Contents

An Approach for Determining Optimal Contrast in Visual Cryptography

Jakob Juhnke[1], Hanno Lefmann[1], and Volker Strehl[2]

[1]Fakultät für Informatik, TU Chemnitz, 09111 Chemnitz, Germany,

[2]Department Informatik, Technische Fakultät,
Friedrich-Alexander-Universität Erlangen-Nürnberg,
91058 Erlangen, Germany

Abstract: Naor and Shamir introduced in 1994 a secret sharing scheme in Visual Cryptography, where, given $2 \leq k \leq n$, among n transparencies any k of these put on each other give complete information, however, less than k transparencies give no information. These (k, n)-schemes are constructed by encoding black and white pixels into subpixels via appropriate $0, 1$-matrices. Schemes with optimal contrast are rarely known. We present an approach towards determining the largest possible contrast of such schemes, and apply this to certain pairs (k, n).

1 Introduction

Naor and Shamir [7] introduced a secret sharing scheme in Visual Cryptography. Given $k \leq n$, there are n transparencies, that are distributed among n people. Any k of these transparencies put on each other provide by recognition through the eye the (secret) information, however, less than any k of these transparencies provide no information. Such a system is called (k, n)-*scheme.*

One can construct such schemes by using $0, 1$-matrices. Given are two families C_0 and C_1 of $0, 1$-matrices, all of dimension $n \times m$. Each pixel of the secret is transformed into n collections of subpixels in the same position on each of the n transparencies. To encode a white pixel, uniformly at random a matrix from C_0 is chosen, else, to encode a black pixel, uniformly at random a matrix from C_1 is chosen. The pixel on transparencies $i = 1, \ldots, n$ gets the i'th row of the chosen matrix as an array of subpixels, with the subpixels arranged in a rectangle, say. Here a "1" corresponds to a black subpixel, and a "0" to a white one. Stacking ℓ transparencies on top of each other means that ℓ subpixels in the same position produce a “1” if at least one of them is “1”, else it gives “0”. This is nothing but parallel boolean disjunction for all subpixels. A pixel will be visually identified as black if there are many (say at least d) black subpixels, otherwise (say at most $d - \alpha m$ black subpixels) it will be identified as white. The difference between black and white is thus given by αm, and α is called the *contrast*. We make this more precise as follows.

For boolean vectors and matrices we will use the usual notion of Hamming-weight (shortly: *weight*) and the operation of parallel (component-wise) disjunction for vectors (matrices, resp.) of the same format.

Definition 1 *A (k, n)-scheme (in Visual Cryptography) with parameters (d, α) consists of two families C_0 and C_1 of boolean $(n \times m)$-matrices having the following properties:*

1. *For each matrix M from C_0 the parallel disjunction of any k rows of M gives a vector of weight $\leq d - \alpha m$.* (contrast condition 1).
2. *For each matrix M from C_1 the parallel disjunction of any k rows of M gives a vector of weight $\geq d$.* (contrast condition 2).
3. *For all subsets $\{i_1, \ldots, i_q\} \subset \{1, \ldots, n\}$ with $q < k$, the families of $(q \times m)$-matrices D_0 und D_1, obtained by restricting the matrices in C_0 und C_1 to their submatrices to rows $i_1, \ldots, i_q$, contain the same matrices with the same relative frequencies.* (security condition).

In Definition 1 the parameter d is called *threshold*, as black pixels are identified by the occurrence of at least d black subpixels, while white pixels are identified by at most $d - \alpha m$ black subpixels. The parameter α is called *contrast*. The larger the contrast α is, the better is the discrimination between black and white pixels. The general goal is to determine (k, n)-schemes with largest possible contrast.

Naor and Shamir [7] constructed (k, k)-schemes with optimal contrast $2^{-(k-1)}$ for any $k \geq 2$, which is also an upper bound on the optimal contrast of any (k, n)-scheme. Extending work of Droste [3], Hofmeister, Krause, and Simon [4] determined the optimal contrast of $(2, n)$-schemes to be $n/(4(n-1))$ for n even. For $(3, n)$-schemes (n divisible by 4) they proved that the optimal contrast is $n^2/(16(n-1)(n-2))$. In [4] it is shown that one can restrict attention to families of totally symmetric matrices. A matrix is *totally symmetric* if all columns with the same weight occur with the same frequency. They were able to transform the problem of determining optimal (k,n)-schemes to the problem of solving the following linear program.

