Determining the Optimal Contrast for Secret Sharing Schemes in Visual Cryptography

Matthias Krause
Theoretische Informatik
Universität Mannheim
D-68131 Mannheim, Germany
krause@th.informatik.uni-mannheim.de

Hans Ulrich Simon
Fakultät für Mathematik
Ruhr-Universität Bochum
D-44780 Bochum, Germany
simon@lmi.ruhr-uni-bochum.de.

Abstract

This paper shows that the largest possible contrast $C_{k,n}$ in a k-out-of-n secret sharing scheme is approximately $4^{-(k-1)}$. More precisely, we show that $4^{-(k-1)} \leq C_{k,n} \leq 4^{-(k-1)} n^k / (n(n-1) \cdots (n-(k-1)))$. This implies that the largest possible contrast equals $4^{-(k-1)}$ in the limit when n approaches infinity. For large n, the above bounds leave almost no gap. For values of n that come close to k, we will present alternative bounds (being tight for $n = k$). The proofs of our results proceed by revealing a central relation between the largest possible contrast in a secret sharing scheme and the smallest possible approximation error in problems occuring in Approximation Theory.

1 Introduction

Visual cryptography and k-out-of-n secret sharing schemes are notions introduced by Naor and Shamir in [8]. A sender wishing to transmit a secret message distributes n transparencies among n recipients, where the transparencies contain seemingly random pictures. A k-out-of-n scheme achieves the following situation: If any k recipients stack their transparencies together, then a secret message is revealed visually. On the other hand, if only $k-1$ recipients stack their transparencies, or analyze them by any other means, they are not able to obtain any information about the secret message. The reader interested in more background information about secret sharing schemes is referred to [8].

An important measure of a scheme is its *contrast*, i.e., the clarity with which the message becomes visible. This parameter lies in interval $[0, 1]$, where contrast 1 means "perfect clarity" and contrast 0 means "invisibility". Naor and Shamir constructed k-out-of-k secret sharing schemes with contrast $2^{-(k-1)}$ and were also able to prove optimality. However, they did not determine the largest possible contrast $C_{k,n}$ for arbitrary k-out-of-n secret sharing schemes.

In the following, there were made several attempts to find accurate estimations for the optimal contrast and the optimal tradeoff between contrast and subpixel expansion for arbitrary k-out-of-n secret sharing schemes [1], [2], [3], [4], [5]. For $k = 2$ and arbitrary n this problem was completely solved by Hofmeister, Krause, and Simon in [5]. But the underlying methods, which are based on the theory of linear codes, do not work for $k \geq 3$. Strengthening the approach of Droste [4], the first step in the direction of determining $C_{k,n}$ for some values k and n, where $k \geq 3$, was taken in [5]. They presented a simple linear program $\mathrm{LP}(k,n)$ whose optimal solution represents a contrast-optimal k-out-of-n secret sharing scheme. In particular, the value associated with this solution equals $C_{k,n}$. Although, $C_{k,n}$ was computable in $\mathrm{poly}(n)$ steps this way, and even elementary formulas were given for $k = 3, 4$, there was still no general formula for $C_{k,n}$ (or for good bounds). Based on computations of $C_{k,n}$ for specific choices of k, n, it was conjectured in [5] that $C_{k,n} \geq 4^{-(k-1)}$ with equality in the limit when n approaches infinity. In [3] and [2], some of the results from [5] concerning $k = 3, 4$ and arbitrary n could be improved. Furthermore, in [2], Blundo, D'Arco, DeSantis and Stinson determine the optimal contrast of k-out-of-n secret sharing schemes for arbitrary n and $k = n - 1$.

In this paper, we confirm the above conjecture of [5] by showing the following bounds on $C_{k,n}$:

$$4^{-(k-1)} \leq C_{k,n} \leq 4^{-(k-1)} \frac{n^k}{n(n-1)\cdots(n-(k-1))} \quad .$$

This implies that the largest possible contrast equals $4^{-(k-1)}$ in the limit when n approaches infinity. For large n, the above bounds leave almost no gap. For values of n that come close to k, we will present alternative bounds (being tight for $n = k$). The proofs of our results proceed by revealing a central relation between the largest possible contrast in a secret sharing scheme and the smallest possible approximation error in problems occuring in Approximation Theory. A similar relation was used in the paper [7] of Linial and Nisan about Approximate Inclusion-Exclusion (although there are also some differences and paper [7] ends-up with problems in Approximation Theory that are different from ours).

2 Definitions and Notations

For the sake of completeness, we recall the definition of visual secret sharing schemes given in [8]. In the sequel, we simply refer to them under the notion *scheme*. For a 0-1–vector v, let $H(v)$ denote the Hamming weight of v, i.e., the number of ones in v.

Definition 2.1 *A k-out-of-n scheme $\mathcal{C} = (\mathcal{C}_0, \mathcal{C}_1)$ with m subpixels, contrast $\alpha = \alpha(\mathcal{C})$, and threshold d consists of two collections of Boolean $n \times m$ matrices $\mathcal{C}_0 = [C_{0,1}, \ldots, C_{0,r}]$ and $\mathcal{C}_1 = [C_{1,1}, \ldots, C_{1,s}]$, such that the following properties are valid:*

1. *For any matrix $S \in \mathcal{C}_0$, the OR v of any k out of the n rows of S satisfies $H(v) \leq d - \alpha m$.*

2. *For any matrix $S \in \mathcal{C}_1$, the OR v of any k out of the n rows of S satisfies $H(v) \geq d$.*

