Strongly Cancellative and Recovering Sets on Lattices

Hoda Bidkhori
Department of Mathematics
Northwestern University, Illinois, USA
hbidkho@ncsu.edu

ShinnYih Huang
Department of Mathematics
Yale University, Connecticut, USA
shinnyih.huang@yale.edu

Submitted: Dec 28, 2010; Accepted: Mar 24, 2011; Published: Mar 31, 2011

Abstract

We use information theory to study recovering sets $\mathbf{R}_L$ and strongly cancellative sets $\mathbf{C}_L$ on different lattices. These sets are special classes of recovering pairs and cancellative sets previously discussed in the papers of Simonyi, Frankl, and Füredi. We mainly focus on the lattices B_n and D_l^k. Specifically, we find upper bounds and constructions for the sets $\mathbf{R}_{B_n}$, $\mathbf{C}_{B_n}$, and $\mathbf{C}_{D_l^k}$.

1 Introduction

In this paper, we study the strongly cancellative sets $\mathbf{C}_L$ and recovering sets $\mathbf{R}_L$ that are subsets of points in lattices L, see Definition 2.1 and 2.2. On one hand, the study of the former set is motivated by the work of Ahlswede, Frankl, and Füredi [8] and Fredman [7]. Specifically, strongly cancellative sets are a special class of cancellative sets. On the other hand, the study of recovering sets is prompted by the previous work of Simonyi [9] on recovering pairs. A recovering pair (A, B) is an ordered pair of subsets A, B of points in a lattice such that for any $a, a' \in A$ and $b, b' \in B$, we have the following:

$$a \wedge b = a' \wedge b' \Rightarrow a = a',$$
$$a \vee b = a' \vee b' \Rightarrow b = b'.$$

The paper of Korner and Olistky [5] shows that the upper bound of $|A||B|$ plays an important role in the zero-error information theory. Cohen gave an upper bound 3^n for the size of $|A||B|$ on the Boolean lattice while Holzman and Korner improved the bound to 2.3264^n afterward. Throughout this paper, we study a special class of the recovering pairs $(\mathbf{R}_L, \mathbf{R}_L)$ which takes a single set $\mathbf{R}_L$. We call $\mathbf{R}_L$ a recovering set. As Definition 2.1 and 2.2 shows, a recovering set is a special case of a strongly cancellative set. Here, we focus on the upper bounds and structures of these two sets by using Information Theory.

This paper is organized as follows: Section 2 presents the definitions of strongly cancellative sets, recovering sets, and some results on the entropy function in Information

Theory. In Section 3, we study the recovering set $\mathbf{R}_{B_n}$ on the Boolean lattice B_n and find an upper bound $|\mathbf{R}_{B_n}| \leq \sqrt{3}\cdot 2^{0.4056n}$. As a result, this class of the recovering pairs has an upper bound $3\cdot 2^{0.8112n} = 3\cdot (1.7546703)^n$ on its size. In Section 4, we study strongly cancellative sets $\mathbf{C}_{B_n}$ on B_n. We give a tight upper bound $2^{\lfloor \frac{n}{2} \rfloor}$ on $|\mathbf{C}_{B_n}|$ for this lattice. Finally, Section 5 considers the strongly cancellative sets $\mathbf{C}_{D_{l_1,\ldots,l_k}}$ on the lattice $D_{l_1,\ldots,l_k}$ which is the product of k chains of length $l_1 - 1, \ldots, l_k - 1$. We show that when $l_1 = \cdots = l_k = l$, there exists a strongly cancellative set of size $l^{\lfloor \frac{k}{2} \rfloor}$ and $|\mathbf{C}_{D_{l,\ldots,l}}| \leq (2l)^{\frac{k}{2}} + \frac{k(l-1)}{2} + 1$.

2 Preliminaries

For basic definitions and results concerning lattices, we encourage readers to consult Chapter 3 of [11]. In particular, the Boolean lattice B_n is the lattice of all subsets of the set $\{1, \ldots, n\}$ ordered by inclusion, and $D_{l_1,\ldots,l_k}$ is the lattice formed by the product of k chains of length $l_1 - 1, \ldots, l_k - 1$, so that the points in $D_{l_1,\ldots,l_k}$ correspond to k-dimensional vectors $(v_1, \ldots, v_k)$ with $0 \leq v_i \leq l_i - 1$. The ordering of points in $D_{l_1,\ldots,l_k}$ is as follows:

$$v \preceq w \Leftrightarrow v_i \leq w_i, \text{ for all } 1 \leq i \leq k.$$

A cancellative set is a subset of points in lattice L such that any three different points v_1, v_2, v_3 in this set satisfy the following condition:

$$v_1 \wedge v_2 \neq v_1 \wedge v_3.$$

We define strongly cancellative sets as a special class of cancellative sets.

