Construction of Visual Secret Sharing Schemes with Almost Optimal Contrast

Christian Kuhlmann* Hans Ulrich Simon†

Abstract

It was shown in [4] that the largest possible contrast $C(k,n)$ in a k-out-of-n secret sharing scheme is approximately $4^{-(k-1)}$ (with equality in the limit when n approaches infinity). However, the proof of this result was not constructive and did not answer the question how schemes with almost optimal contrast might look like. In this paper, we present an easy and universal construction of an appropriate k-out-of-n secret sharing scheme. The construction works for all values of k and n and achieves contrast-optimality in the limit with a fairly small gap for finite n. For small values of k (and all values of n), we get even contrast-optimality (without any gap). Finally, we argue that the problem to close the gap in general is related to a long standing open question in Approximation Theory.

1 Introduction

Visual cryptography and k-out-of-n secret sharing schemes are notions introduced by Naor and Shamir in [6]. 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 [6].

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. They left open the questions of determining the optimal contrast $C(k,n)$ in general, and of constructing a general k-out-of-n secret sharing scheme whose contrast comes close to optimality.

One step in the direction of determining $C(k,n)$ was gone by Hofmeister, Krause, and Simon in [3]. They presented a simple linear program $LP(k,n)$ whose optimal solution represented a contrast-optimal k-out-of-n secret sharing scheme. The profit realized by this solution equals $C(k,n)$. Although $C(k,n)$ was computable in poly(n) steps this way, and even elemantary formulas were given for small k (for $k=2$ and all even n, and for $k=3$ and all n that are multiples of 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 [3] that $C(k,n) \geq 4^{-(k-1)}$ with equality in the limit when n approaches infinity.

In [4], this conjecture was confirmed and the following bounds on $C(k,n)$ were presented:

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

This implies that the largest possible contrast equals $4^{-(k-1)}$ in the limit when n approaches infinity. These bounds were proven 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] However, the proof of this result was not constructive and did not answer the question how schemes with almost optimal contrast might look like.

*Fakultät für Mathematik, Ruhr-Universität Bochum, D-44780 Bochum, Germany.

†Fakultät für Mathematik, Ruhr-Universität Bochum, D-44780 Bochum, Germany.

[1] A similar relation was used in the paper [5] of Linial and Nisan about Approximate Inclusion-Exclusion.

In this paper, we present a "universal construction" of a k-out-of-n secret sharing scheme for arbitrary values of k and n. We make use of the fact from [3] that each solution for linear program $LP(k,n)$ implicitly represents a k-out-of-n secret sharing scheme (and can be converted into an explicit representation). Thus, we may focus on the problem of providing a universal construction for an almost optimal basic feasible solution for $LP(k,n)$. Using results from approximation theory and basic techniques from the theory of linear programming, we are able to show that an almost-optimal basic feasible solution can be obtained in a surprisingly simple manner from the extrema of the Chebyshev polynomial of degree k.

The paper is structured as follows. Section 2 recalls the definition of a secret sharing scheme from [6] and the linear program $LP(k,n)$ from [3], and makes some notational conventions. Section 3 first recalls some classical notions and facts from Approximation Theory, which were needed in [4] to derive tight bounds on the optimal contrast (and will also be needed later in section 5). Afterwards the bounds themselves are given. They can be stated in terms of a classical measure for approximation error. In order to provide a universal construction of asymptotically contrast-optimal schemes, we are forced to study a more unconventional measure. This is done in section 4. The universal construction is presented in section 5. After drawing some conclusions at the end of the regular paper, we briefly sketch the construction of contrast-optimal schemes for $k \le 4$ and arbitrary n in Appendix A. The reader interested in more details is referred to the full paper.

2 Definitions and Notations

For the sake of completeness, we recall the definition of visual secret sharing schemes given in [6]. 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 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 $H(v) \le d - \alpha m$.
2. For any matrix $S \in \mathcal{C}_1$, the OR v of any k out of the n rows of S satisfies $H(v) \ge d$.
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 sets 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 $1 \le i \le n$, 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 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, 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.[2]

In [3], it was shown that the largest possible contrast $C(k,n)$ in a k-out-of-n scheme coincides with the maximal profit in the following linear program (with variables $\xi_0, \ldots, \xi_n$ and $\eta_0, \ldots, \eta_n$):

Linear Program $LP(k,n)$

[2]The basic notion of a secret sharing scheme, as given in Definition 2, 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 [7].

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). We assume that the reader is familiar with the theory of linear programming and knows the concepts of feasibility, boundedness, basic and basic feasible solutions, and the relations between a primal problem and its dual. However, we do not go beyond the contents of standard books (like [8], for instance).

We make the following notational 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 $\vec{0}$. The analogous convention holds for $\vec{1}$. For sake of simplicity, we do not properly distinguish between row and column vectors when the meaning is well understood without this distinction. For instance, the inner product of two vectors is simply written as $\vec{a}\vec{b}$ (as opposed to $\vec{a}'\vec{b}$). If A is a matrix and J is a subset of its column indices, then A_J denotes the submatrix of A consisting of all columns indexed by J. Similarly, if $\vec{a}$ is a (row or column) vector, then $\vec{a}_J$ denotes the subvector consisting of all components indexed by J. For $J = \{j\}$, we simply write A_j to denote the j-th column vector of A and a_j to denote the j-th component of $\vec{a}$. A'_J denotes the transpose of submatrix A_J (as opposed to the submatrix of the transpose).

