Two Results on the Bit Extraction Problem

Katalin Friedl* Shi-Chun Tsai†

Abstract

An (n,s,t)-resilient function is a function $f:\{1,-1\}^n \to \{1,-1\}^s$, such that every element in $\{1,-1\}^s$ has the same probability to occur when t arbitrary input variables are fixed by an adversary and the remaining $n-t$ variables are assigned -1 or 1 uniformly and independently. A basic problem is to find the largest possible t given n and s such that an (n,s,t)-resilient function exists. As mentioned in [5, 2, 3] resilient functions have been involving in some interesting cryptographic applications, such as amplifying privacy and generating shared random strings in the presence of faulty processors.

The following coloring problem is closely related to resilient functions. A good coloring of the n-dimensional boolean cube with $c=2^s$ colors is such that in every k-dimensional subcube each color appears $2^k/c$ times. Here we are interested in the smallest k for which such a coloring exists.

A coloring is locally symmetric if each vertex in the n-cube has the same number of neighbors from each color other than its own. An XOR-type coloring is one obtained by a linear map $GF(2)^n \to GF(2)^s$. We answer the following problems proposed by Friedman [5]: *(1) If $c-1|n$, are all optimal colorings necessarily locally symmetric? (2) Are there optimal colorings not obtainable as XOR type colorings?*

We provide positive answers to both questions. For (2), we show that there are infinitely many non-XOR type optimal solutions, which is also proved by Stinson et al. with a different method [8]. Our main tool is an expression of the eigenvalues of the distance-i adjacency matrix of the n-cube via the Krawtchouk polynomials.

With the technique, we are able to make the background of some claims in [5, page 318] clearer. Along the way we prove some identities involving the distance distribution of color classes, in order to gain a better understanding of the structure of color classes.

keywords: resilient function; bit extraction; Krawtchouk polynomial

1 Introduction

Let $n \geq s \geq 1$ be integers and $f:\{1,-1\}^n \to \{1,-1\}^s$. We call f an (n,s,t)-resilient function, if for every t-subset $\{i_1,...,i_t\} \subseteq \{1,...,n\}$, for every choice of $z \in \{1,-1\}^t$ and every $y \in \{1,-1\}^s$, we have $Pr[f(x_1,...,x_n)=(y_1,...,y_s)|x_{i_j}=z_j,\ 1 \leq j \leq t] = 1/2^s$. Resilient

*Computer and Automation Research Institute, Hungarian Academy of Sciences, Budapest, Lágymányosi u. 11. H-1111, Hungary. Email: kati@ilab.sztaki.hu. Most of the work was done while at the Department of Computer Science, University of Chicago. Supported in part by OTKA Grant No. 2581.

†Department of Information Management, National Chi-Nan University, 1 University Road, Pu-Li, Nan-Tou 545, TAIWAN, Email: tsai@csie.ncnu.edu.tw. Most of the work was done while at the Department of Computer Science, University of Chicago.

functions were introduced and studied in [2, 4, 6, 8, 3]. The problem to construct resilient functions is also known as the bit extraction problem. Resilient functions arise in the context of cryptography, such as amplifying privacy and generating shared random strings in the presence of faulty processors [2, 5]. Recently, Stinson et al. [6, 3, 8] have made some progress on designing certain resilient functions, by using techniques from coding theory. Using the Nordstrom-Robinson code, they constructed a non-linear optimal $(16, 8, 5)$-resilient function [8]. In [3], Stinson et al. proved upper and lower bounds for the optimal values of t for $1 \leq n \leq 25$ and $1 \leq s \leq n$. However, it is still not clear how to construct optimal resilient functions in general.

In this paper we focus on an equivalent problem about a special type of coloring of the n-dimensional boolean cube. Consider the n-dimensional boolean cube B^n with vertex labels from $\{1, -1\}^n$. A k-dimensional sub-cube is a subset of B^n with certain $n-k$ coordinates fixed. We use $\mathcal{H}_k$ to denote the set of all k-dimensional sub-cubes. The *coloring problem* we consider is to color B^n with $c = 2^s$ colors such that every color appears in every k-dimensional sub-cube exactly $2^k/c$ times. Following Friedman [5] we call such a coloring a $(c; n, k)$-coloring. We are interested in the smallest integer k achievable for given n and c. Such a $(c; n, k)$-coloring is *optimal* if k is the smallest one for given c and n. This minimal value of k (with given n and c) is denoted by $\kappa(c, n)$. It is clear that $\log c$ is always a lower bound for κ. This bound is useful when c is large. Note that c can be as large as 2^n and when $c = 2^{O(n)}$, $\log c$ is a good lower bound. We mostly study cases when c is not this large, say $O(n)$. In these cases, as Friedman proved, the $\log n$ bound is far from the best possible.

