

**Research article****Construction of blocked designs with multi block variables****Yuna Zhao***

School of Mathematics and Statistics, Shandong Normal University, Jinan 250358, China

* **Correspondence:** Email: yunazhao0504@163.com.

Abstract: When experimental units are inhomogeneous, blocking the experimental units into categories is crucial so as to estimate the treatment effects precisely. In practice, the inhomogeneity often comes from different sources known as block variables in design terminology. The paper considers the blocking problems with multi block variables. The construction methods of the optimal blocked regular 2^{n-m} designs with multi block variables under the general minimum lower order confounding criterion for $\frac{5N}{16} + 1 \leq n \leq N - 1$ are provided, where $N = 2^{n-m}$.

Keywords: blocked design; factorial factorial design; general minimum lower order confounding; multi block variables; optimality

Mathematics Subject Classification: 62K05, 62K15

1. Introduction

Regular two-level designs are widely used in factorial experiments. When the size of experimental units is large, inhomogeneity of experimental units has bad influences on estimating treatment effects (see, [1, 2]). A useful way to reduce such bad influences is to block the experimental units into categories known as blocks. Thus, choosing optimal blocked regular two-level designs becomes an important issue.

As pointed out by [1], there are two kinds of blocking problems. One is called the single block variable problem which involves only one block variable and the other is called the multi block variables problem which considers two or more block variables. In the last decades, most of the literature were concerned with the single block variable problem. Sitter et al. [3], H. Chen and C. S. Cheng [4], R. C. Zhang and D. K. Park [5], and S. W. Cheng and C. F. J. Wu [6] respectively proposed different minimum aberration (MA) criteria which are suitable for selecting blocked designs with single block variable. Under these MA criteria, the construction methods of blocked designs with single block variable were discussed in [7–9].

Zhang et al. [10] proposed the general minimum lower-order confounding (GMC) criterion for

choosing optimal regular two-level designs. The GMC criterion is preferable when there are some prior knowledge on the importance ordering of treatment effects. R. C. Zhang and R. Mukerjee [11] extended the GMC criterion to blocked designs with single block variable, referred as B-GMC criterion, and gave the construction methods of B-GMC blocked designs via complementary designs. From different considerations, [12] proposed another GMC criterion for blocked designs with single block variable, referred as B¹-GMC. Zhao et al. [13] and Zhao et al. [14] studied the construction methods of B¹-GMC designs. Zhang et al. [15] proposed multi-stage differential evolution algorithm for constrained *D*-optimal design. Gashi [16] considered symmetric block design.

Compared to the experiments involving a single block variable, the experiments involving multi block variables are often encountered in practice. As has been mentioned in [1], in the agricultural context, when designs are laid out in rectangular schemes, both row and column inhomogeneity effects probably exist in the soil. Another example of multi block variables problem is from [2], which considers comparing two gasoline additives by testing them on two cars with two drivers over two days. In this experiment, three variables, cars, drivers and days, have to be considered to partition the experimental units.

Despite the wide application background, the multi block variables problem is less studied due to its complexity. In particular, constructing optimal designs with multi block variables is considerably challenging. Under the MA criterion, [17] developed some rules for constructing optimal regular two-level blocked designs with multi block variables. Zhang et al. [18] extended the idea of the GMC criterion to the case of multi block variables problem and developed the blocked GMC criterion, called B²-GMC criterion. Inheriting the advantage of the GMC criterion, a B²-GMC design is particularly preferable when some prior information on importance ordering of treatment effects is present. Zhang et al. [18] tabulated some B²-GMC designs with small numbers of treatment factors and small run sizes by computer search. When n or N is large, computer search becomes computationally challenging, where $N = 2^{n-m}$. Zhao et al. [19] studied the B²-GMC criterion and constructed a small number of B²-GMC designs. In this paper, the B²-GMC designs with the number of treatment factors n all over $5N/16 + 1 \leq n \leq N - 1$ are constructed. The construction results cover all that of [19]. The structures of the constructed B²-GMC designs are concise and easy to implement.

The rest of the paper is organized as follows. Section 2 reviews the B²-GMC criterion and introduces some notation. The construction methods of B²-GMC designs are provided in Section 3. Section 4 gives concluding remarks. Some proofs are deferred to Appendix.