We close this section with the definition of a central notion in this paper. A vector $(w_0, w_1, \ldots, w_n)$ is the *evaluation vector of polynomial* p if $w_j = p(j)$ for $j = 0, \ldots, n$.

3 Approximation Error and Contrast

In this section, we recall some basic approximation-theoretic notions and facts (subsection 3.1) and the tight bounds on $C(k, n)$ from [4] (subsection 3.2).

3.1 Prerequisites from Approximation Theory In this subsection, we mention several classical results from Approximation Theory. The corresponding proofs can be looked up in any standard book (e.g., Chapter 1 in [9]).

Let P_k denote the set of polynomials (over the reals) of degree at most k. With each closed interval or finite set $I \subset \Re$, each continuous function $f : \Re \to \Re$, and each nonnegative integer k, we associate the following quantity:

$$E_k(f, I) = \min_{q \in P_k} \max_{x \in I} |f(x) - q(x)|. \tag{3.1}$$

$f - q$ is called *the error function (of polynomial q as approximation for f)*, and

$$E(f, I, q) = \max_{x \in I} |f(x) - q(x)| \tag{3.2}$$

is called *approximation error (of polynomial q as approximation for f on domain I)*. Given f and I, term $E_k(f, I)$ can therefore be interpreted as the smallest possible approximation error that can be achieved by a polynomial of degree at most k. It is well-known that the minimum in equation (3.1) is attained for a unique polynomial in P_k, called the *best approximating polynomial of degree at most k for f on domain I* and denoted by $q_{k,f,I}$, or simply by q_* if k, f, I are evident from context.

In this paper, we will most of the time discuss problems, where f is itself a polynomial of degree $k > 0$ that we want to approximate by a polynomial of degree at most $k-1$. The following fact will be of particular importance:

$$E_{k-1}(2^{k-1}x^k, [-1, 1]) = 1 \tag{3.3}$$

Moreover, the error function $2^{k-1}x^k - q_{k-1, 2^{k-1}x^k, [-1,1]}$ is the Chebyshev polynomial T_k (visualized in Figure 1). $T_k(x) = \cos(k\theta)$ is a polynomial of degree k in $x = \cos(\theta) \in [-1, 1]$ with leading coefficient

2^{k-1}. The extremal values ± 1 of T_k are attained in an alternating fashion $k+1$ times in interval $[-1,1]$ on the point set

$$Z_k = \{\cos((k-i)\pi/k) : i = 0, \ldots, k\}. \tag{3.4}$$

It is well-known (see [5], for instance) that the first derivation of T_k satisfies $T_k'(x) \le k^2$ for all $x \in [-1,1]$.

Clearly, $E_{k-1}(f,I) = 0$ if I is a finite set of size at most k. We may therefore assume that I contains at least $k+1$ points. Let $q \in P_{k-1}$ and J be a subset of I containing $k+1$ points $x_0 < x_1 < \cdots < x_k$. We say that *error function* $f-q$ *alternates on* J if the sign of $(f-q)(x_j)$ alternates for $j = 0,1,\ldots,k$. If, in addition, $|(f-q)(x_j)| = E(f,I,q)$, then J is called *an alternating set for* $f-q$ *on domain* I. It is well-known that there exists an alternating set for $f-q$ on domain I, iff $q = q_* = q_{k-1,f,I}$. We use the notation $J_{k-1,f,I}$ or simply J_* to indicate an alternating set for $f - q_*$ on domain I. It is furthermore known that $q_{k-1,f,I} = q_{k-1,f,J_*}$. It follows that

$$E_{k-1}(f,I) = \max_{J: J \subseteq I, |J| = 1+k} E_{k-1}(f,J), \tag{3.5}$$

where $J = J_{k-1,f,I}$ maximizes the right hand of this equation. Especially for $f \equiv 2^{k-1}x^k$ and $I = [-1,1]$, we get $J_{k-1,2^{k-1}x^k,[-1,1]} = Z_k$ and $q_{k-1,2^{k-1}x^k,[-1,1]} = q_{k-1,2^{k-1}x^k,Z_k}$.

3.2 Tight General Bounds on the Optimal Contrast In this subsection, we recall some of the main results from [4]. As explained in section 2, the largest possible contrast in a k-out-of-n scheme is the maximal profit in linear program $LP(k,n)$. The particular structure of $LP(k,n)$ is captured in more abstract terms by the following definition. We say that a linear program LP is of *type BAP (Best Approximating Polynomial)* if there exists a matrix $A \in \Re^{k \times (1+n)}$ and a vector $\vec{c} \in \Re^{n+1}$ 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 BAP

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

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

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

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

Furthermore, A and $\vec{c}$ must satisfy the following conditions:

(LP4) The vector space V_A spanned by the row vectors of A contains the all-ones vector $\vec{1}$.

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

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

(LP7) Each row vector in A is the evaluation vector of a polynomial of degree at most $k-1$.

Conditions (LP6) and (LP7) imply that V_A is the vector space consisting of all evaluation vectors of polynomials from P_{k-1}.[3]

Let

$$I_n = \{0,1,\ldots,n\} \text{ and } G_n = \{-1 + 2i/n : i = 0,1,\ldots,n\}. \tag{3.6}$$

The following result was proven in [4]:

THEOREM 3.1. *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 maximal profit $C(A,\vec{c})$ in $LP(A,\vec{c})$ satisfies*

$$C(A,\vec{c}) = 2E_{k-1}(\lambda x^k, I_n\}) = 4^{-(k-1)} n^k |\lambda| E_{k-1}(2^{k-1}x^k, G_n) \le 4^{-(k-1)} n^k |\lambda|.$$

[3]Thus, (LP4) is implied by (LP6) and (LP7). We mentioned (LP4) explicitly for ease of later reference.