It is easy to see that the existence of a $(c; n, k)$-coloring implies the existence of a $(c; n, k+1)$-coloring and a $(c/2; n, k)$-coloring, while a $(c; n, k)$-coloring does not imply a $(c; n, n-k)$-coloring, unless $k \leq n/2$.

It is not hard to see that the coloring problem is equivalent to the t-resilient function problem. Given n and s, from a $(2^s; n, k)$-coloring we can define an $(n, s, n-k)$-resilient function, and vice versa. The range of the resilient function corresponds to the possible colors in the coloring problem. For example the above-mentioned non-linear optimal (16,8,5)-resilient function defines an optimal $(2^8; 16, 11)$-coloring. Note that in this case the number of colors is much larger than the dimension of the cube.

Given c and n, Friedman [5] proved that $\kappa(c, n) \geq 1 + \frac{(c-2)n}{2(c-1)}$. This lower bound for $\kappa(c, n)$ is not tight when c is large. For instance, if $c = 2^{n-2}$ then $\kappa(c, n) = n - 1$ whereas the lower bound is about $n/2$.

Chor et al. [4] introduced XOR-colorings, defined as $f : B^n \rightarrow B^s$, where $f = (f_1, ..., f_s)$ and each f_i is an XOR function on a subset of the inputs. Friedman proved that the XOR-colorings constructed in [4] achieve the lower bound in the case when $n \geq 2$ and $n \equiv -2, -1, 0, 1, c/2 - 1, c/2, c/2 + 1 \,(mod\ c - 1)$, and thus are optimal in these cases. For general c and n, it is not clear whether XOR-colorings are the best possible [5]. The XOR-colorings of [4] are the only known systematic coloring method that achieves the optimal coloring (for certain c and n [5]).

To classify all optimal colorings for $c-1|n$, Friedman [5] defined *locally symmetric colorings* as colorings $\gamma : B^n \rightarrow B^s$, such that for some η and for all $v \in B^n$, v has exactly $n(1-\eta)/(c-1)$ neighbors of each color other than $\gamma(v)$; and he proposed the following two open problems:

1. *If $c - 1|n$, are all optimal colorings necessarily locally symmetric?*

2. *Are there optimal colorings not obtainable as XOR type colorings?*

Our main results are the followings. They are proved in Theorem 11 and 12.

1. *If $c-1|n$, then all optimal $(c;n,k)$-coloring must be locally symmetric.*
2. *For $c-1|n-1, c \geq 4$, there exist optimal colorings for B^n which are neither locally symmetric nor XOR type coloring.*

We also make clear a couple equations in [5, page 318], which were not known to have direct combinatorial proofs. The main technique used in this paper, as in [5], is the spectral method. We simplify some of the proofs of [5] by considering the distance-i adjacency matrix $A_{n,i}$ of the boolean cube B^n instead of the i-th power of the adjacency matrix of B^n, and relating Krawtchouk polynomials, a class of orthogonal polynomials, to the eigenvalues of $A_{n,i}$.

Along the way we study the distance distribution of the color classes and prove some identities involving the distance distribution of a color class, and between two different color classes. For $c-1|n$ we can calculate the distance distribution precisely for each color class. In this case it follows that all color classes of a $(c;n,k)$-coloring share the same distance distribution.

The rest of the paper is organized as follows. In Section 2 we give some basic definitions and review known facts. In Section 3 we present the connection between Krawtchouk polynomials and the eigenvalues of distance-i adjacency matrix, and some related results. In Section 4 we prove the main results which answer the open questions in [5]. Section 5 contains some open problems.

2 Notation, definitions and facts

We denote the distance-i adjacency matrix of the n-dimensional boolean cube by $A_{n,i}$, i.e. for all $x,y \in \{-1,1\}^n$, $A_{n,i}(x,y)=1$ if the Hamming distance of x and y is i; 0 otherwise. Note that each $A_{n,i}$ is a $2^n \times 2^n$ matrix and it corresponds to a regular graph of degree $\binom{n}{i}$ on the vertex set $\{-1,1\}^n$. Let x,y be two vectors of the same dimension, then $<x,y>=\sum_i x_i y_i$ denotes their inner product. We use $[n]$ to denote the set $\{1,...,n\}$ and $\mathcal{H}_k$ for the k dimensional subcube.

Definition. A set $C \subset B^n$ is called $1/c$ *dense in* $\mathcal{H}_k$ if for every $H \in \mathcal{H}_k$, $|C \cap H| = |H|/c$.