Definition 2.1. A *strongly cancellative set* $\mathbf{C}_L$ of lattice L is a subset of points in L such that for any three different points $a_1, a_2, a_3 \in \mathbf{C}_L$,

$$a_1 \wedge a_2 \neq a_1 \wedge a_3 \text{ and } a_1 \vee a_2 \neq a_1 \vee a_3. \tag{2.1}$$

Secondly, a recovering set meets all the conditions that define a strongly cancellative set. In addition, any recovering set $\mathbf{R}_L$ forms a recovering pair $(\mathbf{R}_L, \mathbf{R}_L)$ on L. Here, we give a formal definition for $\mathbf{R}_L$.

Definition 2.2. A *recovering set* $\mathbf{R}_L$ of lattice L is a subset of points in L such that for any four different points $a_1, a_2, a_3, a_4 \in \mathbf{R}_L$, we have

$$a_1 \wedge a_2 \neq a_3 \wedge a_4 \text{ and } a_1 \vee a_2 \neq a_3 \vee a_4, \tag{2.2}$$

$$a_1 \wedge a_2 \neq a_1 \wedge a_3 \text{ and } a_1 \vee a_2 \neq a_1 \vee a_3. \tag{2.3}$$

Now, we introduce the *entropy function* and show an inequality of it.

Given a discrete random variable X with m possible values $x_1, \ldots, x_m$, we define the *entropy function* $\mathcal{H}$ of X as follows:

$$\mathcal{H}(X) = -\sum_{i=1}^{m} p(x_i) \log_b p(x_i) = \sum_{i=1}^{m} p(x_i) \log_b \frac{1}{p(x_i)}, \tag{2.4}$$

where p is the probability mass function of X and x_i is the value of X. In this paper, we always set $b = 2$. Also, the function $x \log \frac{1}{x}$ is concave down when $x > 0$. Therefore, for any s values $0 \le p_1, \ldots, p_s \le 1$, we have

$$\sum_{j=1}^{s} \left(p_j \log \frac{1}{p_j} \right) \le s \cdot \left(\frac{\sum_{j=1}^{s} p_j}{s} \right) \cdot \log \left(\frac{s}{\sum_{j=1}^{s} p_j} \right). \tag{2.5}$$

The following inequality of entropy functions is the major inequality throughout this paper. A proof of the inequality is given in [3].

Theorem 2.3. *If $\xi = (\xi_1, \ldots, \xi_m)$ is an n-dimensional random variable, then*

$$\mathcal{H}(\xi) \le \sum_{i=1}^{n} \mathcal{H}(\xi_i). \tag{2.6}$$

3 Recovering Set on Boolean lattice B_n

In this section, we study recovering sets on Boolean lattices where we use $\cap$ and $\cup$ instead of $\wedge$ and $\vee$. In the following theorem, we give an upper bound for $|\mathbf{R}_{B_n}|$.

Theorem 3.1. *For any recovering set $\mathbf{R}_{B_n}$, we have $|\mathbf{R}_{B_n}| \le \sqrt{3} \cdot 2^{0.4056n}$.*

Remark 3.2. In particular, $(\mathbf{R}_{B_n}, \mathbf{R}_{B_n})$ is a special class of recovering pairs on the Boolean lattice, and we give a bound $\left(\sqrt{3} \cdot 2^{0.4056n}\right)^2$ which is significantly better than the cardinalities of a general recovering pair discussed in [1], [9], and [10].

Proof. Let us define a random variable $\xi = a_i \cap a_j$, where a_i and a_j are independently chosen according to the uniform distribution on $\mathbf{R}_{B_n}$. We wish to show that for any value a in ξ, there are at most three ordered pairs (a_i, a_j) such that $a = a_i \cap a_j$. Fixed an ordered pair (a_t, a_s) for (a_i, a_j), and suppose that there exists another ordered pair (a_{t_1}, a_{s_1}) such that $a_{t_1} \cap a_{s_1} = a_t \cap a_s = a_s \cap a_t$. We have the following two cases:

1. $a_t \ne a_s$. By Definition 2.2, a_{t_1} and a_{s_1} should be the same element in B_n, and we have the following possible cases:

   (a) $a_{t_1} = a_{s_1} \notin \{a_t, a_s\}$.
   In this case, since $a_t \cap a_s = a_{t_1} \cap a_{t_1}$, the set a_{t_1} is contained in a_t and a_s. It follows that $a_{t_1} \cap a_t = a_{t_1} \cap a_s$ which contradicts the second requirement of Definition 2.2.

   (b) $a_{t_1} = a_{s_1} \in \{a_t, a_s\}$.
   This leaves us exactly one choice for (a_{t_1}, a_{s_1}).

2. $a_t = a_s$. This is the same condition as case (b) in (1). That is to say, one of a_{t_1} and a_{s_1} must be the set a_t , and (a_{t_1}, a_{s_1}) has only two possible choices.

Consequently, at most three different ordered pairs obtain the same value in ξ. We can give a lower bound on the entropy function of ξ based on this property.