We introduce the notation

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

for so-called "falling powers" and proceed with the following results from [4]:

LEMMA 3.1. *The linear program $LP(k,n)$ is of type BAP. The leading coefficient of the polynomial p with evaluation vector $\vec{c}$ is $(-1)^k/n^{\underline{k}}$.*

Making use of $\lim_{n\to\infty} E_{k-1}(2^{k-1}x^k, G_n) = E_{k-1}(2^{k-1}x^k, [-1,1])$, one easily gets

COROLLARY 3.1. *Let $C(k,n)$ denote the largest possible contrast in a k-out-of-n scheme. Then the following holds:*

$$4^{-(k-1)} = \lim_{n\to\infty} C(k,n) \le C(k,n) = 2E_{k-1}(x^k/n^{\underline{k}}, I_n) = 4^{-(k-1)}\frac{n^k}{n^{\underline{k}}}E_{k-1}(2^{k-1}x^k, G_n) \le 4^{-(k-1)}\frac{n^k}{n^{\underline{k}}}.$$

In other words, the largest possible contrast in a k-out-of-n scheme approaches $4^{-(k-1)}$ when n approaches infinity. For finite n, it exceeds this lower bound at most by factor $n^k/n^{\underline{k}}$.

4 Some Auxiliary Approximation-Theoretic Results

The equality $C(A,\vec{c}) = 2E_{k-1}(\lambda x^k, I_n)$ in Theorem 3.1 was derived in [4] by showing that $DLP(A,\vec{c})$ — the problem obtained from $LP(A,\vec{c})$ by dualization — is essentially the problem to find the polynomial $q \in P_{k-1}$ with smallest approximation error $E(\lambda x^k, I_n, q)$. In order to construct an asymptotically optimal basic feasible solution (bfs) for $LP(A,\vec{c})$, we will study modified linear programs obtained from $LP(A,\vec{c})$ by selecting a collection of basic variables and deleting each column in A which does not correspond to one of the selected variables. It turns out in section 5 that the dual to such a modified linear program has a more complex interpretation. The term that has to be minimized cannot in general be interpreted as the classical approximation error. Rather, it is a sort of "one-sided approximation error", where polynomial $q \in P_{k-1}$ is penalized for being below a target value λx^k for some points x, and penalized for being above a target value for others (but for each fixed point penalized in only one direction). In this section, we derive some central properties of this more complex measure for approximation error.

Let $J \subseteq I$ consist of points $x_0 < x_1 < \cdots < x_k$. Consider the following partition of J:

$$J_{even} = \{x_i : 0 \le i \le k, i \text{ is even}\} \text{ and } J_{odd} = \{x_i : 0 \le i \le k, i \text{ is odd}\} \tag{4.7}$$

An error function $f-q$ which alternates on J attains negative values on J_{even} and positive values on J_{odd}, or vice versa. In the former case, we say that $f-q$ *is of alternation-type* $\mp$ *on* J. In the latter case $f-q$ *is of alternation-type* $\pm$ *on* J. If J is an alternating set for $f-q$ on domain I, then $(f-q)(x) = -E_{k-1}(f,I)$ for all $x \in J_{even}$ and $(f-q)(x) = E_{k-1}(f,I)$ for all $x \in J_{odd}$, or vice versa. Let

$$\tau(f,J,q) = \min_{x\in J}|f(x)-q(x)|, \tag{4.8}$$

and observe that $\tau(f,J,q) > 0$ if $f-q$ alternates on J, and $\tau(f,J,q) = E_{k-1}(f,I)$ if J is an alternating set for $f-q$ on domain I. Inequality $E(f,J,q) \ge \tau(f,J,q)$ is valid for all $q \in P_{k-1}$.

We now define the new measure for approximation error that will play a central role in the construction of an almost optimal bfs in section 5. Quantity $E^{\mp}(f,J,q)$ is defined as the smallest real s such that

$$\forall x \in J_+ : q(x) + s \ge f(x) \text{ and } \forall x \in J_- : q(x) - s \le f(x), \tag{4.9}$$

where $J_- = J_{even}$ and $J_+ = J_{odd}$. Quantity $E^{\pm}(f,J,q)$ is defined symmetrically with $J_+ = J_{even}$ and $J_- = J_{odd}$. Note that $E^{\mp}(f,J,q) = E(f,j,q)$ if $f-q$ alternates on J with alternation-type $\mp$. Symmetrically, $E^{\pm}(f,J,q) = E(f,j,q)$ if $f-q$ alternates on J with alternation-type $\pm$. The central result in this subsection is the following

LEMMA 4.1. *Let $q_0 \in P_{k-1}$ and assume that $f-q_0$ alternates on J with alternation-type $\alpha \in \{\mp,\pm\}$. Then $\min_{q\in P_{k-1}} E^{\alpha}(f,J,q) \ge \tau(f,J,q_0)$.*

