots, c_n \in \{b, w\}$. Für jede Matrix $M \in C_w^{c_1,\ldots,c_n}$ gilt:
   Sei v der Vektor, der aus der komponentenweisen Disjunktion der p Zeilen $i_1, \ldots, i_p$ von M entsteht. Dann gilt: $H(v) \leq t_X - \alpha(m) \cdot m$.

2. Sei $X = \{i_1, \ldots, i_p\} \in \Gamma_{qual}$ und $c_1, \ldots, c_n \in \{b, w\}$. Für jede Matrix $M \in C_b^{c_1,\ldots,c_n}$ gilt:
   Sei v der Vektor, der aus der komponentenweisen Disjunktion der p Zeilen $i_1, \ldots, i_p$ von M entsteht. Dann gilt: $H(v) \geq t_X$.

3. Sei $X = \{i_1, \ldots, i_p\} \in \Gamma_{forb}$ und $c_1, \ldots, c_n \in \{b, w\}$. Die zwei Kollektionen $(D_w^{c_1,\ldots,c_n}, D_b^{c_1,\ldots,c_n})$ von $p \times m$-Matrizen, welche aus $(C_w^{c_1,\ldots,c_n}, C_b^{c_1,\ldots,c_n})$ hervorgehen, indem man sich bei den enthaltenen Matrizen auf die Zeilen $i_1, \ldots, i_p$ beschränkt, enthalten die selben Matrizen mit den selben Häufigkeiten.

4. Für alle $i \in \{1, \ldots, n\}$ und alle $c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n \in \{b, w\}$ gilt:

$$\min_{M \in \mathcal{M}_b} H(M_i) > \min_{M \in \mathcal{M}_w} H(M_i)$$

   mit $\mathcal{M}_b = \bigcup_{c_1,\ldots,c_{i-1},c_{i+1},\ldots,c_n \in \{b,w\}} C_w^{c_1,\ldots,c_{i-1},b,c_{i+1},\ldots,c_n \in \{b,w\}}$
   und $\mathcal{M}_w = \bigcup_{c_1,\ldots,c_{i-1},c_{i+1},\ldots,c_n \in \{b,w\}} C_w^{c_1,\ldots,c_{i-1},w,c_{i+1},\ldots,c_n \in \{b,w\}}$.

Die ersten drei Bedingungen entsprechen den Bedingungen aus Definition 4.5, angepasst an die erweiterte Visuelle Kryptographie. Die vierte Bedingung garantiert, dass ein Teilnehmer das Originalbild auf seiner Folie erkennen kann.
Neben dieser Definition geben Ateniese, Blundo, De Santis und Stinson in [11] auch Verfahren an, mit denen $(\Gamma_{qual}, \Gamma_{forb}, m)$-EVCS erzeugt werden können. Diese Verfahren beruhen auf Färbungen von Hypergraphen. Details hierzu sind in der entsprechenden Literatur [11] nachzulesen.

4.2.1 S-EVCS

Durch die EVCS kann die Existenz einer verschlüsselten Nachricht verborgen werden. Jedoch ist es für eine Menge von Teilnehmern immer noch möglich zu entscheiden, ob sie eine qualifizierte Menge sind oder nicht, da nur beim Übereinanderlegen von Folien einer qualifizierten Menge das geheime Bild sichtbar wird. Möchte man verhindern, dass eine nicht qualifizierte Menge von Teilnehmern feststellen kann, ob sie eine qualifizierte Menge bilden oder nicht, können S-EVCS verwendet werden. Dabei entstehen auch für

nicht qualifizierte Mengen von Teilnehmern Bilder beim Übereinanderlegen der Folien, die jedoch nichts mit dem geheimen Bild zu tun haben müssen.
Die Idee von S-EVCS wird erstmalig von Droste in [19] beschrieben. Desweiteren gibt Droste ein entsprechendes (k, k)-Schema an, dessen Optimalität bezüglich der Pixelexpansion in [4] von Klein und Wessler nachgewiesen wird.