For any a in ξ, let $\mathbf{C}(a) = \{(a_i, a_j) : a_i \cap a_j = a, \text{ and } a_i, a_j \in \mathbf{R}_{B_n}\}$ and $\mathcal{P}_a = \Pr(\xi = a) = \frac{|\mathbf{C}(a)|}{|\mathbf{R}_{B_n}|^2}$. By the above argument, we have $|\mathbf{C}(a)| \leq 3$ and $\mathcal{P}_a \leq \frac{3}{|\mathbf{R}_{B_n}|^2}$, for any a in ξ. Considering the entropy function in (2.4), we obtain the following inequality:

$$\mathcal{H}(\xi) = \sum_{a\in\xi} \mathcal{P}_a \log \frac{1}{\mathcal{P}_a} \geq \sum_{a\in\xi} \mathcal{P}_a \log \frac{|\mathbf{R}_{B_n}|^2}{3} = \log \frac{|\mathbf{R}_{B_n}|^2}{3}.$$

On the other hand, ξ is an n-dimensional random variable $(\xi_1, \ldots, \xi_n)$, where

$$\xi_t = \begin{cases} 1, & t \in a_i \cap a_j. \\ 0, & t \notin a_i \cap a_j. \end{cases}$$

We set $\mathbf{R}_{B_n}(t) = \{a_i \mid a_i \in \mathbf{R}_{B_n}, t \in a_i\}$ and $\mathcal{P}_{\mathbf{R}_{B_n}}(t) = \frac{|\mathbf{R}_{B_n}(t)|}{|\mathbf{R}_{B_n}|}$, for any $1 \leq t \leq n$. This shows that, $\Pr(\xi_t = 1) = \left(\mathcal{P}_{\mathbf{R}_{B_n}}(t)\right)^2$, for any $t \in \{1, \ldots, n\}$. Let us denote $h(x)$ as $x \log \frac{1}{x} + (1-x) \log \frac{1}{1-x}$. We have by Theorem 2.3 that

$$\log \frac{|\mathbf{R}_{B_n}|^2}{3} \leq \mathcal{H}(\xi) \leq \sum_{t=1}^{n} \mathcal{H}(\xi_t) = \sum_{t=1}^{n} \left[h\left(\mathcal{P}_{\mathbf{R}_{B_n}}(t)^2\right)\right], \tag{3.1}$$

Consider the random variable $\xi' = a_i \cup a_j$. Since entropy functions have the property that $h(x) = h(1-x)$, we similarly get

$$\log \frac{|\mathbf{R}_{B_n}|^2}{3} \leq \sum_{t=1}^{n} h\left(1 - \left(1 - \left(\mathcal{P}_{\mathbf{R}_{B_n}}(t)\right)\right)^2\right) = \sum_{t=1}^{n} h\left(\left(1 - \left(\mathcal{P}_{\mathbf{R}_{B_n}}(t)\right)\right)^2\right). \tag{3.2}$$

Now, averaging (3.1) and (3.2), we obtain an upper bound for $\log \frac{|\mathbf{R}_{B_n}|^2}{3}$, namely:

$$\begin{aligned} \log \frac{|\mathbf{R}_{B_n}|^2}{3} &\leq \frac{1}{2} \sum_{t=1}^{n} \left[h\left(\mathcal{P}_{\mathbf{R}_{B_n}}(t)^2\right) + h\left(\left(1 - \mathcal{P}_{\mathbf{R}_{B_n}}(t)\right)^2\right)\right] && (3.3) \\ &\leq \frac{n}{2} \left[\max_{0\leq x\leq 1} \left(h(x^2) + h\left((1-x)^2\right)\right)\right] && (3.4) \\ &\leq \frac{n}{2} \left[\max_{0\leq x\leq 1} \left(x \frac{h(x^2)}{x} + (1-x) \frac{h\left((1-x)^2\right)}{1-x}\right)\right]. && (3.5) \end{aligned}$$

Finally, by the work of D. J. Kleitman, J. Shearer and D. Sturtevant [3], we know that the function $\frac{h(x^2)}{x}$ is concave down, hence, Jensen's inequality gives

$$\max_{0\leq x\leq 1} \left(x \frac{h(x^2)}{x} + (1-x) \frac{h\left((1-x)^2\right)}{1-x}\right) \leq \max_{0\leq x\leq 1} \frac{h((x^2 + (1-x)^2)^2)}{x^2 + (1-x)^2}.$$

By some simple calculation, one can see that the function $\frac{h(x^2)}{x}$ is decreasing with $\frac{1}{2} \leq x \leq 1$. Therefore, $2h(\frac{1}{4}) = 0.8112$ is an upper bound for $\frac{h(x^2)+h\left((1-x)^2\right)}{2}$, and we obtain an upper bound for $|\mathbf{R}_{B_n}|$:

$$|\mathbf{R}_{B_n}| \leq \sqrt{3} \cdot 2^{0.4056n}$$

□

4 Strongly Cancellative set on Boolean lattice B_n

In this section, we show that the maximal size of $\mathbf{C}_{B_n}$ on B_n, see Definition 2.1, is $2^{\lfloor \frac{n}{2} \rfloor}$. In addition, this is the tightest bound.