3. *For any $q < k$ and any q-element subset $\{i_1, \ldots, i_q\} \subseteq \{1, \ldots, n\}$, the two collections of $q \times m$ matrices $\mathcal{D}_0$ and $\mathcal{D}_1$ obtained by restricting each $n \times m$ matrix in $\mathcal{C}_0$ and $\mathcal{C}_1$ to rows $i_1, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same relative frequencies.*

k-out-of-n schemes are used in the following way to achieve the situation described in the introduction. The sender translates every pixel of the secret image into n vectors of arrays of subpixels, in the following way: If the sender wishes to transmit a white pixel, then she chooses one of the matrices from $\mathcal{C}_0$ according to the uniform distribution. In the case of a black pixel, one of the matrices from $\mathcal{C}_1$ is chosen. For all $1 \leq i \leq n$, recipient i obtains the i-th row of the chosen matrix as an array of subpixels, where a 1 in the row corresponds to a black subpixel and a 0 corresponds to a white subpixel. The subpixels are arranged in a fixed pattern, e.g. a rectangle. (Note that in this model, stacking transparencies corresponds to "computing" the OR of the subpixel arrays.)

The third condition in Definition 2.1 is often referred to as the "security property" which guarantees that any $k-1$ of the recipients cannot obtain any information out of their transparencies. The "contrast property", represented by the first two conditions in Definition 2.1, guarantees that k recipients are able to recognize black pixels visually since any array of subpixels representing a black pixel contains a "significant" amount of black subpixels more than any array representing a white pixel.[1]

In [5], it was shown that the largest possible contrast $C_{k,n}$ in an k-out-of-n scheme coincides with the value of an optimal solution for the following linear program (with variables $\xi_0, \ldots, \xi_n$ and $\eta_0, \ldots, \eta_n$):

The linear program LP(k, n)

max $\sum_{j=0}^{n-k} \binom{n-k}{j} \binom{n}{j}^{-1} (\xi_j - \eta_j)$ **subject to**

1. For $j = 0, \ldots, n : \xi_j \geq 0, \eta_j \geq 0$.

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

3. For $l = 0, \ldots, k-1$: $\sum_{j=l}^{n-k+l+1} \binom{n-k+1}{j-l} \binom{n}{j}^{-1} (\xi_j - \eta_j) = 0$.

The following sections only use this linear program (and do not explicitly refer to Definition 2.1).

We make the following conventions concerning matrices and vectors. For matrix A, A' denotes its transpose (resulting from A by exchanging rows and columns). A vector which is denoted by $\vec{c}$ is regarded as a column vector. Thus, its transpose $\vec{c}'$ is a row vector. The all-zeros (column) vector is denoted as $\vec{0}$. For matrix A, A_j denotes its j-th row vector. A'_j denotes the j-th row vector of its transpose (as opposed to the transpose of the j-th row vector).

[1] The basic notion of a secret sharing scheme, as given in Definition 2.1, has been generalized in several ways. The generalized schemes in [1], for instance, intend to achieve a situation where certain subsets of recipients can work successfully together, whereas other subsets will gain no information. If the two classes of subsets are the sets of at least k recipients and the sets of at most $k-1$ recipients, respectively, we obtain (as a special case) the schemes considered in this paper. Another model for 2-out-of-2 schemes involving three colors is presented in [9].

3 Approximation Error and Contrast

In Subsection 3.1, we relate the problem of finding the best k-out-of-n secret sharing scheme to the following two kinds of approximation problems. Problem BAV (Best Approximating Vector) asks for the "best approximation" of a given vector $\vec{c}$ within a vector space V. Problem BAP (Best Approximating Polynomial) asks for the "best approximation" of a given polynomial p of degree k within the set of polynomials of degree $k-1$ or less. It turns out that, choosing $\vec{c}, V, p$ properly, the largest possible contrast is twice the smallest possible approximation error. In Subsection 3.2, we use this relationship to determine lower and upper bounds. Moreover, the largest possible contrast is determined exactly in the limit (when n approaches infinity). In Subsection 3.3, we derive a criterion that helps to determine those pairs (k, n) for which $C_{k,n}$ coincides with its theoretical upper bound from Subsection 3.2.

3.1 Secret Sharing Schemes and Approximation Problems

As explained in Section 2, the largest possible contrast in an k-out-of-n secret sharing scheme coincides with the value of an optimal solution for the linear program LP(k, n). The special form exhibited by LP(k, n) is captured by the more abstract definitions of a linear program of type BAV or of type BAP.

We start with the discussion of type BAV. We say that a linear program LP is of *type BAV* if there exists a matrix $A \in \mathbb{R}^{k\times(1+n)}$ and a vector $\vec{c} \in \mathbb{R}^{n+1}$ such that LP (with variables $\vec{\xi} = (\xi_0, \ldots, \xi_n)$ and $\vec{\eta} = (\eta_0, \ldots, \eta_n)$) can be written in the following form:

The primal linear program LP$(A, \vec{c})$ of type BAV

max $\vec{c}'(\vec{\xi} - \vec{\eta})$ **subject to**

(LP1) $\vec{\xi} \geq \vec{0}, \vec{\eta} \geq \vec{0}$.

(LP2) $\sum_{j=0}^{n} \xi_j = \sum_{j=0}^{n} \eta_j = 1$.

(LP3) $A(\vec{\xi} - \vec{\eta}) = \vec{0}$.

Condition (LP2) implies that

$$\sum_{j=0}^{n} (\xi_j - \eta_j) = 0 \ .$$

Thus, we could add the all-ones row vector $(1, \ldots, 1)$ to matrix A in (LP3) without changing the set of legal solutions. For this reason, we assume in the sequel that the following condition holds in addition to (LP1), (LP2), (LP3):

(LP4) The vector space V_A spanned by the row vectors of A contains the all-ones vector.