2. Preliminaries: B²-GMC criterion and notation

Let $q = n - m$ and $N = 2^q$. Denote the regular two-level saturated design as

$$\mathbf{H}_q = \{\mathbf{1}, \mathbf{2}, \mathbf{12}, \mathbf{3}, \mathbf{13}, \mathbf{23}, \mathbf{123}, \dots, \mathbf{123 \cdots q}\}$$

in Yates order, where the columns $\mathbf{1}, \mathbf{2}, \dots$, and \mathbf{q} are q independent columns in the form of

$$\begin{aligned} \mathbf{1}' &= (1, -1, 1, -1, \dots, 1, -1)_{2^q}, \\ \mathbf{2}' &= (1, 1, -1, -1, \dots, 1, 1, -1, -1)_{2^q}, \\ &\dots \\ \mathbf{q}' &= (1, \dots, 1, -1, \dots, -1)_{2^q}, \end{aligned}$$

where the superscript of each column denotes transpose, in **1** the entry 1, followed by -1 , is repeated 2^{q-1} times, and in **2** the two successive entries 1's, followed by two successive -1 's, are repeated 2^{q-2} times, \dots , and in **q** the 2^{q-1} successive entries 1's are followed by 2^{q-1} successive -1 's. The remaining columns in \mathbf{H}_q are generated by taking the component-wise products of any k of the q independent columns, where $k = 2, 3, \dots, q$. For example, the column **12** is generated by taking component-wise products of the independent columns **1** and **2**. Denote $\mathbf{H}_1 = \{\mathbf{1}\}$, $\mathbf{H}_r = \{\mathbf{H}_{r-1}, \mathbf{r}, \mathbf{rH}_{r-1}\}$ for $r = 2, \dots, q$, where $\mathbf{rH}_{r-1} = \{\mathbf{rd} : \mathbf{d} \in \mathbf{H}_{r-1}\}$ and \mathbf{H}_r consists of the first $2^r - 1$ columns of \mathbf{H}_q . Let $\mathbf{F}_{qr} = \{\mathbf{q}, \mathbf{qH}_{r-1}\}$ for $r = 2, \dots, q$, then \mathbf{F}_{qr} consists of the first 2^{r-1} columns of \mathbf{F}_{qq} and \mathbf{F}_{qq} consists of the last 2^{q-1} columns of \mathbf{H}_q .

Suppose that the inhomogeneity of the units of an experiment comes from s different sources, i.e., s block variables, denoted as b_1, b_2, \dots, b_s . Suppose the block variable b_j has 2^{l_j} levels, i.e., the 2^{n-m} units are grouped into 2^{l_j} blocks with respect to the block variable b_j . Then there should be l_j independent columns of \mathbf{H}_q to implement such a blocking schedule. Such columns are called block columns in the following. Denote F_j as the collection of the l_j independent block columns corresponding to the block variable b_j . It is worth noting that the columns in F_j have the following two relations:

- (i) the l_j columns in F_j are independent of each other for $j = 1, 2, \dots, s$;
- (ii) a column from F_j is not necessarily independent of the columns from F_i , $i \neq j$.

Clearly, when $s = 1$, the blocking problem with multi block variables reduces to that with a single block variable. For simplicity, we consider only the case of $l_j = 1$ for $j = 1, 2, \dots, s$. Then there are s block columns and each of them blocks the 2^{n-m} experimental units into 2 groups. Here, we would like to emphasize that the s block columns are not necessarily independent of each other.