Definition 2 *The linear program $L(k,n)$ with $n \geq 2$ und $k \in \{2,\ldots,n\}$ for the variables $(x,y) = ((x_0,\ldots,x_n),(y_0,\ldots,y_n))$ is given by the target function*
$L(k,n) = \sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) \longrightarrow$ *maximize*
subject to the feasibility conditions:

1. *x and y are probability distributions on $\{0,\ldots,n\}$*
2. $\sum_{j=\ell}^{n-k+\ell+1} \binom{n-k+1}{j-\ell} \cdot \binom{n}{j}^{-1} \cdot (x_j - y_j) = 0 \qquad \ell = 0,\ldots,k-1.$

Any solution $((x_0,\ldots,x_n),(y_0,\ldots,y_n))$ to $L(k,n)$ determines the families C_0 and C_1 of all totally symmetric matrices, for which any boolean column vector of weight j occurs with relative frequency x_j (y_j, resp.) in every matrix from C_0 (C_1, resp.), $j = 0,\ldots,n$. The contrast of this (k,n)-scheme is equal to the value of the target function of $L(k,n)$, compare [4].

No closed expression for the optimal target value $L_{opt}(k,n)$ of $L(k,n)$ is known. In [4] it has been conjectured that $\lim_{n\to\infty} L_{opt}(k,n) = 4^{-(k-1)}$ for fixed $k \geq 2$. Using Chebyshev polynomials and results from approximation theory, Krause and Simon [6] have shown that for any $2 \leq k \leq n$:

$$4^{-(k-1)} \leq L_{opt}(k,n) \leq 4^{-(k-1)} \cdot \frac{n^k}{n(n-1)\cdots(n-k+1)}.$$

However, for k close to n these lower and upper bounds are quite apart.

Blundo et al. [2] determined the optimal contrast of $(n-1,n)$-schemes and $(3,n)$-schemes for any $n \geq 4$. They also presented $(4,n)$- and $(5,n)$-schemes of contrast asymptotically equal to $1/64$ and $1/256$, respectively, for which they conjectured optimality. All these calculations are rather lengthy.

Here we use another approach. The algebraic dependencies in the security condition (2.) of the linear program $L(k,n)$ will be transformed using hypergeometric functions to get some "nice" representation of the variables in terms of basis variables. With this one can derive certain properties of optimal solutions to $L(k,n)$. In this work in progress, having developed this machinery, we apply our approach to $(k-j,k)$-schemes for $j = 0,1,2$. It turns out that the cases $j = 0,1$ are now simple, while the case $j = 2$ still needs some further consideration to determine the optimal contrast precisely.

2 Properties of the Linear Program

We recall some properties of the linear program $L(k,n)$ from [4].

Lemma 1 ([4]) *Let $(x,y) = ((x_0,\ldots,x_n),(y_0,\ldots,y_n))$ be an optimal solution to the linear program $L(k,n)$. Then the target value of $L(k,n)$ is positive and the vectors x,y are orthogonal.*

Setting $z = x - y$ (component-wise) we recover x and y from z by $x = z^+ = \max(z,0)$, $y = z^- = -\min(z,0)$ (component-wise), where 0 is the zero vector. This allows us to reformulate the linear program $L(k,n)$ using the z-variables:

Definition 3 *The linear program $L(k,n)_z$ with $n \geq 2$ und $k \in \{2,\ldots,n\}$ for the variables $(z_0,\ldots,z_n)$ is given by the target function*

$$L(k,n)_z = \sum_{j=0}^{n-k} \binom{n-k}{j} \cdot \binom{n}{j}^{-1} \cdot z_j \longrightarrow \textit{maximize}$$

subject to the feasibility conditions:

1. *z^+ and z^- are probability distributions on $\{0,\ldots,n\}$*
2. $\sum_{j=\ell}^{n-k+\ell+1} \binom{n-k+1}{j-\ell} \cdot \binom{n}{j}^{-1} \cdot z_j = 0 \qquad \ell = 0,\ldots,k-1.$

Optimal solutions z to $L(k,n)_z$ then can be transformed into optimal solutions (x,y) to $L(k,n)$ by setting $x = \max(z,0)$, $y = -\min(z,0)$.

In the following we will only deal with the linear program $L(k,n)_z$, and we derive some crucial properties of it. We will make use of tools from the field of hypergeometric functions, see, e.g., [1] for details.