We aim to show that linear program LP$(A, \vec{c})$ can be reformulated as the problem of finding the "best" approximation of $\vec{c}$ in V_A. To this end, we pass to the dual problem[2] (with variables s, t and $\vec{u} = (u_0, \ldots, u_{k-1})$):

The dual linear program DLP$(A, \vec{c})$ of type BAV

min s+t **subject to**

(DLP1) $A'\vec{u} + (s, \ldots, s)' \geq \vec{c}$.

(DLP2) $A'\vec{u} - (t, \ldots, t)' \leq \vec{c}$.

Conditions (DLP1) and (DLP2) are obviously equivalent to

$$s \geq \max_{j=0,\ldots,n} (c_j - A'_j\vec{u}) \text{ and } t \geq \max_{j=0,\ldots,n} (A'_j\vec{u} - c_j) \ ,$$

and an optimal solution certainly satisfies

$$s = \max_{j=0,\ldots,n} (c_j - A'_j\vec{u}) \text{ and } t = \max_{j=0,\ldots,n} (A'_j\vec{u} - c_j) \ .$$

Note that vector $A'\vec{u}$ is a linear combination of the row vectors of A. Thus, $V_A = \{A'\vec{u} | \ \vec{u} \in \mathbb{R}^k\}$. DLP$(A, \vec{c})$ can therefore be rewritten as

$$\min_{\vec{v} \in V_A} \left[\max_{j=0,\ldots,n} (c_j - v_j) + \max_{j=0,\ldots,n} (v_j - c_j) \right] \ .$$

Consider a vector $\vec{v} \in V_A$ and let $j_-(\vec{v})$ and $j_+(\vec{v})$ be chosen such that

$$\begin{aligned} c_{j_-(\vec{v})} - v_{j_-(\vec{v})} &= \max_{j=0,\ldots,n} (c_j - v_j) \ , \\ v_{j_+(\vec{v})} - c_{j_+(\vec{v})} &= \max_{j=0,\ldots,n} (v_j - c_j) \ . \end{aligned}$$

Term $S(\vec{v}) := c_{j_-(\vec{v})} - v_{j_-(\vec{v})}$ represents the penalty for $v_{j_-(\vec{v})}$ being smaller than $c_{j_-(\vec{v})}$. Symmetrically, $L(\vec{v}) := v_{j_+(\vec{v})} - c_{j_+(\vec{v})}$ represents the penalty for $v_{j_+(\vec{v})}$ being larger than $c_{j_+(\vec{v})}$. Note that the total penalty $S(\vec{v}) + L(\vec{v})$ does not change if we translate $\vec{v}$ by a scalar multiple of the all-ones vector $(1, \ldots, 1)'$. According to (LP4), any translation of this form can be performed within V_A. Choosing the translation of $\vec{v}$ appropriately, we can achieve $S(\vec{v}) = L(\vec{v})$, that is, a perfect balance between the two penalty terms. Consequently, the total penalty for $\vec{v}$ is twice the distance between $\vec{c}$ and $\vec{v}$ measured by the metric induced by the maximum-norm. We thus arrive at the following result:

Theorem 3.1 *Given linear program LP$(A, \vec{c})$ of type BAV, the value C of an optimal solution for LP$(A, \vec{c})$ satisfies*

$$C = 2 \cdot \min_{\vec{v} \in V_A} \max_{j=0,\ldots,n} |c_j - v_j| \ .$$

[2] The rules, describing how the dual linear program is obtained from a given primal, can be looked up in any standard text about linear programming (like [10], for instance). The dual has an optimal solution iff the primal has an optimal solution. Moreover, the value of an optimal solution for the dual coincides with the value of an optimal solution for the primal.

Thus, the problem of finding an optimal solution to LP$(A, \vec{c})$ boils down to the problem of finding a best approximation of $\vec{c}$ in V_A w.r.t. the maximum-norm.

We move on to the discussion of linear programs of type BAP. We call $\vec{d} \in \mathbb{R}^{1+n}$ *evaluation-vector* of polynomial $p \in \mathbb{R}[X]$ if $d_j = p(j)$ for $j = 0, \ldots, n$. We say that a linear program LP$(A, \vec{c})$ of type BAV is of *type BAP* if, in addition to Conditions (LP1),..,(LP4), the following holds:

(LP5) $\vec{c}$ is the evaluation vector of a polynomial, say p, of degree k.

(LP6) Matrix $A \in \mathbb{R}^{k \times (1+n)}$ has rank k, i.e., its row vectors are linearly independent.

(LP7) For $l = 0, \ldots, k-1$, row vector A_l is the evaluation vector of a polynomial, say q_l, of degree at most $k-1$.