Throughout the paper, we use $\mathbf{D} = (\mathbf{D}_t, \mathbf{D}_b)$ to denote a blocked regular $2^{n-m} : 2^s$ design, where \mathbf{D}_t is a regular 2^{n-m} design, and \mathbf{D}_b consists of s block columns. We will not differentiate block variables, block columns, and block factors in the following. B. Tang and C. F. J. Wu [20] introduced the concept of isomorphism which helps to narrow down the search for optimal blocked designs in this paper. An isomorphism ϕ is a one-to-one mapping from \mathbf{H}_q to \mathbf{H}_q such that $\phi(\mathbf{xy}) = \phi(\mathbf{x})\phi(\mathbf{y})$ for every $\mathbf{x} \neq \mathbf{y} \in \mathbf{H}_q$. Two $2^{n-m} : 2^s$ designs $\mathbf{D}^1 = (\mathbf{D}_t^1, \mathbf{D}_b^1)$ and $\mathbf{D}^2 = (\mathbf{D}_t^2, \mathbf{D}_b^2)$ are isomorphic if there exists an isomorphism ϕ that maps \mathbf{D}_t^1 onto \mathbf{D}_t^2 , and \mathbf{D}_b^1 onto \mathbf{D}_b^2 .

Zhang et al. [18] put forward the effect hierarchy principle for blocked designs with multi block variables as follows:

- (i) Lower order treatment factorial effects are more likely to be important than higher order ones, and treatment factorial effects of the same order are equally likely to be important.
- (ii) Lower order block factorial effects are more likely to be important than higher order ones, and block factorial effects of the same order are equally likely to be important.
- (iii) All the interactions between treatment and block factors are negligible.

With the effect hierarchy principle and weak assumption of effects involving three or more factors are usually not important and negligible, [18] proposed the B^2 -GMC criterion which considers only the confounding among the main effects and two-factor interactions. As a common assumption in the blocking issues, if a treatment effect is confounded with a potentially significant block effect, the treatment effect cannot be estimated. Thus, confounding of the main effects of treatment factors with any potentially significant block effect is not allowed. In the following, we always suppose the main effects and the two-factor interactions of the block factors are potentially significant.

Denote ${}_1^{\#}C_2^{(p)}(\mathbf{D})$ as the number of main treatment effects which are aliased with p two-treatment-factor interactions (2tfi's) but not with any potentially significant block effects, where $p = 0, 1, 2, \dots, P$, $P = n(n-1)/2$. Similarly, ${}_2^{\#}C_2^{(p)}(\mathbf{D})$ denotes the number of 2tfi's which are aliased with the other p 2tfi's but not with any potentially significant block effects. Denote

$$\begin{aligned} {}_1^{\#}C_2(\mathbf{D}) &= ({}^{\#}C_2^{(0)}(\mathbf{D}), {}^{\#}C_2^{(1)}(\mathbf{D}), \dots, {}^{\#}C_2^{(P)}(\mathbf{D})), \\ {}_2^{\#}C_2(\mathbf{D}) &= ({}^{\#}C_2^{(0)}(\mathbf{D}), {}^{\#}C_2^{(1)}(\mathbf{D}), \dots, {}^{\#}C_2^{(P)}(\mathbf{D})), \\ {}^{\#}C(\mathbf{D}) &= ({}^{\#}C_2(\mathbf{D}), {}^{\#}C_2(\mathbf{D})). \end{aligned} \quad (2.1)$$

A blocked design $\mathbf{D} = (\mathbf{D}_t, \mathbf{D}_b)$ is called a B^2 -GMC design if \mathbf{D} sequentially maximizes (2.1). Let ${}^{\#}C_j^{(p)}(\mathbf{D}_t)$ be the number of i -th order effects which are aliased with p j -th order effects of \mathbf{D}_t . Let

$$\begin{aligned} {}_1^{\#}C_2(\mathbf{D}_t) &= ({}^{\#}C_2^{(0)}(\mathbf{D}_t), {}^{\#}C_2^{(1)}(\mathbf{D}_t), \dots, {}^{\#}C_2^{(P)}(\mathbf{D}_t)), \\ {}_2^{\#}C_2(\mathbf{D}_t) &= ({}^{\#}C_2^{(0)}(\mathbf{D}_t), {}^{\#}C_2^{(1)}(\mathbf{D}_t), \dots, {}^{\#}C_2^{(P)}(\mathbf{D}_t)), \\ {}^{\#}C(\mathbf{D}_t) &= ({}^{\#}C_2(\mathbf{D}_t), {}^{\#}C_2(\mathbf{D}_t)). \end{aligned} \quad (2.2)$$

A 2^{n-m} design \mathbf{D}_t is called a GMC design if \mathbf{D}_t sequentially maximizes (2.2).