For any set $S \subseteq B^n$, we use χ_S to represent its characteristic vector. By averaging, every set which is $1/c$ dense in $\mathcal{H}_k$ has size $2^n/c$. We define 2^n vectors in the 2^n-dimensional space. The vectors will be indexed by subsets of $[n]$, the coordinates correspond to n-tuples of ± 1. For $(x_1,...,x_n) \in B^n$ and $T \subseteq [n]$, we define $v_T(x_1,...,x_n) := \Pi_{i \in T} x_i$. In particular, v_0 is the constant vector with all entries 1. It is clear that for $S,T \subseteq [n]$, if $S \neq T$ then $v_S \perp v_T$. Therefore $\{v_T | T \subseteq [n]\}$ forms a basis of the 2^n-dimensional vector space; in fact these vectors form a $2^n \times 2^n$ Hadamard matrix. Let $C \subseteq B^n$ be a $1/c$ dense subset in $\mathcal{H}_k$. Then χ_C has the following property, which plays a crucial role in [5]. For completeness we include a proof of this important property.

Fact 1 *[5, 4] For every $T \subset [n]$ with $1 \leq |T| \leq n-k$, $\chi_C \perp v_T$.*

Proof. Let M be a $2^n \times n$ matrix, whose (i,j) entry is $(-1)^{bin(i)_j}$, where $bin(i)_j$ denotes the j-th bit of the n-bit binary expansion of i. Let $T \subseteq [n]$ then v_T can be obtained by doing the component wise multiplications of the columns in M indexed by the set T. As we mentioned earlier, v_T is also the truth table of the parity function $\Pi_{i\in T} x_i$, for $x_i \in \{-1,1\}, i = 1,...,n$.

Each row of M can be used to represent a vertex of B^n. Given any $T \subset [n]$, let M_T be the sub-matrix of M that has the columns of M indexed by T. It is clear that each element in $\{-1,1\}^{|T|}$ appears exactly $2^{n-|T|}$ times in M_T as a row. And each set of identical rows in M_T denotes an $(n-|T|)$-subcube. As long as $1 \leq |T| \leq n-k$, χ_C has $2^{n-|T|}/c$ 1's at the entries corresponding to each set of identical rows, because C is a $1/c$ dense subset in $\mathcal{H}_k$. It is clear that v_T has half of the entries 1 and the others -1. Therefore $< \chi_C, v_T >= 0$. $\square$

Definition. Let $S \subset B^n$. We define $N_i(S)$ to be $|\{(s,t) : s,t \in S, \text{and } \text{dist}(s,t) = i\}|$, where $\text{dist}(s,t)$ is the number of positions in which s and t differ (Hamming distance). We call the sequence $(N_0(S),...,N_n(S))$ the *distance distribution* of S.

Note that for any set $S \subset B_n$, $\sum_{i=0}^{n} N_i(S) = |S|^2$. It is not hard to see that $< \chi_S A_{n,k}, \chi_S >= N_k(S)$.

Definition. [7] For any positive integer n and any prime power q, the *Krawtchouk polynomial* $P_i(x;n,q)$ is defined by

$$P_i(x;n,q) = \sum_{j=0}^{i} (-1)^j (q-1)^{i-j} \binom{x}{j} \binom{n-x}{i-j}, i = 0,1,2,...$$

where x is an indeterminate.

Observe that $P_i(x;n,q)$ is the coefficient of z^i in the expansion of $(1+(q-1)z)^{n-x}(1-z)^x$. In this paper we use only the case $q = 2$, and we let $P_i(x) = P_i(x;n,2)$. The first few Krawtchouk polynomials are $P_0(x) = 1, P_1(x) = n-2x, P_2(x) = \binom{n}{2} - 2nx + 2x^2$. There are many interesting properties of the Krawtchouk polynomials [7]. They form (finite) families of orthogonal polynomials w.r.t. certain discrete weight distributions, as seen from the following formula.

Fact 2 *[7] For non-negative integers r, s,*

$$\sum_{i=0}^{n} \binom{n}{i} (q-1)^i P_r(i;n,q) P_s(i;n,q) = q^n (q-1)^r \binom{n}{r} \delta_{r,s}.$$

It follows that any polynomial $P(x)$ of degree $\ell \leq n$ can be represented as $P(x) = \sum_{i=0}^{\ell} a_i P_i(x)$, which is called the *Krawtchouk expansion* of $P(x)$.

3 Technical results

We start with an expression of the eigenvalues of the distance-i adjacency matrix of the n-cube through the Krawtchouk polynomials (cf. [1], Chap. 3.2). In section 4, we use this relation to prove our main results.