Let P_m denote the set of polynomials of degree at most m. Conditions (LP6) and (LP7) imply that V_A is the vector space of evaluation vectors of polynomials from P_{k-1}. Theorem 3.1 implies that the value C of an optimal solution for a linear program of type BAP satisfies

$$C = 2 \cdot \min_{q \in P_{k-1}} \max_{j=0,\ldots,n} |p(j) - q(j)| \ .$$

Let λ denote the leading coefficient of p. Thus p can be written as sum of λX^k and a polynomial in P_{k-1}. Obviously, p is as hard to approximate within P_{k-1} as $|\lambda| X^k$. We obtain the following result:

Corollary 3.2 *Given linear program LP$(A, \vec{c})$ of type BAP, let p denote the polynomial of degree k with evaluation vector $\vec{c}$, and λ the leading coefficient of p. Then the value C of an optimal solution for LP$(A, \vec{c})$ satisfies*

$$C = 2 \cdot \min_{q \in P_{k-1}} \max_{j=0,\ldots,n} \left| |\lambda| j^k - q(j) \right| \ .$$

We introduce the notation

$$n^{\underline{k}} = n(n-1) \cdots (n-(k-1))$$

for so-called "falling powers" and proceed with the following result:

Lemma 3.3 *The linear program LP(k, n) is of type BAP. The leading coefficient of the polynomial p with evaluation vector $\vec{c}$ is $(-1)^k / n^{\underline{k}}$.*

Proof: The form of LP(k, n) certainly fits the definition of type BAV programs. In order to verify Condition (LP5), it suffices to show that the j-th component of the cost vector in LP(k, n) is a polynomial of degree k in j. This can be accomplished by a direct calculation:

$$\begin{aligned} \frac{\binom{n-k}{j}}{\binom{n}{j}} &= \frac{(n-j)!}{(n-j-k)!} \cdot \frac{(n-k)!}{n!} \\ &= \frac{(n-j)(n-1-j)\cdots(n-(k-1)-j)}{n(n-1)\cdots(n-(k-1))} \\ &= \left(1 - \frac{j}{n}\right)\left(1 - \frac{j}{n-1}\right) \cdots \left(1 - \frac{j}{n-(k-1)}\right) \end{aligned}$$

Thus, $\vec{c}$ is the evaluation vector of polynomial

$$p_{k,n}(X) = \left(1 - \frac{X}{n}\right)\left(1 - \frac{X}{n-1}\right)\cdots\left(1 - \frac{X}{n-(k-1)}\right) \in P_k$$

with leading coefficient $(-1)^k/n^{\underline{k}}$.

Condition (LP7) can be shown by a similar computation. Condition (LP6) easily follows from the observation that matrix $A \in \mathbb{R}^{k\times(1+n)}$ has entries

$$a_{l,j} = \frac{\binom{n-(k-1)}{j-l}}{\binom{n}{j}} .$$

These entries vanish for $j < l$ and for $j \geq n + l - k + 2$, but do not vanish for $j = l$. Thus, A is an upper triangular matrix with nonzeros on the main diagonal. Obviously, its rank is k. •

Corollary 3.4 *Let $C_{k,n}$ denote the largest possible contrast in an k-out-of-n secret sharing scheme. Then:*

$$C_{k,n} = 2 \cdot \min_{q\in P_{k-1}} \max_{j=0,\ldots,n} \left|j^k/n^{\underline{k}} - q(j)\right| .$$

Thus, the largest possible contrast in an k-out-of-n secret sharing scheme is identical to twice the smallest "distance" between polynomial $X^k/n^{\underline{k}}$ and a polynomial in P_{k-1}, where the "distance" between two polynomials is measured as the maximum absolute difference of their evaluations on points $0, 1 \ldots, n$.

3.2 Lower and Upper Bounds

Finding the "best approximating polynomial" of X^k within P_{k-1} is a classical problem in Approximation Theory. Most of the classical results are stated for polynomials defined on the interval $[-1, 1]$. In order to recall these results and to apply them to our problem at hand, the definition of the following metric will be useful:

$$d_\infty(f, g) = \max_{x\in[-1,1]} |f(x) - g(x)| .$$

This definition makes sense for functions that are continuous on $[-1, 1]$ (in particular for polynomials). The metric implicitly used in Corollaries 3.2 and 3.4 is different because distance between polynomials is measured on a finite set of points rather than on a continuous interval. For this reason, we consider the sequence

$$z_j = -1 + \frac{2j}{n} \text{ for } j = 0, \ldots, n .$$

It forms a regular subdivision of the interval $[-1, 1]$ of step width $2/n$. The following metric is a "discrete version" of d_∞:

$$d_n(f, g) = \max_{j=0,\ldots,n} |f(z_j) - g(z_j)| .$$

Let $U_k(X) = X^k$ and $U^*_{k,\infty}$ be the best approximation of U_k within P_{k-1} w.r.t. d_∞. Analogously, $U^*_{k,n}$ denotes the best approximation of U_k within P_{k-1} w.r.t. d_n. Then

$$D_{k,\infty} = d_\infty(U_k, U^*_{k,\infty}) \text{ and } D_{k,n} = d_n(U_k, U^*_{k,n})$$

are the corresponding approximation errors. It is well known from Approximation Theory[3] that

$$U^*_{k,\infty}(X) = X^k - 2^{-(k-1)} T_k(X)$$

where T_k denotes the Chebyshev polynomial of the first find of degree k (defined and visualized in Figure 1). It is well known that $T_k = \cos(k\theta)$ is a polynomial of degree k in $X = \cos(\theta) \in [-1, 1]$ with leading coefficient 2^{k-1}. Thus, $U^*_{k,\infty}$ is indeed from P_{k-1}. Note that $2^{-(k-1)} T_k(X) = X^k - U^*_{k,\infty}(X)$ is the "error polynomial" that indicates the difference between X^k and $U^*_{k,\infty}(X)$. Since $\max_{-1 \le x \le 1} T_k(x) = 1$, we get

$$D_{k,\infty} = 2^{-(k-1)} \quad . \tag{1}$$

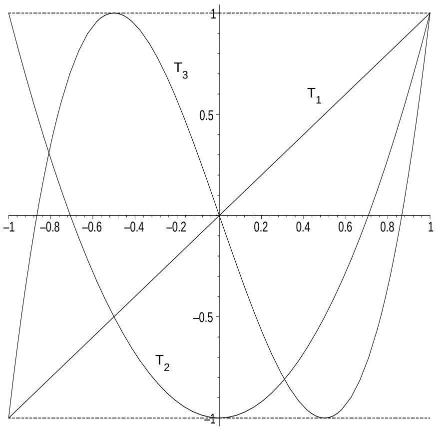

Figure 1: The Chebyshev polynomial T_k of degree k for $k = 1, 2, 3$. $T_k(X) = \cos(k\theta)$, where $0 \le \theta \le \pi$ and $X = \cos(\theta)$.