Let

$$U(\mathbf{D}_b) = \{\gamma \in \mathbf{H}_q : \gamma \in \mathbf{D}_b \text{ or } \gamma = \mathbf{a}\mathbf{b} \text{ with } \mathbf{a}, \mathbf{b} \in \mathbf{D}_b\},$$

i.e., $U(\mathbf{D}_b)$ contains the potentially significant block effects. As aforementioned, confounding between main treatment effects and potentially significant block effects is not allowed which leads to $\mathbf{D}_t \cap U(\mathbf{D}_b) = \emptyset$, the empty set, and consequently ${}^{\#}C_2^{(p)}(\mathbf{D}) = {}^{\#}C_2^{(p)}(\mathbf{D}_t)$, $p = 0, 1, 2, \dots, P$.

As a preparation of deriving B^2 -GMC designs, we introduce one more piece of notation. For $\mathbf{D}_t \subset \mathbf{H}_q$ and $\gamma \in \mathbf{H}_q$, define

$$B_2(\mathbf{D}_t, \gamma) = \#(\{\mathbf{d}_1, \mathbf{d}_2 : \mathbf{d}_1, \mathbf{d}_2 \in \mathbf{D}_t, \mathbf{d}_1\mathbf{d}_2 = \gamma\}),$$

where $\#$ denotes the cardinality of a set, and $\mathbf{d}_1\mathbf{d}_2$ stands for the two-factor interaction of \mathbf{d}_1 and \mathbf{d}_2 . Thus, $B_2(\mathbf{D}_t, \gamma)$ equals the number of 2tfi's of \mathbf{D}_t appearing in the alias set that contains γ .

3. Constructions of B^2 -GMC designs

3.1. B^2 -GMC designs with $\frac{5N}{16} + 1 \leq n \leq \frac{N}{2}$

To construct B^2 -GMC designs, one should first consider the first part in (2.1), i.e., ${}^{\#}C_2(\mathbf{D})$. Recall that ${}^{\#}C_2^{(p)}(\mathbf{D}) = {}^{\#}C_2^{(p)}(\mathbf{D}_t)$ for $p = 0, 1, \dots, P$, then choosing \mathbf{D} to maximize ${}^{\#}C_2(\mathbf{D})$ reduces to choosing \mathbf{D}_t to maximize ${}^{\#}C_2(\mathbf{D}_t)$.

A 2^{n-m} design \mathbf{D}_t is said to have *resolution R* if no c -factor interaction is confounded with any other interaction involving less than $R - c$ factors (see, [21]). Note that a 2^{n-m} design \mathbf{D}_t with resolution at least IV has ${}^{\#}C_2^{(0)}(\mathbf{D}_t) = n$ and ${}^{\#}C_2^{(p)}(\mathbf{D}_t) = 0$ for $p = 1, \dots, P$. This implies that a 2^{n-m} design \mathbf{D}_t with resolution at least IV must maximize ${}^{\#}C_2(\mathbf{D}_t)$. When $\frac{5N}{16} + 1 \leq n \leq \frac{N}{2}$, if \mathbf{D}_t has resolution at least IV, then $\mathbf{D}_t \subset \mathbf{F}_{qq}$ (see, [22]). In the remaining part of this section, we suppose $\mathbf{D}_t \subset \mathbf{F}_{qq}$. By Lemma 1 in [13], to choose \mathbf{D}_b from \mathbf{H}_q , there are two possibilities: (i) $\mathbf{D}_b \cap \mathbf{F}_{qq} = \emptyset$, and (ii) $\mathbf{D}_b \cap \mathbf{F}_{qq} \neq \emptyset$. As has been pointed out, when constructing B^2 -GMC designs, there should be $\mathbf{D}_t \cap U(\mathbf{D}_b) = \emptyset$. This leads to the constraint

$$\#\{U(\mathbf{D}_b) \cap \mathbf{F}_{qq}\} \leq \frac{N}{2} - n. \quad (3.1)$$

Certainly, for \mathbf{D}_b in the case (i), $U(\mathbf{D}_b) \subset \mathbf{H}_{q-1}$ and thus \mathbf{D}_b satisfies the constraint (3.1). For \mathbf{D}_b in the case (ii), there must be $U(\mathbf{D}_b) \cap \mathbf{F}_{qq} \neq \emptyset$ resulting in the necessity to investigate the number of columns in $U(\mathbf{D}_b) \cap \mathbf{F}_{qq}$. The following lemma addresses this question.