Theorem 3 *For any non-negative integer $k \le n$, $A_{n,k}$ has eigenvalues $P_k(i)$, for $i = 0, 1, \cdots, n$ and $\{A_{n,k} : k = 0, ..., n\}$ can be diagonalized simultaneously. More specifically, $A_{n,k}v_T = P_k(|T|)v_T$, for all $T \subseteq [n]$.*

Proof.

For completeness , we include a simple proof. Recall that $B^n = \{-1, 1\}^n$. Let $x \in B^n$ and $T \subseteq [n]$. Consider the vector v_T defined earlier. For any $y \in B^n$, let y_T be the substring of y indexed by T. We count the number of distance-k neighbors of x. Let $D_j(x) = \{y : \text{dist}(x, y) = k \text{ and } \text{dist}(x_T, y_T) = j\}$, for $j = 0, ..., k$. By simple counting, we have $|D_j(x)| = \binom{|T|}{j}\binom{n-|T|}{k-j}$. Let $A_{n,k}(x)$ be the row of the matrix $A_{n,k}$ indexed by x. Then

$$\begin{aligned} < A_{n,k}(x), v_T > &= \sum_{y \in B^n; \text{dist}(x,y)=k} (\prod_{i \in T} y_i) \\ &= \sum_{j=0}^{k} \sum_{y \in D_j(x)} (\prod_{i \in T} y_i)(\prod_{i \in T} x_i)^2 \\ &= (\prod_{i \in T} x_i) \sum_{j=0}^{k} (-1)^j \binom{|T|}{j} \binom{n - |T|}{k - j} \\ &= (\prod_{i \in T} x_i) P_k(|T|). \end{aligned}$$

Thus we have proved that $A_{n,k}v_T = P_k(|T|)v_T$. $\square$

It follows that the eigenvalues of the matrix $\sum_{k=0}^{n} a_k A_{n,k}$ are $\sum_{k=0}^{n} a_k P_k(i)$, for $i = 0, ..., n$ and all such matrices share the same set of eigenvectors. For each i the corresponding eigenspace is of dimension $\binom{n}{i}$. Since every polynomial $f(x) \in R[x]$ of degree at most n can be represented in terms of Krawtchouk polynomials, there is a corresponding matrix M_f with eigenvalues $f(i)$, for $i = 0, ..., n$. The following important identity is stated as a problem in [7], on page 153.

Lemma 4 $\sum_{i=0}^{j} \binom{n-i}{n-j} P_i(x; n, q) = q^j \binom{n-x}{j}$.

Proof. Follows from the equation $(1 + (q - 1)z)^{n-x}(1 - z)^x = \sum_{i=0}^{n} P_i(x; n, q)z^i$, substituting $\frac{1}{1+y}$ for z. Then

$$\begin{aligned} (1 + y)^n \sum_{i=0}^{n} P_i(x; n, q)(1 + y)^{-i} &= \sum_{i=0}^{n} P_i(x; n, q)(1 + y)^{n-i} \\ &= \sum_{i=0}^{n} P_i(x; n, q) \sum_{j=0}^{n-i} \binom{n - i}{j} y^j \\ &= \sum_{j=0}^{n} \sum_{i=0}^{j} P_i(x; n, q) \binom{n - i}{n - j} y^{n-j}. \end{aligned}$$

So $\sum_{i=0}^{j} \binom{n-i}{n-j} P_i(x; n, q)$ is simply the coefficient of y^{n-j} in the expansion of $(1 + y)^n(1 + (q - 1)/(1 + y))^{n-x}(1 - 1/(1 + y))^x$, which turns out to be

$$(1 + y)^n (\frac{q + y}{1 + y})^{n-x} (\frac{y}{1 + y})^x = (q + y)^{n-x} y^x$$

$$= \sum_{j=0}^{n-x} q^j \binom{n-x}{j} y^{n-j}.$$

This completes the proof. $\square$

This identity helps to simplify some of the proofs in [5] and obtain a better understanding of the $1/c$ dense sets. More importantly, for $c-1|n$, we can precisely calculate the distance distribution.