Theorem 4.1. *There exists a strongly cancellative set $\mathbf{C}_{B_n}$ of size $2^{\lfloor \frac{n}{2} \rfloor}$ on B_n.*

Proof. We construct $\mathbf{C}_{B_n}$ as follows. First, let us divide the set $\{1, \ldots, 2\lfloor \frac{n}{2} \rfloor\}$ into $\lfloor \frac{n}{2} \rfloor$ blocks $S_i = \{2i-1, 2i\}$, for $1 \leq i \leq \lfloor \frac{n}{2} \rfloor$. We define $\mathbf{C}_{B_n}$ to be the family of all the subsets $s = \left\{s_1, \ldots, s_{\lfloor \frac{n}{2} \rfloor}\right\}$ such that $s_i \in S_i$, for $1 \leq i \leq \lfloor \frac{n}{2} \rfloor$. Thus, we have $|\mathbf{C}_{B_n}| = 2^{\lfloor \frac{n}{2} \rfloor}$. Now, we show that $\mathbf{C}_{B_n}$ satisfies the conditions defining strongly cancellative set.

Consider different elements $b = \left\{b_1, \ldots, b_{\lfloor \frac{n}{2} \rfloor}\right\}$ and $c = \left\{c_1, \ldots, c_{\lfloor \frac{n}{2} \rfloor}\right\}$ in $\mathbf{C}_{B_n}$, so that there exists some $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$ such that $b_k \neq c_k$. Without lost of generality, assume that $b_k = 2k - 1$ and $c_k = 2k$. Consequently, for any element $a = \left\{a_1, \ldots, a_{\lfloor \frac{n}{2} \rfloor}\right\}$, we have the following properties:

1. $b_k \notin a \cap c$ and $c_k \notin a \cap b$,
2. $b_k \in a \cup b$ and $c_k \in a \cup c$,
3. $a_k = b_k$ or $a_k = c_k$,
4. $b_k \in a \cap b$ or $c_k \in a \cap c$,
5. $c_k \notin a \cup b$ or $b_k \notin a \cup c$.

Clearly, property (3) implies (4) and (5). Moreover, (1) and (4) imply that $a \cap b \neq a \cap c$, and similarly, (2) and (5) imply that $a \cup b \neq a \cup c$. Therefore, $\mathbf{C}_{B_n}$ is a strongly cancellative set. □

Now, we show that $|\mathbf{C}_{B_n}| \leq 2^{\lfloor \frac{n}{2} \rfloor}$.

Theorem 4.2. *For any strongly cancellative $\mathbf{C}_{B_n}$ on B_n, we have $|\mathbf{C}_{B_n}| \leq 2^{\lfloor \frac{n}{2} \rfloor}$.*

Proof. Fix an element $v' \in \mathbf{C}_{B_n}$. We consider the following sets:

$$\mathbf{C}_1(v') = \{v \cap v' : v \neq v', v \in \mathbf{C}_{B_n}\},$$
$$\mathbf{C}_2(v') = \{v \cup v' : v \neq v', v \in \mathbf{C}_{B_n}\}.$$

By Equation (2.1), we have $|\mathbf{C}_1(v')| = |\mathbf{C}_2(v')| = |\mathbf{C}_{B_n}| - 1$. This implies that

$$|\mathbf{C}_{B_n}| \leq 1 + \min\left(|\{v : v \subseteq v'\}|, |\{v : v \supseteq v'\}|\right). \tag{4.1}$$

Moreover,

$$\min\left(|\{v : v \subseteq v'\}|, |\{v : v \supseteq v'\}|\right) \leq \left|\left\{v : v \subseteq v^*, \mathrm{rank}(v^*) = \left\lfloor \frac{n}{2} \right\rfloor\right\}\right|. \tag{4.2}$$

We consider the following two cases:

1. $2 \mid n$. Then we have $\mathrm{rank}(v') = \left\lfloor \frac{n}{2} \right\rfloor$ if the equality holds in (4.2). Suppose that the equalities in (4.1) and (4.2) hold for every $v' \in \mathbf{C}_{B_n}$. Consequently, $\mathrm{rank}(v') = \left\lfloor \frac{n}{2} \right\rfloor$, for every $v' \in \mathbf{C}_{B_n}$, which implies that any two elements in the set are incomparable. One can easily see that, $\mathbf{C}_1(v') \neq |\{v : v \subseteq v'\}|$ and $\mathbf{C}_2(v') \neq |\{v : v \supseteq v'\}|$. Therefore, the equalities in (4.1) and (4.2) can not hold at the same time.

2. $2 \nmid n$. Then $\mathrm{rank}(v') = \left\lfloor \frac{n}{2} \right\rfloor$ or $\left\lfloor \frac{n+1}{2} \right\rfloor$ if the equality hold in (4.2). Suppose that the equalities in (4.1) and (4.2) holds for every $v' \in \mathbf{C}_{B_n}$. Pick some element $w \in \mathbf{C}_{B_n}$. If $\mathrm{rank}(w) = \left\lfloor \frac{n}{2} \right\rfloor$, then by (4.1) there exist other two elements w' and w'' in the set such that $w \cap w' = w$ and $w \cap w'' = \emptyset$. This implies that $\mathrm{rank}(w') = \left\lfloor \frac{n+1}{2} \right\rfloor$ and $w' \backslash w = \{x\}$, where $1 \leq x \leq n$.