Unfortunately, there is no such simple formula for $D_{k,n}$ (the quantity we are interested in). It is however easy to see that the following inequalities are valid:

$$\left(1 - \frac{k^2}{n}\right) 2^{-(k-1)} \le D_{k,n} \le D_{k,\infty} = 2^{-(k-1)} \quad . \tag{2}$$

Inequality $D_{k,n} \le D_{k,\infty}$ is obvious because $d_n(f, g) \le d_\infty(f, g)$ for all f, g. The first inequality could be derived from the fact that the first derivation of T_k is bounded by k^2 on $[-1, 1]$.[4] We skip this derivation because we are able to prove the stronger inequality (7) below.

[3] See Chapter 1.2 in [11], for instance.

[4] A proof of this fact can be found in [7], for instance.

Quantities $D_{k,n}$ and $C_{k,n}$ are already indirectly related by Corollary 3.4. In order to get the precise relation, we have to apply the linear transformation $X \to \frac{n}{2}(X+1)$, because the values attained by a function $f(X)$ on $X = 0, \ldots, n$ coincide with the values attained by function $f\left(\frac{n}{2}(X+1)\right)$ on $X = z_0, \ldots, z_n$. This transformation, applied to a polynomial of degree k with leading coefficient λ, leads to a polynomial of the same degree with leading coefficient $\lambda\left(\frac{n}{2}\right)^k$. The results corresponding to Corollaries 3.2 and 3.4 now read as follows:

Corollary 3.5 *Given a linear program $LP(A, \vec{c})$ of type BAP, let p denote the polynomial of degree k with evaluation vector $\vec{c}$, and λ the leading coefficient of p. Then the value C of an optimal solution for $LP(A, \vec{c})$ satisfies*

$$C = 2 \cdot |\lambda| \left(\frac{n}{2}\right)^k D_{k,n} \quad .$$

Plugging in $(-1)^k/n^{\underline{k}}$ for λ, we obtain

Corollary 3.6 *The largest possible contrast in an k-out-of-n secret sharing scheme satisfies*

$$C_{k,n} = \frac{n^k}{n^{\underline{k}}} 2^{-(k-1)} D_{k,n} \quad .$$

Since $D_{k,\infty} = 2^{-(k-1)}$, we get the following result:

Corollary 3.7 *For any fixed $k \geq 2$, the limit of the largest possible contrast in an k-out-of-n secret sharing scheme, when n approaches infinity, satisfies*

$$C_{k,\infty} = \lim_{n\to\infty} C_{k,n} = 4^{-(k-1)} \quad .$$

The derivation of $C_{k,\infty}$ from $D_{k,\infty}$ profited from the classical equation (1) from Approximation Theory. For $n = k$, we can go the other way and derive $D_{k,k}$ from the fact (see [8]) that the largest possible contrast in an k-out-of-k secret sharing scheme is $2^{-(k-1)}$:

$$C_{k,k} = 2^{-(k-1)} \quad .$$

Applying Corollary 3.6, we obtain

$$D_{k,k} = \frac{k!}{k^k} \quad . \tag{3}$$

According to Stirling's formula, this quantity is asymptotically equal to $\sqrt{2\pi k}e^{-k}$. Equation (3) presents the precise value for the smallest possible approximation error when X^k is approximated by a polynomial of degree $k-1$ or less, and the distance between polynomials is measured by metric d_k.

Sequence $C_{k,n}$ monotonically decreases with n because the secret sharing scheme becomes harder to design when more people are going to share the secret (and threshold k is fixed). Thus, the unknown value for $C_{k,n}$ must be somewhere between $C_{k,\infty} = 4^{-(k-1)}$ and $C_{k,k} = 2^{-(k-1)}$. We don't expect the sequence $D_{k,n}$ to be perfectly monotonous. However, we know that $D_{k,n} \leq D_{k,\infty}$. If n is a multiple of k, the regular subdivision of $[-1, 1]$ with step width

$2/n$ is a refinement of the regular subdivision of $[-1,1]$ with step width $2/k$. This implies $D_{k,ck} \geq D_{k,k}$ for all natural k, c.

Figure 2 presents an overview over the results obtained so far. An edge from a to b with label s should be interpreted as $b = s \cdot a$. For instance, the edges with labels $r_{k,n}, r'_{k,n}, s'_{k,n}, s_{k,n}$ represent the equations

$$\begin{aligned} C_{k,n} &= r_{k,n} \cdot C_{k,\infty} \text{ with } r_{k,n} \geq 1, \\ C_{k,k} &= r'_{k,n} \cdot C_{k,n} \text{ with } r'_{k,n} \geq 1, \\ D_{k,n} &= s'_{k,n} \cdot D_{k,k} \text{ with } s'_{k,n} \geq 1 \text{ if } n \text{ is a multiple of } k, \\ D_{k,\infty} &= s_{k,n} \cdot D_{k,n} \text{ with } s_{k,n} \geq 1, \end{aligned}$$

respectively. The edges between $C_{k,n}$ and $D_{k,n}$ explain how $D_{k,n}$ is derived from $C_{k,n}$ and vice versa, i.e., these edges represent Corollary 3.6. Figure 2 can be used to obtain approximations for the unknown parameters $r_{k,n}, r'_{k,n}, s'_{k,n}, s_{k,n}$. The simple path from $C_{k,\infty} = 4^{-(k-1)}$ to $D_{k,\infty} = 2^{-(k-1)}$ corresponds to equation

$$2^{-(k-1)} = s_{k,n} \cdot 2^{k-1} \frac{n^{\underline{k}}}{n^k} \cdot r_{k,n} \cdot 4^{-(k-1)} \ .$$