Definition 4 *Let $a_1,\ldots,a_p,b_1,\ldots,b_q,z \in \mathbb{C}$ with $b_i \notin \{0,-1-2,\ldots\}$ for $i = 1,\ldots,q$. The* hypergeometric function *${}_pF_q$ is defined as the formal series*

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

where $(c)_n := c \cdot (c+1) \cdot \ldots \cdot (c+n-1)$ is the Pochhammer symbol.

The following facts are needed in our computations.

Lemma 2 (Chu-Vandermonde) *Let $b, c \in \mathbb{C}$ and $m \in \mathbb{N}$. Then*

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

Lemma 3 (Pfaff-Saalschütz) *Let $a, b, c, d \in \mathbb{C}, m \in \mathbb{N}$ and let $d = 1 + a + b - c - m$. Then*

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

Proofs of these identities can be found in [1]. Theorem 3 is only applicable if $d = 1 + a + b - c - m$ holds. As this is not always the case, transformations are necessary. We need the following one.

Lemma 4 (Gauss' contiguous relation) *Let $a_1, a_2, a_3, b_1, b_2, z \in \mathbb{C}$. Then*

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

In our computations we also use the following lemma.

Lemma 5 *Let $c(t) = \sum_{j \geq 0} c_j \cdot t^j$ be a formal series and let*

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

for some $k \geq 0$ and $n > k$, thus $p_{k+1} = \ldots = p_n = 0$. Then the series coefficients c_m, $m = k+1, \ldots, n$, can be expressed in terms of the c_i, $i = 0, \ldots, k$, as follows:

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

These technical Lemmas 2–5 allow to represent the variables of the linear program $L(k,n)_z$ as follows.

Proposition 1 *The structure of the feasible solutions $z = (z_0, \ldots, z_n)$ to the linear program $L(k,n)_z$ for $\ell = 0, \ldots, n$ is given by*

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

With Proposition 1 we see that the feasibility of Definition 3 can be replaced by (1), which we will use in Section 3.

Concerning the optimization in $L(k,n)_z$, we have the following.

Lemma 6 *Let $z' = (z'_0, \ldots, z'_n)$ and $z'' = (z''_0, \ldots, z''_n)$ be two feasible solutions to the linear program $L(k,n)_z$ with the same target value α. The for any convex combination $z''' = (z'''_0, \ldots, z'''_n)$ with $z'''_i = \lambda \cdot z'_i + (1-\lambda) \cdot z''_i$, $i = 0, \ldots, n$ and $0 \leq \lambda \leq 1$,*

1. *either z''' is feasible with the same target value α as for z' and z'', or*
2. *z''' is not feasible, but from it one can construct a feasible solution z'''', that yields a target value $\alpha^* > \alpha$.*

Proposition 2 *Let $z = (z_0, \ldots, z_n)$ be a feasible solution to $L(k,n)_z$ with target value α. Then, $z' = (z'_0, \ldots, z'_n)$ with $z'_i := (-1)^k \cdot z_{n-i}$, $i = 0, \ldots, n$, is also a feasible solution to $L(k,n)_z$ with the same target value.*

From Lemma 6 and Proposition 2 we obtain:

Corollary 1 *For the linear program $L(k,n)_z$ there always exists an optimal solution $z = (z_0, \ldots, z_n)$ with $z_i = (-1)^k \cdot z_{n-i}$, $i = 0, \ldots, n$.*

Corollary 1 allows us to reduce the number of variables in $L(k,n)_z$ by a factor of approximately 2. We will make use of this in Section 3.

3 Applications

3.1 The Linear Program $L(k,k)_z$

For the linear program $L(k,k)_z$, by Proposition 1, for $\ell = 0,\ldots,k$, we get

$$z_\ell = (-1)^\ell \cdot \binom{k}{\ell} \cdot \sum_{j=0}^{0} \frac{(\ell)_{-j} \cdot (\ell+1-j)_j}{(k+1-j)_j \cdot (-j)!} \cdot z_j = (-1)^\ell \cdot \binom{k}{\ell} \cdot z_0. \tag{2}$$

Thus, the linear program $L(k,k)_z$ can be formulated as

$$L(k,k)_z = z_0 \longrightarrow \text{ maximize}$$

subject to $\sum_{\substack{j=0 \\ z_j>0}}^{k} z_j = 1$ and $z_\ell = (-1)^\ell \cdot \binom{k}{\ell} \cdot z_0 \qquad \ell = 0,\ldots,k.$

As $L(k,k)_z = z_0$, in an optimal solution z we have $z_0 > 0$, hence, using that the sum of the positive variables has to be equal to 1, we infer that

$$1 \stackrel{!}{=} \sum_{\substack{j=0 \\ j \text{ even}}}^{k} z_j = z_0 \cdot \sum_{\substack{j=0 \\ j \text{ even}}}^{k} \binom{k}{j} = z_0 \cdot 2^{k-1}, \tag{3}$$

thus $z_0 = 2^{-k+1}$, which is the (unique) optimal value of the target function.

