A Note on the Exposure Property of SBIBD

Yejing Wang, Jennifer Seberry, Reihaneh Safavi-Naini

School of Information Technology and Computer Science
University of Wollongong
Wollongong 2522, Australia

Ryoh Fuji-Hara

Institute of Policy and Planning Sciences
University of Tsukuba
Tsukuba 305-8573, Japan

1 Introduction

In this paper we define an *exposure property of SBIBD*. Informally, if a subset F is included in a union of a number of blocks, and F has a constant number of common points with each block building up the union, then the family of these blocks is uniquely determined. It was motivated by cryptographic problems such as, in broadcast encryption systems, ensuring that only authorized users can receive the content. In broadcast encryption system, the content is encrypted. Each user is assigned a decoder which contains a number of decryption keys such that he can decrypt and receive the content. When some users produce another decoder, which is not identical to each of their decoders, consisting of an equal number of keys from each of their decoders, it is expected to identify all of them.

2 Preliminaries

Definition 2.1 *Let v, k and λ be positive integers such that $v > k \geq 2$. A (v, k, λ)-balanced incomplete block design is a pair $(X, \mathcal{B})$ such that the following properties are satisfied:*

(1) X is a set of v points;
(2) $\mathcal{B}$ is a family of k-subsets, called blocks, of X; and
(3) every pair of distinct points of X is contained in exactly λ blocks.

Email addresses: [yejing/jennie/rei]@uow.edu.au (Yejing Wang, Jennifer Seberry, Reihaneh Safavi-Naini), fujihara@sk.tsukuba.ac.jp (Ryoh Fuji-Hara).

We use the notation (v,k,λ)-BIBD instead of a (v,k,λ)-balanced incomplete block design. A (v,k,λ)-BIBD has the following properties.

Definition 2.2 *A (v,k,λ)-BIBD is called symmetric if $b=v$.*

Consider a block design $(X,\mathcal{B})$ and a set of blocks $\mathcal{C}=\{B_1,B_2,\cdots,B_c\}\subseteq\mathcal{B}$. Let F be a k-subset of X satisfying the following properties,

$$\begin{cases} |F\cap B_1|=|F\cap B_2|=\cdots=|F\cap B_c| \\ F\setminus(B_1\cup B_2\cup\cdots\cup B_c)=\emptyset. \end{cases} \tag{1}$$

Denote by $\widetilde{\mathcal{C}}$ the set of all k-subsets $F\subseteq X$ that satisfy (1). The set $\mathcal{C}$ is called exposed if the intersection of members of $\mathcal{C}$ with any member $F\in\widetilde{\mathcal{C}}$ has maximum size, and no other block of $\mathcal{B}$ has the same size intersection with F. In other words, $\mathcal{C}$ satisfies the following. For every $F\in\widetilde{\mathcal{C}}$

(i) $|F\cap B_i|=\max_{B\in\mathcal{B}}|F\cap B|$, for all $B_i\in\mathcal{C}$; and

(ii) there is no $B\notin\mathcal{C}$ such that $|F\cap B|=|F\cap B_1|$.

Definition 2.3 *A block design is c-exposed if every family of c blocks is exposed.*

3 3-Exposed Block Designs

Theorem 3.1 *A (v,k,λ)-SBIBD is 3-exposed if $\lambda<k/9$.*

Example 3.1 *Let $X=Z_{133}$, $\mathcal{B}=\{B_0,B_1,\cdots,B_{132}\}$, where the blocks of the (133,12,1)-SBIBD are*

$$B_i=\{0{+}i,1{+}i,3{+}i,12{+}i,20{+}i,34{+}i,38{+}i,81{+}i,88{+}i,94{+}i,104{+}i,109{+}i\}$$

for $0\le i\le 132$. Take 3 blocks $\mathcal{C}=\{B_0,B_1,B_2\}$ and a false block F

$$\begin{aligned} B_0&=\{0,\ 1,\ 3,\ 12,\ 20,\ 34,\ 38,\ 81,\ 88,\ 94,\ 104,\ 109\}\\ B_1&=\{1,\ 2,\ 4,\ 13,\ 21,\ 35,\ 39,\ 82,\ 89,\ 95,\ 105,\ 110\}\\ B_2&=\{2,\ 3,\ 5,\ 14,\ 22,\ 36,\ 40,\ 83,\ 90,\ 96,\ 106,\ 111\}\\ F&=\{1,\ 2,\ 3,\ \ 4,\ \ \ 5,\ \ 12,\ 13,\ 14,\ 20,\ 21,\ \ 22,\ \ \ 34\} \end{aligned}$$

It is clear that $F\subset(B_0\cup B_1\cup B_2)$ and

$$|F\cap B_0|=|F\cap B_1|=|F\cap B_2|=5$$

For an $i > 2$, if $|F \cap B_i| \geq 5$ then one of the following three

$$|B_0 \cap B_i| \geq 2,\ |B_1 \cap B_i| \geq 2,\ |B_2 \cap B_i| \geq 2$$

is satisfied, but we know that

$$|B_0 \cap B_i| = 1,\ |B_1 \cap B_i| = 1,\ |B_2 \cap B_i| = 1$$

This shows that $|F \cap B_i| < 5$ for $i > 2$. That is, B_0, B_1, B_2 are the only blocks that have the maximum intersections with F.

4 Remark

The existence of a block design with c-exposure property remains open for $c > 3$.