After some cancellation, we arrive at

$$r_{k,n} \cdot s_{k,n} = \frac{n^k}{n^{\underline{k}}} \ . \tag{4}$$

A similar computation associated with the simple path from $D_{k,k}$ to $C_{k,k}$ leads to

$$r'_{k,n} \cdot s'_{k,n} = \frac{k^k n^{\underline{k}}}{k! n^k} = \left(\frac{k}{n}\right)^k \binom{n}{k} \ . \tag{5}$$

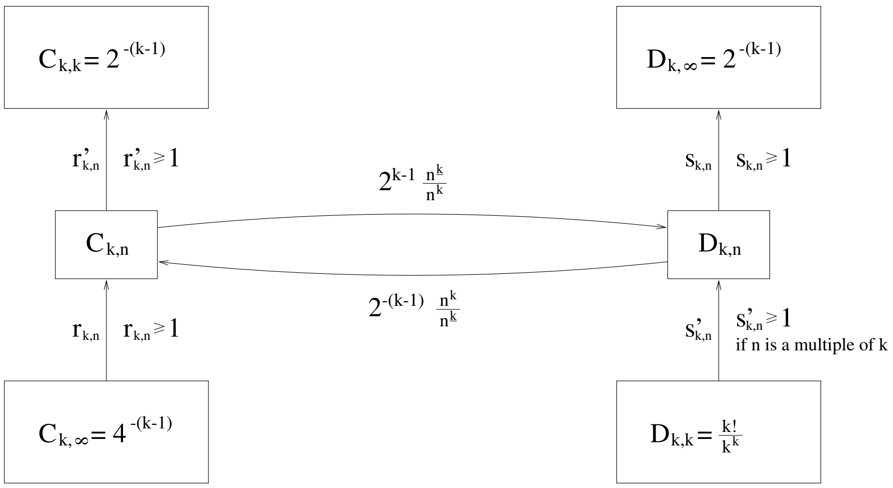

Figure 2: Sequence $C_{k,n}$, sequence $D_{k,n}$ and relations between them.

The following bounds on $C_{k,n}$ and $D_{k,n}$ are now evident from Figure 2 and (4):

$$4^{-(k-1)} \le C_{k,n} = r_{k,n} 4^{-(k-1)} \le \frac{n^k}{n^{\underline{k}}} 4^{-(k-1)} \ , \tag{6}$$

$$\frac{n^{\underline{k}}}{n^k} 2^{-(k-1)} \le \frac{2^{-(k-1)}}{s_{k,n}} = D_{k,n} \le 2^{-(k-1)} \ . \tag{7}$$

In both cases, the upper bound exceeds the lower bound by factor $n^k/n^{\underline{k}}$ only (approaching 1 when n approaches infinity).[5] An elementary computation[6] shows that $1-k^2/n < n^{\underline{k}}/n^k \le 1$ holds for all $1 \le k \le n$. Thus, (7) improves on the classical inequality (2) from Approximation Theory.

Although bounds (6) and (7) are excellent for large n, they are quite poor when n comes close to k. In this case however, we obtain from Figure 2 and (5)

$$\frac{(n/k)^k}{\binom{n}{k}} 2^{-(k-1)} \le C_{k,n} \le 2^{-(k-1)} \ , \tag{8}$$

and

$$\frac{k!}{k^k} \le D_{k,n} \le \frac{n^{\underline{k}}}{n^k} \ , \tag{9}$$

where the first inequality in (8) and the first inequality in (9) are only guaranteed if n is a multiple of k. These bounds are tight for $n = k$.

3.3 Discussion of the MAX-Condition

Paper [5] presented some explicit formulas for $C_{k,n}$, but only for small values of k. For instance, it was shown that $C_{k,n} = 4^{-(k-1)} \cdot n^k/n^{\underline{k}}$ holds for the following specific choices of k, n:

- $k = 2$ and n is even,
- $k = 3$ and n is a multiple of 4.

Thus $C_{k,n}$ coincides with its theoretical upper bound $4^{-(k-1)} n^k/n^{\underline{k}}$ from (6) in theses cases. However, the following table supports the conjecture that there is no such coincidence for most other choices of k, n. The entry in row k and column n is $C_{k,n}$ on top of its upper bound:

[5] Because of (4), the two gaps cannot be maximal simultaneously. For instance, at least one of the upper bounds exceeds the corresponding lower bound at most by factor $\sqrt{n^k/n^{\underline{k}}}$.

[6] Making use of $e^{-2x} \le 1 - x \le e^{-x}$, where the first inequality holds for all $x \in [0, 1/2]$ and the second for all $x \in \mathbb{R}$.