Naor and Shamir [7] already gave a proof of the optimality of this contrast for $L(k,k)_z$ by using approximate inclusion-exclusion. A simpler argument than that in [7] for the optimal target value of $L(k,k)$ has been given in [4].

3.2 The Linear Program $L(k-1,k)_z$

For the linear program $L(k-1,k)_z$ we have by Proposition 1 for $\ell = 0,\ldots,k$:

$$\begin{aligned} z_\ell &= (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot \sum_{j=0}^{1} \frac{(\ell-1)_{1-j} \cdot (\ell+1-j)_j}{(k+1-j)_j \cdot (1-j)!} \cdot z_j \\ &= (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot \left(\frac{z_1}{k} + (\ell-1) \cdot \left(z_0 + \frac{z_1}{k}\right)\right). \end{aligned} \tag{4}$$

Identity (4) has already been shown in [5] by another argument.

Thus, the linear program $L(k-1,k)_z$ is given by

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

subject to: $\sum_{\substack{j=0\\ z_j>0}}^{k} z_j = 1$ and

$$z_\ell = (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot \left(\frac{z_1}{k} + (\ell-1) \cdot \left(z_0 + \frac{z_1}{k}\right)\right) \qquad \ell = 0, \ldots, k.$$

By Corollary 1 there must exist an optimal solution z to $L(k-1,k)_z$ with $z_\ell = (-1)^{k-1} \cdot z_{k-\ell}$, $\ell = 0, \ldots, n$, and we infer

$$\begin{aligned}
& 0 = (-1)^{k-1} \cdot z_{k-\ell} - z_\ell \\
& \quad = (-1)^{k-1} \cdot (-1)^{k-\ell-1} \cdot \binom{k}{k-\ell} \cdot \left(\frac{z_1}{k} + (k-\ell-1) \cdot \left(z_0 + \frac{z_1}{k}\right)\right) \\
& \qquad - (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot \left(\frac{z_1}{k} + (\ell-1) \cdot \left(z_0 + \frac{z_1}{k}\right)\right) && \text{(by (4))} \\
& \quad = (-1)^{\ell} \cdot \binom{k}{\ell} \cdot \left(\frac{2z_1}{k} + (k-2) \cdot \left(z_0 + \frac{z_1}{k}\right)\right) \\
\iff \quad & z_0 = -\frac{z_1}{k-2}. && (5)
\end{aligned}$$

By (4) and (5) we obtain for $\ell = 0, \ldots, k$:

$$z_\ell = (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot z_1 \cdot \frac{k-2\ell}{(k-2) \cdot k}, \tag{6}$$

and by (5) the target function of $L(k-1,k)_z$ becomes

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

hence $z_1 < 0$ due to the assumption on the optimality of z.

To satisfy the first feasibility condition, we determine the sum of all positive variables z_ℓ by using (6). Let k be even (the case of odd k is quite similar). From (6) we see that for $\ell < k/2$ each z_ℓ is positive if ℓ is even, as $z_1 < 0$. For $\ell > k/2$ however, those z_ℓ are positive when ℓ is odd. Using $z_\ell = (-1)^{k-1} \cdot z_{k-\ell} = -z_{k-\ell}$, $\ell = 0, \ldots, n$, the sum of the positive z_ℓ for $\ell > k/2$ is equal to the absolute values of the sum of all negative z_ℓ for $\ell < k/2$. Hence, the sum of all positive z_ℓ can be replaced by the negative sum of all negative z_ℓ, which simplifies the calculations, and we obtain by using (4) and (5):