4.3 Visuelle Kryptographie mit Graustufenbildern - GVCS

Naor und Shamir geben in [17] neben der Definition eines (k, n)-Schemas und der Idee der EVCS auch eine mögliche Erweiterung der Visuellen Kryptographie für Graustufenbilder an. Graustufenbilder enthalten neben den schwarzen und weißen Pixeln auch graue Pixel mit bestimmten Abstufungen. Die grauen Pixel müssen bei der Visuellen Kryptographie gesondert behandelt werden.
Naor und Shamir schlagen in [17] die Verwendung von Kreisen als Codierung der Pixel des geheimen Bildes vor. Jedes Pixel soll durch einen Kreis dargestellt werden, der zur Hälfte weiß, zur anderen Hälfte schwarz gefärbt ist. Durch Rotation der Kreise ist es möglich, beliebige Grautöne darzustellen. Das folgende Beispiel verdeutlicht dies.

Beispiel 4.2. *Ein graues Pixel wird entsprechend der Idee von Naor und Shamir durch Kreise codiert. Durch die unterschiedlichen Rotationswinkel lassen sich beliebige Grautöne darstellen:*

Folie 1   *Folie* 2

übereinander gelegt 

Je größer der weiße Teil des rekonstruierten Pixels ist, desto heller wirkt das Pixel.

Sind die Kreise klein genug, nimmt das menschliche Auge die beim Übereinanderlegen entstehenden Kreise als graue Pixel wahr. Das Problem bei diesem Verfahren ist jedoch, dass es technisch sehr schwer ist, die Kreise entsprechend klein zu drucken.
Durch eine Erweiterung der Definition 4.5 ist es möglich, die Visuelle Kryptographie auch für Graustufenbilder zu nutzen, wie Blundo, De Santis und Naor in [6] zeigen. Dazu werden wie bisher unterschiedliche Matrizenklassen genutzt. Allerdings ist hier für jede Graustufe eine Matrizenklasse nötig.

Definition 4.7 - $(\Gamma_{qual}, \Gamma_{forb}, m, g)$-GVCS:
Sei $(\Gamma_{qual}, \Gamma_{forb})$ eine GAS über einer Menge Γ von n Teilnehmern und $g \geq 2$ eine natürliche Zahl.
Ein $(\Gamma_{qual}, \Gamma_{forb}, m, g)$-Schema der Visuellen Kryptographie für Graustufenbilder besteht aus g Multimengen von Boolschen $n \times m$-Matrizen $\widetilde{C_0}, \ldots, \widetilde{C_{g-1}}$, für welche die Werte $\alpha_0, \ldots, \alpha_{g-2}$ und Mengen $\{X, t_{i,X}\}_{X \in \Gamma_{qual}}$ existieren, so dass für alle $i \in \{0, \ldots, g-2\}$ die folgenden zwei Bedingungen erfüllt sind:

1. Sei $X = \{j_1, \ldots, j_p\} \in \Gamma_{qual}$. Für jede Matrix $M \in \widetilde{C}_i$ gilt:
   Sei v der Vektor, der aus der komponentenweisen Disjunktion der p Zeilen $j_1, \ldots, j_p$ von M entsteht. Dann gilt $H(v) \leq t_{i,X} - \alpha_i \cdot m$, während für alle $M \in \widetilde{C_{i+1}}$ die Bedingung $H(v) \geq t_{i,X}$ gilt.

2. Sei $X = \{i_1, \ldots, i_p\} \in \Gamma_{forb}$. Die g Multimengen $\widetilde{D_0}, \ldots, \widetilde{D_{g-1}}$ von $p \times m$-Matrizen, welche aus $\widetilde{C_0}, \ldots, \widetilde{C_{g-1}}$ hervorgehen, indem man sich bei den enthaltenen Matrizen auf die Zeilen $j_1, \ldots, j_p$ beschränkt, enthalten die selben Matrizen mit den selben Häufigkeiten.

Die erste Bedingung ist, wie bei den bisherigen Definitionen auch, die Kontrastbedingung. Allerdings gibt es nun für jede Graustufe einen unterschiedlichen Kontrastwert. Dies ist nötig, damit jeder Teilnehmer alle Graustufen korrekt erkennen kann. Die zweite Bedingung garantiert die Sicherheit des Systems.
Basierend auf dieser Definition gibt MacPherson in [14] verschiedene Verfahren an, mit denen GVCS erstellt werden können. Unter anderem werden hierfür *cumulative arrays* und ein Dekompositions-Ansatz genutzt, analog zu den Verfahren von Ateniese, Blundo, De Santis und Stinson in [12] und [10].
Ein weiteres Verfahren für Graustufenbilder in Kombination mit der erweiterten Visuellen Kryptographie wird von Nakajima und Yamaguchi in [16] vorgestellt. Dort werden zusätzlich zur Codierung auch Verfahren zur Kontrastverstärkung angewandt. Dadurch erreicht man zwar sehr gute Kontrastwerte und eine geringe Pixelexpansion, das Verfahren ist jedoch nicht mehr sicher.