   By Equation (2.1), we have $\emptyset = w \cap w'' \neq w' \cap w''$, and thus $x \in w''$. This means that $w \cup w'' = w' \cup w''$ which is not possible. As a result, the equalities in (4.1) and (4.2) cannot hold at the same time. Similarly, one can prove the same statement when $\mathrm{rank}(w) = \left\lfloor \frac{n+1}{2} \right\rfloor$.

Finally, from (1) and (2), we have

$$|\mathbf{C}_{B_n}| \leq \left|\left\{v : v \subseteq v^*, \mathrm{rank}(v^*) = \left\lfloor \frac{n}{2} \right\rfloor\right\}\right| = 2^{\left\lfloor \frac{n}{2} \right\rfloor}.$$

□

5 Strongly Cancellative Sets on lattices $D_{l_1,\ldots,l_k}$ and D_l^k

For the definition of the lattice $D_{l_1,\ldots,l_k}$, see Section 2. In particular, we say that D_l^k is a lattice of k chains of length $l-1$. It is easy to show that for any two points $v = (v_1, \ldots, v_k)$ and $v' = (v'_1, \ldots, v'_k)$ in $D_{l_1,\ldots,l_k}$,

$$(v_1, \ldots, v_k) \wedge (v'_1, \ldots, v'_k) = \big(\min(v_1, v'_1), \ldots, \min(v_k, v'_k)\big),$$
$$(v_1, \ldots, v_k) \vee (v'_1, \ldots, v'_k) = \big(\max(v_1, v'_1), \ldots, \max(v_k, v'_k)\big).$$

In the following proposition, we give a tight bound for the size of strongly cancellative sets on D_{l_1,l_2}.

Proposition 5.1. *Let $\mathbf{C}_{D_{l_1,l_2}}$ be a strongly cancellative set on the lattice D_{l_1,l_2}. Then*

$$\left|\mathbf{C}_{D_{l_1,l_2}}\right| \leq \min(l_1, l_2).$$

Proof. Without lost of generality, we assume that $l_1 \leq l_2$. Every point v in D_{l_1,l_2} is a vector (v_1, v_2), where $0 \leq v_1 \leq l_1 - 1$ and $0 \leq v_2 \leq l_2 - 1$. We proceed by contradiction.

Suppose that $\left|\mathbf{C}_{D_{l_1,l_2}}\right| > l_1$. Then there exists two points $v = (v_1, v_2)$ and $w = (w_1, w_2)$ such that $v_1 = w_1$ and $v_2 < w_2$. For any point $v^* = (v_1^*, v_2^*) \notin \{v, w\}$, all the following four possible cases lead to contradiction:

1. $v_2^* \leq v_2$ implies that $v^* \wedge v = v^* \wedge w$.
2. $v_2^* > w_2$ implies that $v^* \vee v = v^* \vee w$.
3. $v_2 \leq v_2^* \leq w_2$ and $v_1^* \leq v_1$ imply that $v^* \vee w = v \vee w$.
4. $v_2 \leq v_2^* \leq w_2$ and $v_1^* \geq v_1$ imply that $v^* \wedge v = v \wedge w$.

Therefore, we must have $\left|\mathbf{C}_{D_{l_1,l_2}}\right| \leq l_1 = \min(l_1, l_2)$, as desired. □

The bound $\min(l_1, l_2)$ is tight for $\left|\mathbf{C}_{D_{l_1,l_2}}\right|$. In particular, it is not hard to show that the following set is a strongly cancellative set of size $\min(l_1, l_2)$:

$$\mathbf{C}_{D_{l_1,l_2}} = \{(x, y) \mid x + y = \min(l_1, l_2) - 1\}.$$

In the following, we study the size of the strongly cancellative sets on D_l^k.

Proposition 5.2. *Suppose that $\mathbf{C}_{k_1}$ is a strongly cancellative set on the lattice $D_l^{k_1}$ for some small k_1, and any two elements in $\mathbf{C}_{k_1}$ are incomparable. Then, for any k with $\left\lfloor \frac{k}{k_1} \right\rfloor = s$, there is a strongly cancellative set $\mathbf{C}_k$ of size $|\mathbf{C}_{k_1}|^s$ on D_l^k.*

Proof. Every point in D_l^k is a k-dimensional vector $(v_1, \ldots, v_k)$, where $0 \leq v_i \leq l - 1$ for $1 \leq i \leq k$. For every vector $v = (v_1, \ldots, v_k)$, we define subvectors induced by v as $B_j(v) = (v_{(j-1)k_1+1}, \ldots, v_{jk_1})$, for $1 \leq j \leq s$, and $B_{s+1}(v) = (v_{k_1 s+1}, \ldots, v_k)$. Let $\mathbf{C}_k$ to be the set of all k-dimensional vectors v such that $B_j(v) \in \mathbf{C}_{k_1}$ for all $1 \leq j \leq s$, and $B_{s+1}(v)$ is the zero vector. Clearly, we have $|\mathbf{C}_k| = |\mathbf{C}_{k_1}|^s$.