Proof. W.l.o.g. let $\alpha = \mp$. (The other case is symmetric.) For sake of brevity, let $s = E^{\mp}(f, J, q)$ and $t = \tau(f, J, q_0)$. For sake of contradiction, assume that $s < t$. Note first that for all $x \in J_- = J_{even}$:

$$f(x) - q(x) \geq -s > -t \geq -|f(x) - q_0(x)| = f(x) - q_0(x).$$

Note second that for all $x \in J_+ = J_{odd}$:

$$f(x) - q(x) \leq s < t \leq |f(x) - q_0(x)| = f(x) - q_0(x).$$

Thus, the sign of $(f - q) - (f - q_0) \equiv q_0 - q$ alternates on points $x_0, x_1, \ldots, x_k$, which implies that $q_0 - q$ has $k + 1$ roots. Since $q, q_0 \in P_{k-1}$, it follows that $q \equiv q_0$. Since $f - q_0$ alternates on J with alternation type $\mp$, we finally arrive at the following contradiction:

$$s = E^{\mp}(f, J, q) = E^{\mp}(f, J, q_0) = E(f, J, q_0) \geq \tau(f, J, q_0) = t.$$

The proof of Lemma 4.1 is similar to the proof of the Theorem of de la Vallée-Poussin [2] (which makes a technically slightly different statement).

Note that J must be an alternating set for $f - q_{k-1,f,J}$ on subdomain J, because there exists an alternating set that must be a subset of J of size $k+1$. Since $|J| = k+1$, J is the only candidate. Let $\alpha(J) \in \{\mp, \pm\}$ denote the alternation-type of $f - q_{k-1,f,J}$ on J. We claim that the following holds:

$$\min_{q \in P_{k-1}} E^{\alpha(J)}(f, J, q) = E_{k-1}(f, J) \tag{4.10}$$

$$\max_{J : J \subseteq I, |J| = k+1} \min_{q \in P_{k-1}} E^{\alpha(J)}(f, J, q) = E_{k-1}(f, I) \tag{4.11}$$

In both equations, the left hand cannot exceed the right hand. We claim that the left hand cannot be smaller. As for equation (4.10), this follows from Lemma 4.1 by setting $q_0 \equiv q_{k-1,f,J}$. Then $\min_{q \in P_{k-1}} E^{\alpha(J)}(f, J, q) \geq \tau(f, J, q_0) = E_{k-1}(f, J)$. Equation (4.11) follows similarly by setting $J = J_{k-1,f,I}$.

For each $x \in [-1, 1]$, pick the index $i(x) \in I_n$ such that $\hat{x} = -1 + 2i(x)/n \in G_n$ is the point in G_n that comes closest to x (say with the smaller index $i(x)$ in case of a tie). Let

$$J_{k,n} = \{i(x) : x \in Z_k\} \text{ and } G_{k,n} = \{\hat{x} : x \in Z_k\} = \{-1 + 2i/n : i \in J_{k,n}\}. \tag{4.12}$$

Remember that Z_k is an alternating set for T_k on domain $[-1, 1]$, and $T_k(x) = \pm 1$ for all $x \in Z_k$. Assume that $n > k^2$. Since $|x - \hat{x}| \leq 1/n$ and $T_k'(x) \leq k^2$ for all $x \in [-1, 1]$, $T_k(x) = 1$ implies that $T_k(\hat{x}) \geq 1 - k^2/n$, and $T_k(x) = -1$ implies that $T_k(\hat{x}) \leq -(1 - k^2/n)$. It follows that T_k alternates on $G_{k,n}$ with the same alternation-type, say α_k, as on Z_k, and

$$\tau\left(2^{k-1}x^k, G_{k,n}, q_{k-1,2^{k-1}x^k,[-1,1]}\right) = \min_{x \in G_{k,n}} |T_k(x)| \geq 1 - k^2/n \tag{4.13}$$

Let $\alpha_k^\lambda = \alpha_k$ if $\lambda > 0$, and the opposite alternation type if $\lambda < 0$. It is now easy to see that the following holds:

$$\min_{q \in P_{k-1}} E^{\alpha_k}(2^{k-1}x^k, G_{k,n}, q) \geq 1 - k^2/n \tag{4.14}$$

$$\min_{q \in P_{k-1}} E^{\alpha_k^\lambda}(\lambda x^k, J_{k,n}, q) \geq \frac{1}{2} 4^{-(k-1)} n^k |\lambda| (1 - k^2/n) \tag{4.15}$$

Inequality (4.14) is a direct consequence of Lemma 4.1 (with $q_{k-1,2^{k-1}x^k,[-1,1]}$ in the role of q_0) and (4.13). Inequality (4.15) results from (4.14) by applying a simple scaling argument, using the fact that the linear transformation $i \mapsto -1 + 2i/n$ maps $G_{k,n}$ onto $J_{k,n}$ and taking care of the sign of λ and of the different leading coefficients 2^{k-1} versus λ. We omit the details.

5 Constructions Approaching the Optimal Contrast

Let $1 \le k \le n$, $A \in \Re^{k \times (1+n)}$, and $\vec{c} \in \Re^{1+n}$. Let $LP(A, \vec{c})$ be a linear program of type BAP. Throughout this section, we denote by $p \in P_k$ the polynomial of degree k with evaluation vector $\vec{c}$, and by λ the leading coefficient of p. In matrix notation, constraints (LP2) and (LP3) read as follows:

$$\begin{pmatrix} 1\cdots 1 & 0\cdots 0 \\ 0\cdots 0 & 1\cdots 1 \\ A & -A \end{pmatrix} \begin{pmatrix} \vec{\xi} \\ \vec{\eta} \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \vec{0} \end{pmatrix} \tag{5.16}$$