$$
\begin{aligned}
1 \overset{!}{=} \sum_{\substack{j=0\\ z_j>0}}^{k} z_j &= \sum_{\substack{j=0\\ j \text{ even}}}^{k/2} z_j - \sum_{\substack{j=1\\ j \text{ odd}}}^{k/2} z_j = -\sum_{j=0}^{k/2} \left(\frac{z_1}{k} + (j-1)\left(-\frac{z_1}{k-2} + \frac{z_1}{k}\right)\right) \cdot \binom{k}{j} \\
&= -z_1 \cdot \left[\frac{1}{k} \cdot \sum_{j=0}^{k/2} \binom{k}{j} \cdot j - \frac{1}{k-2} \cdot \sum_{j=0}^{k/2} \binom{k}{j} \cdot j + \frac{1}{k-2} \cdot \sum_{j=0}^{k/2} \binom{k}{j} \right] \\
&= -z_1 \cdot \left[\frac{1}{k} \cdot \frac{k \cdot 2^k}{4} - \frac{1}{k-2} \cdot \frac{k \cdot 2^k}{4} + \frac{1}{k-2} \cdot \left(2^{k-1} + \frac{1}{2} \cdot \binom{k}{\frac{k}{2}} \right) \right] \\
&= -\frac{z_1}{2(k-2)} \cdot \binom{k}{\frac{k}{2}} \\
\Longleftrightarrow \quad z_1 &= (4-2k) \cdot \binom{k}{\frac{k}{2}}^{-1} . \qquad (7)
\end{aligned}
$$

With (5) and (7) we further infer

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

hence for the optimal value of the target function we have

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

By (4) an optimal solution to $L(k-1,k)_z$ for k even is given by

$$
z_\ell = (-1)^{\ell-1} \cdot \binom{k}{\ell} \cdot \binom{k}{\frac{k}{2}}^{-1} \cdot \left(\frac{4\ell}{k} - 2 \right) \qquad \ell = 0, \dots, k.
$$

Lemma 7 *Let k be an even positive integer, and let $z = (z_0, \dots, z_k)$ be an optimal solution to the linear program $L(k-1,k)_z$. Then $z_{k/2} = 0$.*

Proof. Let $z' = (z'_0, \dots, z'_k)$ be an optimal solution to $L(k-1,k)_z$ with $z'_{k/2} \neq 0$. Then, the solution $z'' = (z''_0, \dots, z''_k)$ with $z''_i := -z'_{k-i}$, $i = 0, \dots, k$, is also optimal by Proposition 2. These solutions are distinct as $z''_{k/2} = -z'_{k/2} \neq 0$. We construct another solution $z''' = (z'''_0, \dots, z'''_k)$ with $z'''_i := (z'_i + z''_i)/2$, $i = 0, \dots, k$. From the proof of Lemma 6 it follows, that this solution is only feasible if there is no i such that $sgn(z'_i) = -sgn(z''_i) \neq 0$ holds. For $i = k/2$ however, $sgn(z'_{k/2}) \neq sgn(z''_{k/2})$ holds, which implies that z''' is not feasible. By Lemma 6(2.) we can construct another solution z''''–by scaling the solution z'''–, with a larger target value than that of z' and z'' yield and with $z''''_{k/2} = 0$. □

With $z_{k/2} = 0$ we infer for each optimal solution

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

thus we have (5), the optimal solution is unique for k even (but not for k odd).

The optimal contrast for $(k-1,k)$-schemes has also been obtained by Blundo et al. [2] by using a different approach via *canonical matrices*.

3.3 The Linear Program $L(k-2,k)_z$

For $(k-2,k)$-schemes we have by Proposition 1 for $\ell = 0, \ldots, k$:

$$z_\ell = (-1)^\ell \cdot \binom{k}{\ell} \cdot \left[\frac{(\ell-2)(\ell-1)}{2} \cdot z_0 + \frac{(\ell-2)\ell}{k} \cdot z_1 + \frac{(\ell-1)\ell}{k(k-1)} \cdot z_2 \right]. \tag{8}$$

Hence, the linear program $L(k-2,k)_z$ is given by

$$L(k-2,k)_z = z_0 + \frac{2z_1}{k} + \frac{2z_2}{k(k-1)} \longrightarrow \text{ maximize}$$

subject to $\sum\limits_{\substack{j=0 \\ z_j > 0}}^{k} z_j = 1$ and

$$z_\ell = (-1)^\ell \binom{k}{\ell} \left[\frac{(\ell-2)(\ell-1)}{2} \cdot z_0 + \frac{(\ell-2)\ell}{k} \cdot z_1 + \frac{(\ell-1)\ell}{k(k-1)} \cdot z_2 \right] \quad \ell = 0, \ldots, k.$$