Proposition 5 *Given a subset of B^n $1/c$ dense in $\mathcal{H}_k$, let $\{N_i\}$ be its distance distribution. Then $\sum_{i=0}^{j} \binom{n-i}{n-j} N_i = \frac{2^{n+j}}{c^2}\binom{n}{j}$, for $j \geq k$.*

Proof. Let χ be the characteristic vector of the $1/c$ dense set. We can write $\chi = \sum_{T\subseteq[n]} a_T v_T$. It is clear that $a_0 = \frac{<\chi, v_0>}{<v_0, v_0>} = 1/c$. From Lemma 4, we have $\sum_{i=0}^{j} \binom{n-i}{n-j} P_i(x) = 2^j \binom{n-x}{j}$. Let $B_{n,j} = \sum_{i=0}^{j} \binom{n-i}{n-j} A_{n,i}$. Then $< \chi B_{n,j}, \chi >= \sum_{i=0}^{j} \binom{n-i}{n-j} < \chi A_{n,i}, \chi > = \sum_{i=0}^{j} \binom{n-i}{n-j} N_i$. Note that $\binom{n-x}{j}$ has roots $n, n-1, ..., n-j+1$, which implies for every $S \subseteq [n]$ with $|S| \geq n-j+1$, we have $B_{n,j} v_S = 0 v_S$. Recall that $v_T \perp \chi$, for all $T \subset [n]$ with $1 \leq |T| \leq n-k$. Thus if $j \geq k$ then $< \chi B_{n,j}, \chi >= 2^j \binom{n}{j} a_0^2 < v_0, v_0 >= \frac{2^{n+j}}{c^2}\binom{n}{j}$. $\square$

We can generalize the above to a pair of disjoint $1/c$ dense sets. Let C_1 and C_2 be two disjoint $1/c$ dense sets in $\mathcal{H}_k$, and χ_1 and χ_2 be the corresponding characteristic vectors. We define $N_i(C_1, C_2) = |\{(x, y) : x \in C_1, y \in C_2, \text{ and } \mathrm{dist}(x, j) = i\}|$, which is similar to the distance distribution. It is not hard to see that $< \chi_1 A_{n,i}, \chi_2 >= N_i(C_1, C_2)$. Similarly to the Prop. 5, we can prove the following.

Proposition 6 *For any two disjoint $1/c$ dense sets in $\mathcal{H}_k$, say C_1, C_2, we have*

$$\sum_{i=0}^{j} \binom{n-i}{n-j} N_i(C_1, C_2) = \frac{2^{n+j}}{c^2}\binom{n}{j}, \text{ for } j \geq k. \quad \square$$

We shall use the following results of [5]. We mention that these results also follow from our machinery. Let $S_j(x) = 2^j\binom{n-x}{j}$. As in the proof of Proposition 5 we have $B_{n,j} = \sum_{i=0}^{j} \binom{n-i}{n-j} A_{n,i}$ and $< \chi_C B_{n,j}, \chi_C >= \sum_{i=0}^{j} \binom{n-i}{j-i} N_i$. For $c-1|n$, we always let $k = 1 + \frac{(c-2)n}{2(c-1)}$ unless stated otherwise.

Lemma 7 *[5] Let $C \subset B^n$ be an arbitrary subset of size $2^n/c$.*

1. *For $c-1|n$ and $j < k$, we have*

$$< \chi_C B_{n,j}, \chi_C > = \frac{2^n}{c^2} S_j(0) + \frac{(c-1)2^n}{c^2} S_j(n-k+1).$$

2. *For $c-1 \not| n$, setting $k = 1 + \frac{(c-2)n}{2(c-1)} + \alpha$ with $0 < \alpha < 1$, we have*

$$< \chi_C B_{n,j}, \chi_C > = \frac{2^n}{c^2} S_j(0) + \frac{(c-1)2^n}{c^2}((1-\alpha)S_j(n-k+1) + \alpha S_j(n-k+2)),$$

iff $\sum_{|T|=n-k+1} a_T^2 = \frac{(1-\alpha)(c-1)2^n}{c^2}$ *and* $\sum_{|T|=n-k+2} a_T^2 = \frac{\alpha(c-1)2^n}{c^2}$.

Proof. 1) Let $\chi_C = \sum_{T\subseteq[n]} a_T v_T$. It is clear that

$$\begin{aligned} 0 &\leq <\chi_C A_{n,1}, \chi_C> \\ &= 2^n \sum_{T\subseteq[n]} a_T^2(n-2|T|) \end{aligned}$$

Thus we have $\sum_{T\subseteq[n]} a_T^2|T| \leq \frac{n}{2c}$. Since $\sum_{|T|>0} a_T^2 = (c-1)/c^2$, for convenience we let $\Delta = (c-1)/c^2$. Thus

$$\begin{aligned} \sum_{|T|>0} \frac{a_T^2}{\Delta}|T| &\leq \frac{n}{2c\Delta} \\ &= \frac{cn}{2(c-1)} \\ &= n-k+1. \end{aligned}$$