According to condition (LP4), $A(\vec{\xi} - \vec{\eta}) = \vec{0}$ implies that $\sum_{j=0}^{n} \xi_j = \sum_{j=0}^{n} \eta_j$. Thus, constraint $\sum_{j=0}^{n} \eta_j = 1$ is redundant, and (5.16) can be slightly simplified as follows:

$$M \begin{pmatrix} \vec{\xi} \\ \vec{\eta} \end{pmatrix} = \begin{pmatrix} 1 \\ \vec{0} \end{pmatrix} \text{ where } M = \begin{pmatrix} 1\cdots 1 & 0\cdots 0 \\ A & -A \end{pmatrix}. \tag{5.17}$$

Constraint matrix M has $k+1$ rows and $2n+2$ columns. The first $n+1$ columns, called *ξ-columns* in the sequel, correspond to variables $\xi_0, \ldots, \xi_n$. The last $n+1$ columns, called *η-columns* in the sequel, correspond to variables $\eta_0, \ldots, \eta_n$. The rank of A is k according to (LP6). Since the first row of M cannot be written as linear combination of the row vectors of $(A, -A)$, M has rank $k+1$.

In order to discuss basic feasible solutions (bfs) for $LP(A, \vec{c})$, we introduce the following general notation. With each $K = (J_1, J_2)$, where $J_1, J_2 \subseteq I_n$, we associate the linear program $LP(A, \vec{c}|K)$ resulting from $LP(A, \vec{c})$ by adding the constraints $\xi_j = 0$ for all $j \notin J_1$ and $\eta_j = 0$ for all $j \notin J_2$. The constraint matrix for the remaining variables, denoted as M_K in the sequel, results from M by deleting all ξ- and η-columns with indices outside J_1 and J_2, respectively. $LP(A, \vec{c}|K)$ is obviously bounded. If it is also feasible, then it has a finite optimum denoted by $C(A, \vec{c}|K)$ in the sequel. Clearly, submatrix M_K is a basis of M iff it has $1+k$ columns and is of full rank $1+k$. If M_K is a basis of M, we denote the corresponding unique (not necessarily feasible) basic solution by ζ_K. If ζ_K happens to be feasible, then it is the unique bfs for $LP(A, \vec{c}|K)$ achieving profit $C(A, \vec{c}|K)$.

We will show that the best bfs for $LP(A, \vec{c}|K)$ can be obtained by an index set K of a very special form. To this end, let $J \subseteq I_n$ such that $|J| = k+1$, and define

$$K_J^{\mp} = (J_{odd}, J_{even}) \text{ and } K_J^{\pm} = (J_{even}, J_{odd}). \tag{5.18}$$

We say that K is an *alternating index set* if $K = K_J^{\alpha}$ for some $J \subseteq I_n$ of size $k+1$ and some $\alpha \in \{\mp, \pm\}$.

The main work in this section will be to study the linear program $DLP(A, \vec{c}|K)$ obtained from $LP(A, \vec{c}|K)$ by dualization, and to show the following

THEOREM 5.1. *If $K = K_J^{\alpha}$ is an alternating index set and $\min_{q \in P_{k-1}} E^{\alpha}(\lambda x^k, J, q) > 0$, then M_K is a basis of M and ζ_K is a (unique) bfs for $LP(A, \vec{c}|K)$ achieving profit $2\min_{q \in P_{k-1}} E^{\alpha}(\lambda x^k, J, q)$.*

We will postpone the proof of this theorem to a later stage and first describe our two main applications. The first application is the (non-constructive) specification of an optimal bfs for $LP(A, \vec{c})$. The second application is the construction of an asymptotically optimal bfs for $LP(A, \vec{c})$.

Application 1 Let $J_* = J_{k-1, \lambda x^k, I_n}$, $K_* = K_{J_*}^{\alpha(J_*)}$, and $\zeta_* = \zeta_{K_*}$. Making use of Theorem 5.1, equation (4.10), the special choice of J, and Theorem 3.1, we can conclude that bfs ζ_* achieves the largest possible profit

$$2 \min_{q \in P_{k-1}} E^{\alpha(J_*)}(\lambda x^k, J_*, q) = 2E_{k-1}(f, J_*) = 2E_{k-1}(\lambda x^k, I_n) = C(A, \vec{c}).$$

Thus, ζ_* is an optimal bfs for $LP(A, \vec{c})$. The specification of ζ_* is non-constructive in the sense that the functional dependence of J_* on parameters k and n is not known (although J_* can be computed algorithmically for fixed values of k and n by linear programming).

Especially for linear program $LP(k, n)$, bfs ζ_* achieves the optimal contrast $C(k, n)$ among all k-out-of-n schemes.

Application 2 Let $J_{k,n} \subseteq I_n$ be the index set (constructively) given by equation (4.12). Remember that $J_{k,n}$ is obtained from Z_k (the extrema of the Chebychev polynomial T_k on domain $[-1,1]$) by the simple rule to move each point from Z_k to its closest neighbour on the grid G_n. Let $K_{k,n} = K^{\alpha_k^\lambda}_{J_{k,n}}$, and $\zeta_{k,n} = \zeta_{K_{k,n}}$. According to Theorem 5.1, and (4.15), $\zeta_{k,n}$ achieves profit

$$2 \min_{q \in P_{k-1}} E^{\alpha_k^\lambda}(\lambda x^k, J_{k,n}, q) \geq 4^{-(k-1)} n^k |\lambda| (1 - k^2/n).$$

A comparison with Theorem 3.1 reveals that $\zeta_{k,n}$ is an asymptotically optimal bfs for $LP(A, \vec{c})$ (when n approaches infinity and k is fixed).
Especially for the linear program $LP(k,n)$, $\zeta_{k,n}$ is a bfs whose profit misses the upper bound on the largest possible contrast of a k-out-of-n scheme at most by factor $1 - k^2/n$.