Lemma 1. *Let \mathbf{D}_b be any s -projection of \mathbf{H}_q with $\mathbf{D}_b \cap \mathbf{F}_{qq} \neq \emptyset$. If $2^k \leq s \leq 2^{k+1} - 1$ for some $k \leq q-2$, then $\#\{U(\mathbf{D}_b) \cap \mathbf{F}_{qq}\} \geq 2^k$.*

The proof of Lemma 1 is lengthy and thus deferred to Appendix.

Lemmas 2 and 3 below are straightforward extensions of some results in [19] and [23], respectively. These two lemmas are helpful in deriving the construction methods of B^2 -GMC designs.

Lemma 2. *Let \mathbf{D}_b be any s -projection of \mathbf{H}_q with $2^k \leq s \leq 2^{k+1} - 1$ for some $k \leq q-1$.*

- (i) *If $\mathbf{D}_b \cap \mathbf{F}_{qq} = \emptyset$, then $\#\{U(\mathbf{D}_b) \cap \mathbf{H}_{q-1}\} \geq 2^{k+1} - 1$ and the equality holds when \mathbf{D}_b has $k+1$ independent columns.*
- (ii) *If $\mathbf{D}_b \cap \mathbf{F}_{qq} \neq \emptyset$, then $\#\{U(\mathbf{D}_b) \cap \mathbf{H}_{q-1}\} \geq 2^k - 1$ and the equality holds when \mathbf{D}_b has $k+1$ independent columns.*
- (iii) *If $\mathbf{D}_b \subset \mathbf{H}_{k+1}$, then $U(\mathbf{D}_b) = \mathbf{H}_{k+1}$.*
- (iv) *If $\mathbf{D}_b \subset \mathbf{H}_k \cup \mathbf{F}_{q(k+1)}$, then $U(\mathbf{D}_b) = \mathbf{H}_k \cup \mathbf{F}_{q(k+1)}$.*

Lemma 3. *Suppose \mathbf{D}_t consists of the last n columns of \mathbf{H}_q . For any two columns γ_1 and γ_2 in \mathbf{H}_{q-1} , if γ_1 is ahead of γ_2 in Yates order, then $B_2(\mathbf{D}_t, \gamma_1) \geq B_2(\mathbf{D}_t, \gamma_2)$.*

Combining Lemmas 1, 2 and 3, the following theorem provides the constructions of B^2 -GMC designs with $\frac{5N}{16} + 1 \leq n \leq \frac{N}{2}$, where $N \geq 16$.

Theorem 1. *Suppose $\mathbf{D} = (\mathbf{D}_t, \mathbf{D}_b)$ is a $2^{n-m} : 2^s$ design with $2^r \leq \frac{N}{2} - n \leq 2^{r+1} - 1$ for some $r \leq q-3$ and $2^k \leq s \leq 2^{k+1} - 1$ for some $k \leq q-2$. The design $\mathbf{D} = (\mathbf{D}_t, \mathbf{D}_b)$ is a B^2 -GMC design if \mathbf{D}_t consists of the last n columns of \mathbf{F}_{qq} and*

- (i) \mathbf{D}_b is any s -projection of $\mathbf{H}_k \cup \mathbf{F}_{q(k+1)}$ when $1 \leq k \leq r$,
- (ii) \mathbf{D}_b is any s -projection of \mathbf{H}_{k+1} when $r+1 \leq k \leq q-2$.