Observe that $S_j(x)$ is convex and monotonically decreasing in the interval $[0, n-j+1]$. Define $\overline{S}_j(x) = S_j(x)$, for $x \leq n-j+1$ and $\overline{S}_j(x) = 0$, for $x > n-j+1$. It is clear that $\overline{S}_j(x)$ is convex and monotonically decreasing. Thus

$$\begin{aligned} <\chi_C B_{n,j}, \chi_C> &= \frac{2^n}{c^2}S_j(0) + \Delta 2^n \sum_{|T|>0} \frac{a_T^2}{\Delta} S_j(|T|) \\ &= \frac{2^n}{c^2}S_j(0) + \frac{(c-1)2^n}{c^2} \sum_{|T|>0} \frac{a_T^2}{\Delta} \overline{S}_j(|T|) \\ &\geq \frac{2^n}{c^2}S_j(0) + \frac{(c-1)2^n}{c^2} \overline{S}_j\left(\sum_{|T|>0} \frac{a_T^2}{\Delta}|T|\right), \text{ by the convexity of } \overline{S}_j(x) \\ &\geq \frac{2^n}{c^2}S_j(0) + \frac{(c-1)2^n}{c^2} S_j(n-k+1), \text{ because } \overline{S}_j(x) \text{ is non-increasing.} \end{aligned}$$

To prove the other direction, we have:

$$\begin{aligned} <\chi_C B_{n,j}, \chi_C> &= \frac{2^n}{c^2}S_j(0) + 2^n \sum_{0<|T|\leq n-j} a_T^2 S_j(|T|) \\ &= \frac{2^n}{c^2}S_j(0) + 2^n \sum_{n-k<|T|\leq n-j} a_T^2 S_j(|T|) \\ &\leq \frac{2^n}{c^2}S_j(0) + 2^n \sum_{n-k<|T|\leq n-j} a_T^2 S_j(n-k+1) \\ &\leq \frac{2^n}{c^2}S_j(0) + \frac{(c-1)2^n}{c^2} S_j(n-k+1). \end{aligned}$$

2) Similarly, we have

$$\begin{aligned} \sum_{|T|>0} \frac{a_T^2}{\Delta}|T| &\leq \frac{cn}{2(c-1)} \\ &= n-k+1+\alpha \\ &= (1-\alpha)(n-k+1) + \alpha(n-k+2) \end{aligned}$$

Here we need another convex function $S'_j(x) = S_j(x)$, for $x \leq n-j+1$, $S'_j(x) = 0$, for $x > n-j+1$ and $S'_j(x) = (x-(n-k+1))(S_j(n-k+2) - S_j(n-k+1)) + S_j(n-k+1)$, for $n-k+1 \leq x \leq n-k+2$. Thus

$$\begin{aligned}
< \chi_C B_{n,j}, \chi_C > &= \frac{2^n}{c^2} S_j(0) + \Delta 2^n \sum_{|T|>0} \frac{a_T^2}{\Delta} S_j(|T|) \\
&= \frac{2^n}{c^2} S_j(0) + \frac{(c-1)2^n}{c^2} \sum_{|T|>0} \frac{a_T^2}{\Delta} S'_j(|T|) \\
&\geq \frac{2^n}{c^2} S_j(0) + \frac{(c-1)2^n}{c^2} S'_j(\sum_{|T|>0} \frac{a_T^2}{\Delta}|T|), \text{ by the convexity of } S'_j(x) \\
&\geq \frac{2^n}{c^2} S_j(0) + \frac{(c-1)2^n}{c^2} S'_j(n-k+1+\alpha), \text{ because } S'_j(x) \text{ is non-increasing} \\
&= \frac{2^n}{c^2} S_j(0) + \frac{(1-\alpha)(c-1)2^n}{c^2} S_j(n-k+1) + \frac{\alpha(c-1)2^n}{c^2} S_j(n-k+2).
\end{aligned}$$

For the other direction we have:

$$\begin{aligned}
< \chi_C B_{n,j}, \chi_C > &= \frac{2^n}{c^2} S_j(0) + 2^n \sum_{|T|=n-k+1} a_T^2 S_j(n-k+1) + 2^n \sum_{|T|>n-k+1} a_T^2 S_j(|T|) \\
&\leq \frac{2^n}{c^2} S_j(0) + 2^n \sum_{|T|=n-k+1} a_T^2 S_j(n-k+1) \\
&\quad +2^n \sum_{n-j \geq |T| > n-k+1} a_T^2 S_j(n-k+2).
\end{aligned}$$

The claim follows by taking $j = k-2$. □

The main difference between Friedman's proof and ours is that we use the distance-i adjacency matrix of the n-cube for analysis instead of the i-th power of the adjacency matrix of the n-cube. It follows that we can characterize the $1/c$ dense set in the case $c-1|n$.