In the sequel, we refer to the bfs described in Application 2 as the *Nearest Neighbour Solution.*

The remainder of this section is devoted to the study of $DLP(A, \vec{c}|K)$ and to the proof of Theorem 5.1. The general rule for dualization is as follows. If the primal problem is to maximize $\vec{p}\vec{x}$ subject to $\vec{x} \geq \vec{0}$ and $M\vec{x} = \vec{h}$, the corresponding dual problem is to minimize $\vec{h}\vec{y}$ subject to $M'\vec{y} \geq \vec{p}$.

We want to apply this rule to the primal problem $LP(A, \vec{c}|K)$, where $K = (J_1, J_2)$ and $J_1, J_2 \subseteq I_n$. In matrix notation, this is the problem to maximize $\vec{c}_{J_1}\xi_{J_1} - \vec{c}_{J_2}\eta_{J_2}$ subject to $\vec{\xi}_{J_1} \geq \vec{0}_{J_1}, \vec{\eta}_{J_2} \geq \vec{0}_{J_2}$ and

$$\begin{pmatrix} 1 \cdots 1 & 0 \cdots 0 \\ 0 \cdots 0 & 1 \cdots 1 \\ A_{J_1} & -A_{J_2} \end{pmatrix} \begin{pmatrix} \vec{\xi}_{J_1} \\ \vec{\eta}_{J_2} \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ \vec{0} \end{pmatrix}. \tag{5.19}$$

The corresponding dual problem has $2 + k$ variables, which we denote by s, t and $\vec{u} = (u_0, \ldots, u_{k-1})'$. It follows that $DLP(A, \vec{c}|K)$ is the problem to minimize $s + t$ subject to

$$\begin{pmatrix} \vec{1}_{J_1} & \vec{0}_{J_1} & A'_{J_1} \\ \vec{0}_{J_2} & \vec{1}_{J_2} & -A'_{J_2} \end{pmatrix} \begin{pmatrix} s \\ t \\ \vec{u} \end{pmatrix} \geq \begin{pmatrix} \vec{c} \\ -\vec{c} \end{pmatrix} \tag{5.20}$$

The latter constraints are equivalent to

$$\forall j \in J_1 : A_j\vec{u} + s \geq c_j \text{ and } \forall j \in J_2 : A_j\vec{u} - t \leq c_j. \tag{5.21}$$

Remember that the row vectors of A span the vector space of all evaluation vectors of polynomials from P_{k-1}. Since $A'\vec{u}$ is a linear combination of the row vectors of A, the choice of $\vec{u}$ fixes a particular polynomial q from P_{k-1}. Remember furthermore that $c_j = p(j)$ for polynomial p of degree k with leading coefficient λ. Thus, $DLP(A, \vec{c}|K)$ is the problem to select a polynomial q from P_{k-1} such as to minimize $s + t$ subject to

$$\forall j \in J_1 : q(j) + s \geq p(j) \text{ and } \forall j \in J_2 : q(j) - t \leq p(j). \tag{5.22}$$

It is obvious that $DLP(A, \vec{c}|K)$ is feasible. Given any $q \in P_{k-1}$, the best values for variables s and t are

$$\begin{aligned} s(A, \vec{c}, K, q) &= \min\{r \in \Re : q(j) + r \geq p(j) \text{ for all } j \in J_1\} && (5.23) \\ t(A, \vec{c}, K, q) &= \min\{r \in \Re : q(j) - r \leq p(j) \text{ for all } j \in J_2\}. && (5.24) \end{aligned}$$

Since $p \in P_k$ with leading coefficient λ and q ranges over all polynomials from P_{k-1}, we may assume w.l.o.g. that $p \equiv \lambda x^k$. Finally observe that, by adding an appropriate constant, each polynomial $q \in P_{k-1}$ can be normalized such that $s(A, \vec{c}, K, q) = t(A, \vec{c}, K, q)$. This normalization and $p \equiv \lambda x^k$ is assumed in the sequel.

$DLP(A, \vec{c}|K)$ is bounded iff $LP(A, \vec{c}|K)$ is feasible. In this case, both linear programs have finite optima and, by duality, $C(A, \vec{c}|K) = 2\min_{q \in P_{k-1}} s(A, \vec{c}, K, q)$.
These discussions can be summarized as follows:

THEOREM 5.2. *Let $K = (J_1, J_2)$ for index sets $J_1, J_2 \subseteq I_n$. Then the following holds:*

1. *$DLP(A,\vec{c}|K)$ is the problem to find a polynomial $q \in P_{k-1}$ with* minimal loss *s, where the loss of q, denoted by $s(A,\vec{c},K,q)$, is the smallest $s \in \Re$ such that*

$$\forall j \in J_1 : q(j) + s \geq \lambda j^k \text{ and } \forall j \in J_2 : q(j) - s \leq \lambda j^k. \tag{5.25}$$

2. *$LP(A,\vec{c}|K)$ is always bounded and $DLP(A,\vec{c}|K)$ is always feasible.*

3. *If both linear programs have finite optima, then $C(A,\vec{c}|K) = 2\min_{q\in P_{k-1}} s(A,\vec{c},K,q)$.*

We proceed with a technical auxiliary result, whose (more or less straightforward) proof is omitted in this brief abstract.