Suppose there are three different elements $v, v', v'' \in \mathbf{C}_k$ such that $v \vee v' = v \vee v''$. Since v' and v'' are different, we have $B_{j^*}(v') \neq B_{j^*}(v'')$ for some $1 \leq j^* \leq s$. On the other hand, we know $B_{j^*}(v) \vee B_{j^*}(v') = B_{j^*}(v) \vee B_{j^*}(v'')$ which implies that one of $B_{j^*}(v')$ or $B_{j^*}(v'')$ is equal to $B_{j^*}(v)$. Therefore, $v_i' \preceq v_i''$ or $v_i'' \preceq v_i'$, and this contradicts the assumption that any two different elements in $\mathbf{C}_{k_1}$ are incomparable. Similarly, it is easy to see that $v \wedge v' \neq v \wedge v''$. As a result, $\mathbf{C}_k$ is a strongly cancellative set of size $|\mathbf{C}_{k_1}|^s$. □

We can use this result to give a construction of a strongly cancellative set on D_l^k.

Corollary 5.3. *There exists a strongly cancellative set* $\mathbf{C}_{D_l^k}$ *on the lattice* D_l^k*, such that* $\left|\mathbf{C}_{D_l^k}\right| = l^{\lfloor \frac{k}{2} \rfloor}$.

Proof. We have seen that $\mathbf{C}_{D_l^2} = \{(x,y) \mid x+y = l-1\}$ is a strongly cancellative set of size l on D_l^2 such that any two elements in the set are incomparable. By Proposition 5.2, there exists a strongly cancellative set $\mathbf{C}_{D_l^k}$ of size $l^{\lfloor \frac{k}{2} \rfloor}$. □

We end this section with an upper bound of the size of strongly cancellative sets on D_l^k.

Theorem 5.4. *Let* $\mathbf{C}_{D_l^k}$ *be a strongly cancellative set on* D_l^k*, then*

$$\left|\mathbf{C}_{D_l^k}\right| \leq (2l)^{\frac{k}{2}} + \frac{k(l-1)}{2} + 1.$$

Proof. Any element v on the lattice D_l^k is a k-dimensional vector $v = (v_1, \ldots, v_k)$ such that $0 \leq v_i \leq l-1$ for all $1 \leq i \leq k$. We first define $\mathbf{C}_m(t)$ and $\mathcal{P}_m(t)$.

1. We define $\mathbf{C}_m(t)$ to be set of vectors whose m-th component is t, for any $1 \leq t \leq k$. That is, $\mathbf{C}_m(t) = \{v \mid v \in \mathbf{C}_{D_l^k},\ v_m = t\}$.
2. Let v be a random element uniformly chosen in the set $\mathbf{C}_{D_l^k}$. We denote the probability that the m-th component v_m of v is t by $\mathcal{P}_m(t)$. So,
$$\mathcal{P}_m(t) = \frac{|\mathbf{C}_m(t)|}{\left|\mathbf{C}_{D_l^k}\right|}.$$

Fix an arbitrary element $v \in \mathbf{C}_{D_l^k}$. We define the random variable $\xi_v = v \wedge v^*$, where v^* is the random element uniformly chosen in $\mathbf{C}_{D_l^k} \backslash \{v\}$. Suppose that there exist two elements v_1 and v_2 in $\mathbf{C}_{D_l^k}$ so that we obtain the same value in ξ_v. That is, $v \wedge v_1 = v \wedge v_2$ which is not possible in strongly cancellative sets. Consequently, every value in ξ_v appears exactly once. Since there are totally $\left|\mathbf{C}_{D_l^k}\right| - 1$ different values for ξ_v, the entropy function of ξ_v is

$$\mathcal{H}(\xi_v) = \log\left(\left|\mathbf{C}_{D_l^k}\right| - 1\right). \tag{5.1}$$

For convenience, we set $N = \left|\mathbf{C}_{D_l^k}\right| - 1$.

On the other hand, every value in ξ_v is a k-dimensional vector $(\xi_v(1), \ldots, \xi_v(k))$ such that $\xi_v(m) = \min(v_m, v_m^*)$ for any $1 \leq m \leq k$ and randomly chosen element v^*. Consequently, for any $1 \leq m \leq k$, $\xi_v(m)$ takes all its values in $\{0, 1, \ldots, v_m\}$. We denote the probability that $\xi_v(m) = t'$ by $\mathcal{P}_{\xi_v(m)}(t')$. Moreover, if $0 \leq t' \leq v_m - 1$, we should have $t' = \min(v_m, v_m^*) < v_m$ and thus, $v_m^* = t'$. If $t' = v_m$, we must have $\min(v_m, v_m^*) = t' = v_m$ which implies that $v_m \leq v_m^*$.