$k\backslash n$	2	3	4	5	6	7	8	$\cdots$	100	$\cdots$	∞
2	1/2 1/2	1/3 3/8	1/3 1/3	3/10 5/16	3/10 3/10	2/7 7/24	2/7 2/7		25/99 25/99		1/4 1/4
3		1/4 9/32	1/6 1/6	1/8 25/192	1/10 9/80	1/10 49/480	2/21 2/21		625/9702 625/9702		1/16 1/16
4			1/8 1/6	1/15 125/1536	1/18 9/160	3/70 343/7680	3/80 4/105		425/25608 15625/941094		1/64 1/64

The goal of this subsection is to provide a simple explanation for this phenomenon by exploiting the duality between $C_{k,n}$ and $D_{k,n}$. We start with a general observation, which is evident from Figure 2 and (4).

Corollary 3.8 *The following statements are equivalent:*

1. $C_{k,n} = 4^{-(k-1)} \cdot n^k / n^{\underline{k}}$.
2. $r_{k,n} = n^k / n^{\underline{k}}$.
3. $s_{k,n} = 1$.
4. $D_{k,n} = 2^{-(k-1)} = D_{k,\infty}$.

We say that (k,n) *satisfies the MAX-Condition* if these statements are valid for k,n (or equivalently, one of them is valid). With these notations, the aforementioned results in [5] read as follows: (k,n) satisfies the MAX-Condition for $k=2$ and even n, and for $k=3$ and n a multiple of 4.

In order to provide a simple proof for these and some supplementary results, we bring two classical theorems from Approximation Theory into play. Let $f : [-1,1] \to \mathbb{R}$ be a continuous function and $p \in P_{k-1}$ a polynomial of degree at most $k-1$. A sequence

$$-1 \leq x_0 < x_1 < \cdots < x_{l-1} \leq 1$$

is called an *alternating sequence of length l for error function $f-p$* if

$$\begin{aligned} |f(x_i) - p(x_i)| &= d_\infty(f,p) \text{ for } i = 0,1,\ldots,l-1 \text{ and} \\ f(x_i) - p(x_i) &= -\left(f(x_{i+1}) - p(x_{i+1})\right) \text{ for } i = 0,1,\ldots,l-2. \end{aligned}$$

The following result is well-known in Approximation Theory:

Theorem 3.9 *[Theorem 1.7 in [11]]*
Let $f : [-1,1] \to \mathbb{R}$ be continuous and $p^* \in P_{k-1}$. $f - p^*$ has an alternating sequence of length $k+1$, iff p^* is the (unique) best approximating polynomial for f w.r.t. d_∞.

Example 3.10 *Let $f(X) = U_k(X) = X^k$ and $p^*(X) = U^*_{k,\infty}(X) = X^k - 2^{-(k-1)}T_k(X)$, where $T_k(X)$ is the Chebyshev polynomial of degree k (defined and visualized in Figure 1).*

Note that $2^{-(k-1)}T_k$ is the corresponding error function, which clearly has the same alternating sequences as T_k. It is obvious that

$$x_i = \cos\left(\frac{(k-i)\pi}{k}\right) \quad \textit{for } i = 0, 1, \ldots, k$$

is an alternating sequence for T_k of length $k+1$. Thus, Theorem 3.9 implies that $U^*_{k,\infty}$ is the best approximating polynomial for U_k w.r.t. d_∞.

In the sequel, let

$$E_k = \left\{\cos\left(\frac{(k-i)\pi}{k}\right) \mid i = 0, \ldots, k\right\}$$

denote the set of points in $[-1, 1]$, where T_k attains its $k+1$ extremal values ± 1. Note that values ± 1 alternate. It follows that the sequence of points in E_k, ordered from left to right, is the only alternating sequence for T_k of length $k+1$.

Let Z be a finite subset of $[-1, 1]$. A sequence

$$-1 \leq x_0 < x_1 < \cdots < x_{l-1} \leq 1$$

is called an *alternating sequence for error function $f-p$ of length l w.r.t. Z* if $x_0, x_1, \ldots, x_{l-1} \in Z$ and

$$\begin{aligned} |f(x_i) - p(x_i)| &= \max_{x \in Z} |f(x) - p(x)| \text{ for } i = 0, 1, \ldots, l-1, \\ f(x_i) - p(x_i) &= -\left(f(x_{i+1}) - p(x_{i+1})\right) \text{ for } i = 0, 1, \ldots, l-2. \end{aligned}$$

An important special case is $Z = Z_n$, where

$$Z_n = \{z_0, \ldots, z_n\} = \left\{-1 + \frac{2i}{n} \mid i = 0, \ldots, n\right\} .$$

The following result is well-known in Approximation Theory:

Theorem 3.11 *[Theorem 1.11 in [11]]*
Let $f : [-1, 1] \to \mathbb{R}$ be continuous, $p^* \in P_{k-1}$, and Z a finite subset of $[-1, 1]$. $f - p^*$ has an alternating sequence of length $k+1$ w.r.t. Z iff p^* is the (unique) best approximating polynomial for f on Z, i.e., iff

$$\max_{z \in Z} |f(z) - p^*(z)| = \min_{p \in P_{k-1}} \max_{z \in Z} |f(z) - p(z)| .$$

Note that the best approximating polynomial on Z_n is the best approximating polynomial w.r.t. metric d_n. We now obtain the following

Corollary 3.12 *(k, n) satisfies the MAX-Condition iff $E_k \subseteq Z_n$.*

Proof: Assume that $E_k \subseteq Z_n$. Then the points $x_0, x_1, \ldots, x_k \in E_k$ are also an alternating sequence for T_k w.r.t. Z_n. Thus, $U^*_{k,\infty} = U^*_{k,n}$ and $D_{k,\infty} = D_{k,n}$, implying the MAX-Condition.