4.4 Visuelle Kryptographie mit Farbbildern - CVCS

Farbbilder stellen den momentanen Forschungsschwerpunkt innerhalb der Visuellen Kryptographie dar. Verheul und Tilborg stellen in [9] bereits 1997 ein Verfahren und ein mathematisches Modell für farbige Visuelle Kryptographie vor. Ähnlich zu der von Naor und Shamir in [17] vorgestellten Idee für Graustufenbilder, werden hier die Pixel durch Kreise codiert. Ein Kreis wird dabei in c Sektoren eingeteilt, wobei c die Anzahl an Farben des geheimen Bildes ist. Mit jedem dieser Sektoren wird eine Farbe assoziiert. Bei der Codierung des geheimen Bildes werden einige Sektoren mit den entsprechenden Farben, alle restlichen Sektoren schwarz gefärbt. Legen die Teilnehmer ihre Folien übereinander, werden die meisten Sektoren durch die schwarz gefärbten überdeckt. Die Farbe des ursprünglich codierten Pixels ist jedoch auf allen Folien vorhanden und wird daher nicht überdeckt. Dadurch wird ein Pixel korrekt rekonstruiert. Bei diesem Verfahren besteht, wie auch bei den Graustufenbildern, die technische Schwierigkeit darin, die Kreise entsprechend klein auf die Folien zu drucken. Daher ist es in der Praxis (noch) nicht anwendbar.
Ein ähnliches Verfahren, das allerdings wieder auf Subpixeln und Matrizen beruht, wurde von Yang und Laih in [8] vorgestellt. Hier wird jedes Subpixel mit einer Farbe assozi-

iert. Bei der Codierung wird, analog zum oben beschriebenen Verfahren, nur ein Teil der Subpixel mit Farben gefärbt, die restlichen Subpixel werden schwarz gefärbt. Beim Übereinanderlegen der Folien verdecken also auch hier die schwarzen Subpixel falsche Farben und die ursprüngliche Farbe wird korrekt rekonstruiert. Yang und Laih führen die farbige dabei auf die schwarz-weiße Visuelle Kryptographie zurück und benutzen für die Konstruktion eines CVCS die Basismatrizen eines (k, n)-Schemas. Desweiteren zeigen Yang und Laih in [8], dass auch die Basismatrizen eines $(\Gamma_{qual}, \Gamma_{forb}, m)$-Schemas nach Definition 4.5 genutzt werden können, um ein entsprechendes CVCS für eine General Access Structure zu konstruieren.
In [2] stellt Klein ein Verfahren vor, das mit Farbmodellen arbeitet. Beim Übereinanderlegen der Folien kommt es zu subtraktiver Farbmischung, wenn sich zwei farbige Subpixel überlagern. Liegen zwei farbige Subpixel nebeneinander, kommt es hingegen zu additiver Farbmischung (RGB-Farbmodell vorausgesetzt). Weder das Verfahren von Verheul und Tilborg, noch das Verfahren von Yang und Laih berücksichtigen dies, da jeweils nur eine Farbe beim Übereinanderlegen der Folien für ein Pixel entstehen kann. Klein nutzt in [2] hingegen aus, dass sich die Farben der Pixel des geheimen Bildes durch Farbmischungen auf den Folien ergeben. Allerdings ist durch die Farbmischung der Begriff des Kontrastes der schwarz-weißen Visuellen Kryptographie nicht direkt auf CVCS übertragbar. Deshalb definiert Klein zum einen den Abstand zweier Farben zueinander, zum anderen die Güte eines CVCS. Für diese Definitionen kann Klein in [2] auch optimale Schemata angeben. Ähnlich zu Yang und Laih lässt sich Kleins Verfahren auch auf die schwarz-weiße Visuelle Kryptographie zurückführen. Allerdings ist die daraus resultierende Güte recht niedrig und die Pixelexpansion recht hoch.
Eine neue Methode um CVCS zu konstruieren, 2010 veröffentlicht, beschreiben Koga und Ishihara in [13]. Um ein (t, n)-CVCS für K Farben zu konstruieren, betrachten sie K homogene Polynome vom Grad n, welche in Basismatrizen überführt werden können. Diese Basismatrizen können anschließend genutzt werden, um das eigentliche (t, n)-CVCS zu erstellen. Es ist allerdings noch unklar, wie die homogenen Polynome optimiert werden können, um einen hohen Kontrast garantieren zu können. Für die Fälle $t = 2, 3, n-1, n$ werden bereits Schemata angegeben und die entsprechenden Kontrastwerte und Pixelexpansionen bestimmt. Dabei erhalten Koga und Ishihara bessere Werte als bisher bekannt waren.
Für mathematische Beschreibungen und konkrete Ergebnisse der hier genannten Verfahren sei auf die Literatur [2], [13], [9], und [8] verwiesen.