Theorem 8 *[5] Let $c-1|n$ and C be a set $1/c$ dense in $\mathcal{H}_k$. Then $\chi_C \perp v_T$, for non-empty $T \subseteq [n]$ with $|T| \neq n-k+1$.*

Proof. Take $j = k-1$ in Lemma 7.1. Then it is clear that $\sum_{|T|=n-k+1} a_T^2 = \frac{c-1}{c^2}$, which implies the claim. □

Corollary 9 *Let $c-1|n$ and $k = 1 + \frac{(c-2)n}{2(c-1)}$. Then all the subsets $1/c$ dense in $\mathcal{H}_k$ have the same distance distribution, i.e. $N_i = \frac{2^n}{c^2}(P_i(0) + (c-1)P_i(n-k+1))$ for $i = 0, ..., n$.*

Proof. Consider any $1/c$ dense subset C. Let $\chi = \sum_{T \subseteq [n]} a_T v_T$ be its characteristic vector. Then we have

$$\begin{aligned}
N_i &= < \chi A_{n,i}, \chi > \\
&= \sum_{T \subseteq [n]} a_T^2 P_i(|T|) < v_T, v_T >, \text{ by Theorem 3} \\
&= \frac{2^n}{c^2}(P_i(0) + (c-1)P_i(n-k+1)), \text{ by Theorem 8.}
\end{aligned}$$

□

4 Main results

As in [5], an η-*locally symmetric* coloring is defined as a coloring $\gamma : B^n \to B^s$, such that for all $v \in B^n$ exactly $n\eta$ of v's neighbors are colored $\gamma(v)$, and every other color occurs among v's neighbors exactly $n(1-\eta)/(c-1)$ times. It is clear that to have locally symmetric coloring, c must be at most $n+1$. By adapting the technique of [5], we prove a lower bound for k.

Proposition 10 *For any locally symmetric η-$(c; n, k)$ coloring, $k \geq 1 + \frac{n}{2} + \frac{(c\eta-1)n}{2(c-1)}$.*

Proof. As usual, let χ be the characteristic vector of vertices of an arbitrary color. Let $\chi = \sum_{T\subseteq[n]} a_T v_T$. Recall that $A_{n,1}v_T = (n-2|T|)v_T$. Now consider $< \chi A_{n,1}, \chi >$. It is clear that $\eta n 2^n/c = < \chi A_{n,1}, \chi >$. By some simple calculation, we have $k \geq 1 + \frac{n}{2} + \frac{(c\eta-1)n}{2(c-1)}$. □

The case $\eta = 0$ of this result appears in [5]. A locally symmetric coloring is called *sparse* if $\eta = 0$. In the case of $c-1|n$, all optimal locally symmetric colorings are sparse. The following result gives a positive answer to a problem proposed in [5].

Theorem 11 *If $c-1|n$, then all optimal $(c; n, k)$-coloring must be locally symmetric.*

(**Remark:** Sparsity was shown in [5]. Our result is the local symmetry; our proof also yields an alternative proof of sparsity.)

Proof. Let C be a color class and let $\chi = \sum_{T\subseteq[n]} a_T v_T$ be its characteristic vector. Let e_i be a unit vector corresponding to a vertex i in B^n. It is clear that $< \chi A_{n,1}, e_i >$ is the number of the neighbors of i in C. Then

$$\begin{aligned}
< \chi A_{n,1}, e_i > &= < \sum_{T\subseteq[n]} (n-2|T|)a_T, e_i > \\
&= < nv_0/c + (2k-2-n) \sum_{T\subseteq[n],|T|=n-k+1} a_T v_T, e_i > \\
&= < 2(n+1-k)v_0/c, e_i > + < (2k-2-n)\chi, e_i > \\
&= 2(n+1-k)/c + < (2k-2-n)\chi, e_i >
\end{aligned}$$

The last equality holds because $< v_0, e_i >= 1$. Now it is clear that $< \chi A_{n,1}, e_i >= 0$ if $i \in C$ and $n/(c-1)$ otherwise. We used the fact that $k = 1 + \frac{n}{2} - \frac{n}{2(c-1)}$. This completes the proof. □

Using the matrix $A_{n,j}$, we can prove that i has the same number of distance-j neighbors from each color, i.e. $(P_j(0) - P_j(n-k+1))/c + P_j(n-k+1)\delta_{i\in C}$.

A useful observation about XOR-colorings in [5] is that considering any cycle of length 4, $(p_0, p_1, p_2, p_3, p_0)$, in B^n then XOR-colorings satisfy the following two conditions:

1. $\gamma(p_3)$ depends only on $\gamma(p_0), \gamma(p_1), \gamma(p_2)$, not on the particular cycle.
2. $\gamma(p_0) = \gamma(p_2)$ implies $\gamma(p_1) = \gamma(p_3)$.