By Corollary 1 there exists an optimal solution z with $z_\ell = (-1)^{k-2} \cdot z_{k-\ell}$, $\ell = 0, \ldots, k$, and by (8) we have

$$\begin{aligned} z_2 &= (-1)^{k-2} \cdot z_{k-2} \\ &= \binom{k}{2} \left[\frac{(k-4)(k-3)}{2} z_0 + \frac{(k-4)(k-2)}{k} z_1 + \frac{(k-3)(k-2)}{k(k-1)} z_2 \right] \\ \iff z_2 &= -\frac{(k-3)k}{2} z_0 - (k-2)z_1. \end{aligned} \tag{9}$$

For the target function we obtain with (9)

$$z_0 + \frac{2z_1}{k} + \frac{2z_2}{k(k-1)} = \frac{2}{k-1} \cdot \left(z_0 + \frac{z_1}{k}\right). \tag{10}$$

Inserting (9) into (8), for $\ell = 0, \dots, k$ we infer

$$z_\ell = (-1)^\ell \binom{k}{\ell} \underbrace{\frac{1}{k-1}\left(z_0 + \frac{z_1}{k}\right)}_{A} \underbrace{\left(\ell^2 - k\ell + \frac{z_0 k(k-1)}{z_0 k + z_1}\right)}_{B}. \tag{11}$$

The term A is equal to one half of the target function, thus A can be assumed to be positive. The term B determines, which variables z_ℓ are positive or negative. The zeros ℓ_1 and ℓ_2 of the parabola B, i.e., $B = 0$, are given by

$$\ell_{1,2} = \frac{k}{2} \pm \sqrt{\frac{k^2}{4} - \frac{z_0 k(k-1)}{z_0 k + z_1}}.$$

To satisfy the first feasibility condition, we now need to investigate whether the discriminant is positive, zero, or negative. We briefly discuss the observations. In case of a negative discriminant we obtain that the target value is less than

$$16/(k2^k). \tag{12}$$

For optimal solutions, the zeros a of the parabola B, if at all, have to be in the interval $[0, k]$, say $a \in [0, k/2]$ is such a zero of B. Then, with some computations concerning monotonicity and taking into account the parity of a and k, the optimal solution to $L(k-2, k)$ is given by the largest positive integer $a < (k-1)/2$ such that

$$\sum_{j=0}^{a} \binom{k}{j} < 2^{k-2}.$$

However, this means that for some constant $c > 0$ it is $a \approx k/2 - c \cdot \sqrt{k}$ by Stirling's formula, and we cannot say anything more precise currently. However, assuming that $a = (k-2)/2$, say, determining the corresponding target value of $L(k-2, k)_z$ gives a larger one than (12), hence for an optimal solution there is definitely a zero of the parabola B in the interval $[0, k/2]$.

4 Conclusion

Here we have given a new approach to determine the optimal contrast of (k, n)-schemes in Visual Cryptography. For $k = n$ and $k = n - 1$ this techniques turned out to be quite elegant. For the case $k = n - 2$ this is also the case, however, further considerations are necessary. Our approach should also be successful in the case of $k = n - 3$, however, this is work in progress, and more investigations are left for the future. It would be also of interest to see, whether these methods apply to the case of $(4, n)$-schemes.

References

[1] Andrews, G. E., Askey, R., and Roy, R.: Special Functions, *Cambridge University Press*, 1999.

[2] Blundo, C., D'Arco, P., De Santis, A., and Stinson, D. R.: Contrast optimal threshold visual cryptography schemes, *SIAM Journal on Discrete Mathematics*, 16, 224–261, 2003.

[3] Droste, S.: New Results on Visual Cryptography, *Proc. of the 16th Annual International Cryptology Conference – CRYPTO 96*, LNCS 1109, 401–415, 1996.

[4] Hofmeister, T., Krause, M., and Simon, H. U.: Contrast optimal k out of n secret sharing schemes in visual cryptography, *Theoretical Computer Science*, 240, 471–485, 2000.

[5] Juhnke, J.: Visuelle Kryptographie und (k,n)-Schemata, *Bachelor Thesis*, TU Chemnitz, 2011; see also: Ein Optimierungsproblem aus der Visuellen Kryptographie und seine Eigenschaften, *Master Thesis*, TU Chemnitz, 2013.

[6] Krause, M. and Simon, H. U.: Determining the optimal contrast for secret sharing schemes in visual cryptography, *Combinatorics, Probability and Computing* 12, 285–299, 2003.

[7] Naor, M. and Shamir, A.: Visual Cryptography, *Proc. Advances in Cryptology – EUROCRYPT '94*, LNCS 950, 1–12, 1995.