Therefore, we obtain the following properties for $P_{\xi_v(m)}(t')$:

$$\mathcal{P}_{\xi_v(m)}(t') = \begin{cases} \frac{|\mathbf{C}_m(t')|}{N}, & 0 \le t' \le v_m - 1. \\ \frac{\left[\sum_{t_1'=v_m}^{l-1} |\mathbf{C}_m(t_1')|\right]-1}{N}, & t' = v_m. \\ 0, & v_m + 1 \le t' \le l-1. \end{cases} \tag{5.2}$$

The entropy function of $\xi_v(m)$ can be computed as follows:

$$\begin{aligned} \mathcal{H}\left(\xi_v(m)\right) &= \mathcal{H}\left(\mathcal{P}_{\xi_v(m)}(0), \ldots, \mathcal{P}_{\xi_v(m)}(v_m - 1), \mathcal{P}_{\xi_v(m)}(v_m)\right) \\ &= \sum_{t'=0}^{v_m} \mathcal{P}_{\xi_v(m)}(t') \log \frac{1}{\mathcal{P}_{\xi_v(m)}(t')}. \end{aligned}$$

Furthermore, by Eq.(5.1) and Theorem (2.3), we have

$$\log N \le \sum_{m=1}^{k} \mathcal{H}\left(\xi_v(m)\right) = \sum_{m=1}^{k} \sum_{t'=0}^{v_m} \mathcal{P}_{\xi_v(m)}(t') \log \frac{1}{\mathcal{P}_{\xi_v(m)}(t')}. \tag{5.3}$$

The above equation holds for every element v in the set $\mathbf{C}_{D_l^k}$. If we take the average over all the elements in the set $\mathbf{C}_{D_l^k}$, we obtain

$$\log N \le \frac{\sum_{v \in \mathbf{C}_{D_l^k}} \sum_{m=1}^{k} \mathcal{H}\left(\xi_v(m)\right)}{N+1} = \frac{\sum_{m=1}^{k} \sum_{v \in \mathbf{C}_{D_l^k}} \mathcal{H}\left(\xi_v(m)\right)}{N+1}. \tag{5.4}$$

Moreover, from (2), we know that the probability that $v_m = t$ for some $0 \le t \le l-1$ is $\mathcal{P}_m(t) = \frac{|\mathbf{C}_m(t)|}{N+1}$, and therefore, (5.4) can be rewritten as follows:

$$\log N \le \sum_{m=1}^{k} \sum_{t=0}^{l-1} \mathcal{P}_m(t) \left(\sum_{t'=0}^{t} P_{\xi_v(m)}(t') \log \frac{1}{\mathcal{P}_{\xi_v(m)}(t')} \right). \tag{5.5}$$

Now, we consider the random variable $\xi_v' = v \vee v^*$, where v^* is also independently chosen under the uniform distribution on $\mathbf{C}_{D_l^k} \backslash \{v\}$. Thus, we have the following:

$$\mathcal{P}_{\xi_v'(m)}(t') = \begin{cases} 0, & 0 \le t' \le v_m - 1. \\ \frac{\left[\sum_{t_1'=0}^{v_m} |\mathbf{C}_m(t_1')|\right]-1}{N}, & t' = v_m. \\ \frac{|\mathbf{C}_m(t')|}{N}, & v_m + 1 \le t' \le l-1. \end{cases} \tag{5.6}$$

By similar arguments, Eq.(5.6) implies that:

$$\log N \le \sum_{m=1}^{k} \sum_{t=0}^{l-1} \mathcal{P}_m(t) \left(\sum_{t'=t}^{l-1} \mathcal{P}_{\xi_v(m)}(t') \log \frac{1}{\mathcal{P}_{\xi_v(m)}(t')} \right). \tag{5.7}$$

For convenience, let $\mathcal{P}'_m(t') = \frac{|\mathbf{C}_m(t')|}{N}$. Also, we set $q_m(t) = \frac{\left[\sum_{t'_1=t}^{l-1} |\mathbf{C}_m(t'_1)|\right]-1}{N}$, and $q'_m(t) = \frac{\left[\sum_{t'_1=0}^{t} |\mathbf{C}_m(t'_1)|\right]-1}{N}$.

Consider the following inequality,

$$\sum_{t'=0}^{t} \mathcal{P}_{\xi_v(m)}(t') \log \frac{1}{\mathcal{P}_{\xi_v(m)}(t')} + \sum_{t'=t}^{l-1} \mathcal{P}_{\xi_v(m)}(t') \log \frac{1}{\mathcal{P}_{\xi_v(m)}(t')} \tag{5.8}$$

$$\leq \left(\sum_{t'=0}^{l-1} \mathcal{P}'_m(t') \log \frac{1}{\mathcal{P}'_m(t')} \right) + q_m(t) \log \frac{1}{q_m(t)} + q'_m(t) \log \frac{1}{q'_m(t)} \tag{5.9}$$

$$\leq \left(\frac{N+1}{N} \right) \log \frac{lN}{N+1} + (q_m(t) + q'_m(t)) \cdot \log \left(\frac{2}{q_m(t) + q'_m(t)} \right). \tag{5.10}$$

Note that (5.9) holds because $p \log \frac{1}{p} > 0$, when $0 < p < 1$, and (5.10) holds by the inequality in (2.5).