We use these properties to prove that there are optimal colorings which are not XOR type coloring. This was raised as an open question in [5].

Theorem 12 *For $c-1|n-1$, but $c \geq 4$, there exist optimal colorings for B^n which are neither locally symmetric nor XOR coloring.*

Proof. First consider an optimal coloring $\gamma : B^{n-1} \to \{1, ..., c\}$ with c colors. From the previous theorem, we know it must be a locally symmetric coloring. Let $k = \kappa(c, n-1)$. It is easy to see that $\kappa(c, n) = k + 1$, since $c - 1 | n - 1$ and $\kappa(c, n) \geq 1 + \frac{(c-2)n}{2(c-1)} = k + \frac{c-2}{2(c-1)}$. Note that the n-cube can be constructed from two $(n-1)$-cubes, say B_0 and B_1, by adding appropriate edges. For $i = 0, 1$, let the vertex set of B_i be $\{(-1)^i x : x \in \{-1, 1\}^{n-1}\}$. Then B^n has the vertex set $\{-1, 1\}^n$ and $E(B^n) = E(B_0) \cup E(B_1) \cup \{(-1x, 1x) : x \in \{-1, 1\}^{n-1}\}$.

Now with γ we can construct an optimal coloring γ' for B^n. We define $\gamma'(1x) = \gamma(x)$ and $\gamma'(-1x) = \gamma(x) + 1$ for all $x \in B^{n-1}$. Note that $c + 1$ denotes color 1. Indeed, γ' achieves an optimal $(c; n, k+1)$-coloring for B^n, since every $(k+1)$-subcube is from B_0, B_1 or by combining two corresponding k-subcubes in B_0 and B_1. It is easy to check that in every $(k+1)$-subcube of B^n each color appears exactly $2^{k+1}/c$ times. With the permutation on the colors for B_1, we know the local symmetry property is destroyed, since for each vertex v among its neighbors there is a color class which is more numerous than the others. And we can find a 4-cycle that does not satisfy the second condition of the XOR-coloring. Let $< -1x, 1x, 1y, -1y, -1x >$ be a 4-cycle, with $\mathrm{dist}(x, y) = 1$ and $\gamma'(1y) = \gamma'(1x) + 1$. Such x and y always exist because $c-1|n-1$ and γ is optimal for B^{n-1}. Then it is clear that $\gamma'(1y) = \gamma'(-1x)$ but $\gamma'(-1y) \neq \gamma'(1x)$. This proves the optimal coloring γ' is not an XOR type coloring. $\square$

5 Conclusion and Open problems

We have answered two questions of Friedman:

- For $c - 1 | n$, all optimal $(c; n, k)$-coloring must be locally symmetric.
- For $c - 1 | n - 1$, and $c \geq 4$, there exist optimal colorings for B^n which are neither locally symmetric nor XOR coloring.

There are still some unanswered questions. We shall list some problems which we consider to be interesting.

1. *Given c and n, can we improve the lower bound for the smallest k?* Note that the lower bound proved in [5] is good for small c and the bound is at most $n/2 + 1$.
2. *Is there any other general systematic coloring method?* Note that at this point the XOR-coloring method is the only known systematic coloring method.

Acknowledgments We would like to thank Laszlo Babai, Janos Simon for helpful discussion and comments, and Douglas Stinson for telling us some related new results.

References

[1] E. Bannai and T. Ito. *Algebraic Combinatorics I.* Benjamin/Cummings Pub., 1984.

[2] C. Bennett, G. Brassard, and J. Robert. Privacy amplification by public discussion. *SIAM J. Comput.*, 17:210–229, 1988.

[3] K. Bierbrauer, K. Gopalakrishnan, and D. R. Stinson. Bounds for Resilient Functions and Orthogonal Arrays. *Lecture Notes in Computer Science* (Advances in Cryptology-CRYPTO'94), 839(1994), 247–256.

[4] B. Chor, J. Friedman, O. Goldreich, J. Hastad, S. Rudich, and R. Smolensky. The bit extraction problem or t-resilient functions. In *26th FOCS*, pages 396–407, 1985.

[5] J. Friedman. On the bit extraction problem. In *33rd FOCS*, pages 314–319, 1992.

[6] K. Gopalakrishnan, D. Hoffman, and D. Stinson. A note on a conjecture concerning symmetric resilient functions. *Information Processing Letters*, 47:139–143, 1993.

[7] F.J. McWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, 1977.

[8] D. Stinson and J. Massey. An infinite class of counterexamples to a conjecture concerning non-linear resilient functions. *Journal of Cryptology*, 8(1995), 167–173.