Assume conversely that $E_k \not\subseteq Z_n$. Let $-1 \leq y_0 < y_1 < \ldots < y_k \leq 1$ be an alternating sequence for $U_k - U^*_{k,n}$ of length $k+1$ w.r.t. Z_n. Let $M_k = \{y_0, y_1, \ldots, y_k\}$. We distinguish two cases.

Case 1 $U^*_{k,n} = U^*_{k,\infty}$.

For the sake of brevity, let $\kappa = 2^{-(k-1)}$. The definition of alternating sequences and the fact that $\kappa T_k \equiv U_k - U^*_{k,\infty} \equiv U_k - U^*_{k,n}$ implies that $\kappa|T_k(x)| = D_{k,\infty}$ for all $x \in E_k$ and $\kappa|T_k(y)| = D_{k,n}$ for all $y \in M_k$. Since $E_k \not\subseteq Z_n$ and $M_k \subseteq Z_n$, there must exist a point $y \in M_k$ not belonging to E_k. Note that $|T_k(y)| < 1$ (by definition of E_k). Pick an arbitrary point x from E_k. Then $|T_k(x)| = 1$ holds (again by definition of E_k). Thus, $D_{k,n} = \kappa|T_k(y)| < \kappa|T_k(x)| = D_{k,\infty}$.

Case 2 $U^*_{k,n} \neq U^*_{k,\infty}$.

Since the best approximating polynomial for U_k on Z_n is unique, it follows that $D_{k,n} = d_n(U_k, U^*_{k,n}) < d_n(U_k, U^*_{k,\infty}) \leq d_\infty(U_k, U^*_{k,\infty}) = D_{k,\infty}$.

In both cases, the MAX-Condition is violated. •

The next examples demonstrate that the results from [5], mentioned in the beginning of this subsection (along with some supplementary results), are extremely easy to prove by means of Corollary 3.12.

Example 3.13 $E_2 = \{\cos(\pi), \cos(\pi/2), \cos(0)\} = \{-1, 0, 1\}$. *For even n, $E_2 \subseteq Z_n$. However, $E_2 \not\subseteq Z_n$ for odd n (because $0 \notin Z_n$ in this case). This shows that the MAX-Condition is satisfied for $k = 2$ and even n, but not for $k = 2$ and odd n.*

Example 3.14 $E_3 = \{\cos(\pi), \cos(2\pi/3), \cos(\pi/3), \cos(0)\} = \{-1, -1/2, 1/2, 1\}$. *If n is a multiple of 4, then $E_3 \subseteq Z_n$. However, $E_3 \not\subseteq Z_n$ if n is not a multiple of 4 (because $-1/2, 1/2 \notin Z_n$ in this case). This shows that the MAX-Condition is satisfied for $k = 3$ and n a multiple of 4, but not for $k = 3$ and n not a multiple of 4.*

Example 3.15 *If* $\cos(\pi/k)$ *is irrational, then obviously $E_k \not\subseteq \cup_{n \geq k} Z_n$. Thus, for each $n \geq k$, (k, n) does not satisfy the MAX-Condition. This situation occurs already for $k = 4$ because* $\cos(\pi/4) = \sqrt{2}/2$.

We conclude the paper with a final remark and an open problem. Based on the results of this paper, Kuhlmann and Simon [6] were able to design arbitrary k-out-of-n secret sharing schemes with asymptotically optimal contrast. More precisely, the contrast achieved by their schemes is optimal up to a factor of at most $1 - k^2/n$. For moderate values of k and n, these schemes are satisfactory. For large values of n, they use too many subpixels. It is an open problem to determine (as precise as possible) the tradeoff between the contrast (which should be large) and the number of subpixels (which should be small).

Acknowledgments Thanks to two anonymous referees for their valuable suggestions.

References

[1] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson. Visual cryptography for general access structures. *Information and Computation*, 129(2):86–106, 1996.

[2] Carlo Blundo, Paolo D'Arco, Alfredo De Santis, and Douglas R. Stinson. Contrast optimal threshold visual cryptography schemes. Available at http://www.cacr.math.uwaterloo.ca/$\sim$dstinson/visual.html, 1998.

[3] Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson. On the contrast in visual cryptography schemes. *Journal of Cryptology*, 12:261–289, 1999.

[4] Stefan Droste. New results on visual cryptography. In *Proceedings of the Conference on Advances in Cryptology — CRYPTO '96*, pages 401–415. Springer Verlag, LNCS 1109, 1996.

[5] Thomas Hofmeister, Matthias Krause, and Hans U. Simon. Contrast-optimal k out of n secret sharing schemes in visual cryptography. *Theoretical Computer Science*, 240(2):471–485, 2000.

[6] Christian Kuhlmann and Hans U. Simon. Construction of visual secret sharing schemes with almost optimal contrast. In *Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 263–272, 2000.

[7] Nathan Linial and Noam Nisan. Approximate inclusion-exclusion. *Combinatorica*, 10:349–365, 1990.

[8] Moni Naor and Adi Shamir. Visual cryptography. In *Proceedings of the Conference on Advances in Cryptology — EUROCRYPT '94*, pages 1–12. Springer-Verlag, LNCS 950, 1995.

[9] Moni Naor and Adi Shamir. Visual cryptography II: Improving the contrast via the cover base. In *Proceedings of the Workshop on Security Protocols*, pages 197–202. Springer Verlag, LNCS 1189, 1997.

[10] Christos H. Papadimitriou and Kenneth Steiglitz. *Combinatorial Optimization: Algorithms and Complexity.* Prentice Hall, 1982.

[11] Theodore J. Rivlin. *An Introduction to the Approximation of Functions.* Blaisdell Publishing Company, 1969.