LEMMA 5.1. *Let $J_1, J_2 \subseteq \{0,1,\ldots,n\}$, $|J_1|+|J_2| = 1+k$, and $K = (J_1,J_2)$. If $LP(A,\vec{c}|K)$ is feasible and $C(A,\vec{c}|K) > 0$, then M_K is a basis of M.*

For each alternating index set K_J^α, a comparison of condition (5.25), the definition of $K^\mp, K^\pm$ in (5.18), and the definition of $E^\mp, E^\pm$ in section 4 reveals that

$$s(A,\vec{c},K_J^\alpha,q) = E^\alpha(\lambda x^k, J, q). \tag{5.26}$$

The proof of Theorem 5.1 is now accomplished as follows. Let $K = K_J^\alpha$. According to statement 1 in Theorem 5.2 and equation (5.26), $DLP(A,\vec{c}|K)$ is the problem to find a polynomial $q \in P_{k-1}$ leading to the smallest possible value of $E^\alpha(\lambda x^k, J, q)$. Given the assumption that the smallest possible value is strictly positive, we conclude that $DLP(A,\vec{c}|K)$ is bounded and $LP(A,\vec{c}|K)$ is feasible. Thus both linear programs have finite optima. According to statement 3 in Theorem 5.2 combined with equation (5.26), $C(A,\vec{c}|K) = 2\min_{q\in P_{k-1}} E^\alpha(\lambda x^k, J, q)$. According to Lemma 5.1, M_K is a basis. We conclude that ζ_K is a bfs achieving the desired profit. •

We close this paper with the following final remarks. We have described a universal and surprisingly simple construction of asymptotically optimal basic feasible solutions for linear programs of type BAP. Applied to the particular linear program $LP(k,n)$, this yields a bfs which represents a k-out-of-n scheme with asymptotically optimal contrast. For finite n, there is still a small (asymptotically vanishing) gap between the optimal contrast and the contrast achieved by our construction. This gap cannot be closed without solving an open problem in Approximation Theory, namely to find the best approximating polynomial of degree at most $k-1$ for $2^{k-1}x^k$ on domain G_n (whose error function would be the discrete counterpart of the Chebychev polynomial). As briefly sketched in Appendix A, we are able to close the gap for $k \leq 4$ and arbitrary n. An example of a contrast-optimal 3-out-of-8 scheme is visualized in Figures 2, 3, 4, and 5. We finally mention that the procedure from [3] that converts a given bfs for $LP(k,n)$ to the explicit representation of the underlying k-out-of-n-scheme is constructive, but quite inefficient for large values of k and n. In particular, the number of subpixels per pixel is intolerably large. We leave the task to determine (as precise as possible) the tradeoff between visual contrast (which should be large) and the number of subpixels per pixel (which should be small) as an object of future research.

A Schemes with Optimal Contrast for Small Values of k

In order to determine $J_* = J_{k-1,f,I}$, the following general facts may be helpful. Let $J \subseteq I$ consist of $k+1$ points $x_0 < x_1 < \cdots < x_k$. Let Q be the polynomial of degree k given by $Q(x_i) = f(x_i)$ for all $i = 0,\ldots,k$, and R be the polynomial of degree k given by $R(x_i) = (-1)^i$. Then $q_{k-1,f,J}$ is of the form $Q - cR$, where constant c must be chosen such that $Q - cR \in P_{k-1}$. Thus, if λ_Q and λ_R are the leading coefficients of Q and R, respectively, then $c = \lambda_P/\lambda_R$. Moreover, $E_{k-1,f,J} = |c|$. The punchline of this discussion is as follows. If we consider $\bar{x} = (x_0, x_1, \ldots, x_k)$ as vector of $k+1$ real-valued variables, then $c = c(\bar{x})$ is a rational function in $\bar{x}$ with a unique maximum of $|c|$ in I^{k+1}. The vector $\bar{x}$ leading to this maximum determines $J_{k,f,I}$. We briefly note that

$$\lambda_R = \sum_{i=0}^{k} \frac{(-1)^i}{\prod_{0\leq j\leq k, j\neq i}(x_i - x_j)|} \text{ and } |\lambda_R| = \sum_{i=0}^{k} \frac{1}{\prod_{0\leq j\leq k, j\neq i}|x_i - x_j|}. \tag{1.27}$$

We now pass to the special case, where $I = G_n$ and $f \equiv P \equiv 2^{k-1}x^k$ is a polynomial of degree k with leading coefficient 2^{k-1}. The rational function c discussed above reads now as follows:

$$|c(x_0, x_1, \ldots, x_k)| = 2^{k-1} / \sum_{i=0}^{k} \frac{1}{\prod_{0 \le j \le k, j \ne i} |x_i - x_j|}. \tag{1.28}$$

In order to maximize this function, we have to find the points $x_0^* < x_1^* < \cdots < x_k^*$ from G_k which minimize the function

$$F_k(x_0, x_1, \ldots, x_k) = \sum_{i=0}^{k} \frac{1}{\prod_{0 \le j \le k, j \ne i} |x_i - x_j|}. \tag{1.29}$$

Note that the extremals of the Chebychev polynomial $x_i = \cos((k-i)\pi/k)$ minimize F_k over $[-1,1]^{k+1}$. However, the points x_i must be picked from G_n which makes the minimization problem much more difficult. It is however obvious that $x_0^* = -1$ and $x_k^* = 1$. This leaves open only the determination of $x_1^*, \ldots, x_{k-1}^*$. In the sequel, we discuss the cases $k = 2, 3, 4$.