Literaturverzeichnis

[1] Adi Shamir: *How to Share a Secret.* In: *Communications of the ACM*, Band 22, Seiten 612–613. 1979.

[2] Andreas Klein: *Farbige Visuelle Kryptographie*, Mathematische Schriften Kassel 2001.

[3] Andreas Klein: *Visuelle Kryptographie.* Springer-Verlag, 2007.

[4] Andreas Klein und Markus Wessler: *Extended Visual Cryptography Schemes.* In: *Information and Computation*, Band 205, Seiten 716–732. 2007.

[5] Carlo Blundo, Alfredo De Santis und Douglas R. Stinson: *On the Contrast in Visual Cryptography Schemes.* In: *Journal of Cryptology*, Band 12, Seiten 261–289. 1996.

[6] Carlo Blundo, Alfredo De Santis und Moni Naor: *Visual cryptography for grey level images.* In: *Information Processing Letters*, Band 75, Seiten 255–259. 2000.

[7] 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.

[8] Ching-Nung Yang und Chi-Sung Laih: *New Colored Visual Secret Sharing Schemes.* In: *Designs, Codes and Cryptography*, Band 20, Seiten 325–336. 2000.

[9] Eric R. Verheul und Henk C. A. van Tilborg: *Construction and Properties of k out of n Visual Secret Sharing Schemes.* In: *Designs, Codes and Cryptography*, Band 11, Seiten 179–196. 1997.

[10] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis und Douglas R. Stinson: *Constructions and Bounds for Visual Cryptography.* In: *Automata, Languages and Programming*, Band 1099 der Reihe *Lecture Notes in Computer Science*, Seiten 416–428, 1996.

[11] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis und Douglas R. Stinson: *Extended Schemes for Visual Cryptography.* 1996.

[12] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis und Douglas R. Stinson: *Visual Cryptography for General Access Structures.* In: *Information and Computation*, Band 129, Seiten 86–106. 1996.

[13] Hiroki Koga und Takeru Ishihara: *A general method for construction of threshold visual secret sharing schemes for color images.* In: *Designs, Codes and Cryptography*, Seiten 1–27. 2010.

[14] Lesley Anne MacPherson: *Grey Level Visual Cryptography for General Access Structures*, 2002. Masterarbeit, University of Waterloo, Ontario, Canada.

[15] 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.

[16] Mizuho Nakajima und Yasushi Yamaguchi: *Extended Visual Cryptography for natural images.* In: *Journal of WSCG*, Band 10, Seiten 303–310. 2002.

[17] 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.

[18] Philip A. Eisen und Douglas R. Stinson: *Threshold Visual Cryptography Schemes with Specified Whiteness Levels of Reconstructed Pixels.* In: *Designs, Codes and Cryptography*, Band 25, Seiten 15–61. 2001.

[19] Stefan Droste: *New Results on Visual Cryptography.* In: *Proceedings of the Conference on Advances in Cryptology – CRYPTO '96*, Band 1109 der Reihe *Lecture Notes in Computer Science*, Seiten 401–415, 1996.

[20] Thomas Hofmeister, Matthias Krause und Hans U. Simon: *Contrast-Optimal k out of n Secret Sharing Schemes in Visual Cryptography.* In: *Proceedings of the Conference on Computing and Combinatorics – COCOON '97*, Band 1276 der Reihe *Lecture Notes in Computer Science*, Seiten 176–185, 1997.

[21] Yan Gao: *Visuelle Kryptographie*, 2008. Diplomarbeit, Technische Universität Chemnitz.

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 Bachelorarbeit 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: .....
Juhnke

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