Finally, by adding (5.5) and (5.7), the above result implies that

$$\begin{aligned} 2 \log N &\leq \sum_{m=1}^{k} \sum_{t=0}^{l-1} \mathcal{P}_m(t) \left[(q_m(t) + q'_m(t)) \cdot \log \left(\frac{2}{q_m(t) + q'_m(t)} \right) + \left(1 + \frac{1}{N} \right) \log l \right] \\ &= k \left(1 + \frac{1}{N} \right) \log l + \sum_{m=1}^{k} \sum_{t=0}^{l-1} \mathcal{P}_m(t) \cdot (q_m(t) + q'_m(t)) \cdot \log \left(\frac{2}{q_m(t) + q'_m(t)} \right) \\ &\leq k + k \left(1 + \frac{1}{N} \right) \log l. \end{aligned}$$

The last inequality is due to the fact that function $x \log \frac{2}{x}$ is decreasing with $x \geq 1$ and that $q_m(t) + q'_m(t) = 1 + \frac{|\mathbf{C}_m(t)|-1}{N} \geq 1$ when $\mathcal{P}_m(t) = \frac{|\mathbf{C}_m(t)|}{N+1} \neq 0$.

Therefore, we have

$$N \leq 2^{\frac{k}{2}} l^{\frac{k}{2}\left(1+\frac{1}{N}\right)}. \tag{5.11}$$

Consider the function $f(N) = N - 2^{\frac{k}{2}} l^{\frac{k}{2}\left(1+\frac{1}{N}\right)}$. The inequality (5.11) implies that $f(N) \leq 0$ and is increasing with N. If we set $N_1 = (2l)^{\frac{k}{2}} + \frac{k(l-1)}{2}$, then it is easy to see that

$$f(N_1) = \frac{k(l-1)}{2} + (2l)^{\frac{k}{2}} \cdot \left(1 - (1 + l - 1)^{\frac{k}{2N_1}} \right) \tag{5.12}$$

$$\geq \frac{k(l-1)}{2} + (2l)^{\frac{k}{2}} \cdot \left(1 - \left(1 + \frac{(l-1)k}{2N_1} \right) \right) \tag{5.13}$$

$$= \frac{k(l-1)}{2} - \frac{(2l)^{\frac{k}{2}}}{N_1} \cdot \frac{k(l-1)}{2} \geq 0, \tag{5.14}$$

where (5.12) implies (5.13) because $(1+a)^b \leq 1 + ab$ when $b \leq 1$ and $a \geq 0$.

As a result, since $f(N) \le 0 \le f(N_1)$,

$$\left|\mathbf{C}_{D_l^k}\right| - 1 = N \le N_1 = (2l)^{\frac{k}{2}} + \frac{k(l-1)}{2}.$$

□

Acknowledgement

Part of this research was done at MIT SPUR program. We would like to thank Clifford Smyth for proposing this problem.

References

[1] A. Sali, G. Simonyi: Recovering Set System and Sandglass Conjecture, Combinatorics, Probability, and Computing (1997) **6**, 481-491

[2] Csákány Rita: Some results on the sandglass conjecture. (English summary) 6th International Conference on Graph Theory (Marseille, 2000), 4 pp. (electronic), Electron. Notes Discrete Math., 5, Elsevier, Amsterdam, 2000.

[3] D. J. Kleitman, J. Shearer and D. Sturtevant: Intersections of k -element sets, vol. **1**, Combinatorica, 1981.

[4] I. Csiszár, J. Korner: Information Theory: Coding Theorems for Discrete Memoryless Systems, Academic Press, New York, 1982.

[5] Janos Korner, Alon Orlitsky: Zero-Error Information Theory, Ieee Transactions On Information Thory, vol. **44**, no. 6, October 1998.

[6] James B. Shearer: A New Construction For Cancellative Families of Sets, The Electronic Journal of Combinatorics 3 (1996).

[7] Michael L. Fredman: The Complexity of Maintaining an Array and Computing Its Partial Sums, Journal of the Association for Computing Machinery, Vol. **29**, no I, January 1982, pp 250-260

[8] P. Frankl, Z. Füredi, Union-free Hypergraphs and Probability Theory, European Journal of Combinatorics, **5** (1984), pp. 127-131.

[9] R. Ahlswede, G. Simonyi: On the optimal structure of recovering set pairs in lattices: the sandglass conjecture, Discr. Math., **128**(1994), 389-394

[10] R. Holzman, J. Korner: Cancellative Pairs of Families of Sets, Europ. J. Combinatorics (1995) **16**, 263-266.

[11] R. Stanley: *Enumerative Combinatorics*, vol. **1**, Cambridge University Press, New York/Cambridge, 1999.