Let's first consider the simple case $k = 2$. For even n, $0 \in G_n$ and $x_1^* = 0$. For odd n, it is easy to see that $x_1^* = 1/n$ (or alternatively $-1/n$). Thus, $J_{1,2^{k-1}x^k,G_n} = \{-1, 0, 1\}$ for even n, and $J_{1,2^{k-1}x^k,G_n} = \{-1, 1/n, 1\}$ for odd n. Note that this coincides with the Nearest Neighbour Solution $J_{2,n}$ (described in Section 5). Let $\nu = 0$ ($\nu = 1$, resp.) for n even (odd, resp.). As for the optimal contrast, we obtain

$$C(2,n) = \frac{(n-\nu)(n+\nu)}{4n(n-1)}$$

and the corresponding bfs ξ, η is given by

$$\xi_0 = 1 - \xi_n = \frac{1}{2}\left(1 - \frac{\nu}{n}\right)$$
$$\eta_{(n+\nu)/2} = 1,$$

where the remaining values vanish.

For $k = 3$, a much more involved analysis of F_3 shows that still the Nearest Neighbour Solution $J_{3,n}$ is optimal. The corresponding optimal bfs for $LP(3,n)$ has the form

$$\xi_0 = \eta_n = \frac{n-\nu}{3n-\nu}$$
$$\xi_{n-t} = \eta_t = \frac{2n}{3n-\nu},$$

where $t = n(1-2\nu)/4$ and

$$\nu = \begin{cases} 0 & \text{for } n \equiv 0 \pmod 4 \\ +1 & \text{for } n \equiv 1 \pmod 4 \\ \pm 2 & \text{for } n \equiv 2 \pmod 4 \\ -1 & \text{for } n \equiv 3 \pmod 4. \end{cases}$$

Again, ξ_i and η_i vanish for all remaining variables. Here, the best contrast is

$$C(3,n) = \frac{(n+\nu)(n-\nu)}{16(n-1)(n-2)} \ge \frac{1}{16}.$$

Especially for $n = 8$, the conversion of the above Nearest Neighbour Solution into a 3-out-of-8 secret sharing scheme needs 42 subpixels per pixel. (Compare again with Figures 2, 3, 4, and 5.) Since the optimal contrast is $2/21$ in this case, this is second smallest conceivable number of subpixels.[4]

For $k = 4$, an even more involved analysis shows that Nearest Neighbour Solutions $J_{4,n}$ are not optimal for all values of n. $J_{3,2^{k-1}x^k,G_n}$ can still be exactly determined. The quite complicated formulas for x_i^* (and for the resulting bfs) in dependence of n and for the optimal contrast $C(4,n)$ will be presented in the full paper.

[4]As a function of k and n, the number of subpixels per pixel grows however too fast.

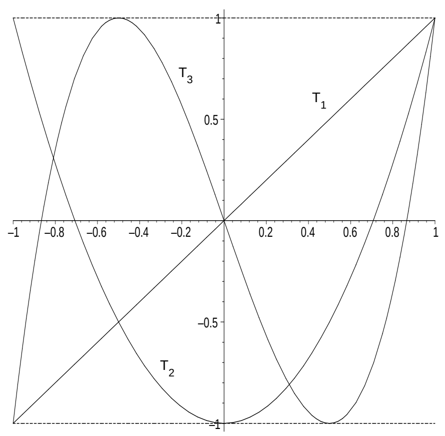

Figure 1: The Chebyshev polynomial T_k of degree k for $k = 1, 2, 3$. $T_k(x) = \cos(k\theta)$, where $0 \leq \theta \leq \pi$ and $x = \cos(\theta)$.

Acknowledgement
We are grateful to Dietrich Braess for helpful comments and for pointing out attention to the Theorem of de la Vallée-Poussin.

References

[1] G. Ateniese, C. Blundo, A. de Santis, and D. R. Stinson. Visual cryptography for general access structures. In *Proceedings of the 23rd International Colloquium on Automata, Languages, and Programming — ICALP '96*, pages 416–428. Springer Verlag, 1996.
[2] Dietrich Braess. Nonlinear Approcimation Theory. Springer Verlag, 1986.
[3] Thomas Hofmeister, Matthias Krause, and Hans Ulrich Simon. Contrast-optimal k out of n secret sharing schemes in visual cryptography. In *Proceedings of the 3rd International Conference on Computing and Combinatorics — COCOON '97*, pages 176–186. Springer Verlag, 1997. Full version will appear in Theoretical Computer Science.
[4] Matthias Krause and Hans Ulrich Simon. On contrast-optimal secret sharing schemes in visual cryptography. Technical Report 255, Fakultät für Mathematik der Ruhr-Universität Bochum, D-44780 Bochum, 1999.
[5] Nathan Linial and Noam Nisan. Approximate inclusion-exclusion. *Combinatorica*, 10:349–365, 1990.
[6] Moni Naor and Adi Shamir. Visual cryptography. In *Proceedings of the Conference on Advances in Cryptology — Eurocrypt '94*, pages 1–12. Springer Verlag, 1995.
[7] Moni Naor and Adi Shamir. Visual cryptography II: Improving the contrast via the cover base. In *Proceedings of the International Workshop on Security Protocols*, pages 69–74. Springer Verlag, 1997.
[8] Christos H. Papadimitriou and Kenneth Steiglitz. *Combinatorial Optimization: Algorithms and Complexity.* Prentice Hall, 1982.
[9] Theodore J. Rivlin. *An Introduction to the Approximation of Functions.* Blaisdell Publishing Company, 1969.