Proof. Let $\mathbf{D}^* = (\mathbf{D}_t^*, \mathbf{D}_b^*)$ be a $2^{n-m} : 2^s$ design with $\mathbf{D}_t^* \subset \mathbf{F}_{qq}$ and $U(\mathbf{D}_b^*) \subset \mathbf{H}_q \setminus \mathbf{D}_t^*$. According to Lemma 1 of [22],

$$B_2(\mathbf{D}_t^*, \gamma) = \begin{cases} 0, & \text{if } \gamma \in \mathbf{F}_{qq}, \\ B_2(\bar{\mathbf{D}}_t^*, \gamma) + n - \frac{N}{4}, & \text{if } \gamma \in \mathbf{H}_{q-1}, \end{cases}$$

where $\bar{\mathbf{D}}_t^* = \mathbf{F}_{qq} \setminus \mathbf{D}_t^*$. Note that \mathbf{D}_t has resolution at least IV, then $\#_1 C_2$ is maximized by \mathbf{D} . Therefore, we consider only $\#_2 C_2$ in (2.1) in the following.

For (i). From Theorem 2 of [22], \mathbf{D}_t is a GMC 2^{n-m} design and thus \mathbf{D}_t maximizes (2.2) among all \mathbf{D}_t^* . From Lemma 2 (iv), if \mathbf{D}_b is any s -projection of $\mathbf{H}_k \cup \mathbf{F}_{q(k+1)}$, then $U(\mathbf{D}_b) = \mathbf{H}_k \cup \mathbf{F}_{q(k+1)}$. Suppose γ_0 is the last column of \mathbf{H}_k in Yates order and $B_2(\mathbf{D}_t, \gamma_0) = p_0$, where $p_0 \geq n - \frac{N}{4} \geq \frac{N}{16} + 1 \geq 2$. From Lemma 3, for any $\gamma \in \mathbf{H}_k$, we have $B_2(\mathbf{D}_t, \gamma) \geq p_0$. Since $\mathbf{D}_t \subset \mathbf{F}_{qq}$, we have $B_2(\mathbf{D}_t, \gamma) = 0$ for any $\gamma \in \mathbf{F}_{qq}$. By the definition of $\#_2 C_2^{(p)}(\mathbf{D})$, when $p \leq p_0 - 2$, we have $1 \leq p+1 \leq p_0 - 1$ and

$$\begin{aligned} \#_2 C_2^{(p)}(\mathbf{D}) &= (p+1)\#\{\gamma \in \mathbf{H}_q : \gamma \notin U(\mathbf{D}_b), B_2(\mathbf{D}_t, \gamma) = p+1\} \\ &= (p+1)\#\{\gamma \in \mathbf{H}_q : B_2(\mathbf{D}_t, \gamma) = p+1\} \end{aligned}$$

$$= \#_2^{\#} C_2^{(p)}(\mathbf{D}_t). \quad (3.2)$$

From Lemma 3, for any $\gamma \in \mathbf{H}_q \setminus \mathbf{H}_k$, we have $B_2(\mathbf{D}_t, \gamma) \leq p_0$. Therefore, when $p \geq p_0$, we have

$$\begin{aligned} \#_2^{\#} C_2^{(p)}(\mathbf{D}) &= (p+1)\#\{\gamma \in \mathbf{H}_q : \gamma \notin U(\mathbf{D}_b), B_2(\mathbf{D}_t, \gamma) = p+1\} \\ &= (p+1)\#\{\gamma \in (\mathbf{H}_{q-1} \setminus \mathbf{H}_k) \cup (\mathbf{F}_{qq} \setminus \mathbf{F}_{q(k+1)}) : B_2(\mathbf{D}_t, \gamma) = p+1\} \\ &= 0. \end{aligned} \quad (3.3)$$

From (3.2), we obtain that \mathbf{D} sequentially maximizes

$$(\#_2^{\#} C_2^{(0)}(\mathbf{D}), \#_2^{\#} C_2^{(1)}(\mathbf{D}), \dots, \#_2^{\#} C_2^{(p_0-2)}(\mathbf{D}))$$

among all \mathbf{D}^* since \mathbf{D}_t is a GMC design.

Suppose \mathbf{D} is not a B²-GMC design, then there exists a \mathbf{D}^* and some $p_1 \geq p_0 - 1$ such that

$$(\#_2^{\#} C_2^{(0)}(\mathbf{D}), \#_2^{\#} C_2^{(1)}(\mathbf{D}), \dots, \#_2^{\#} C_2^{(p_1-1)}(\mathbf{D})) = (\#_2^{\#} C_2^{(0)}(\mathbf{D}^*), \#_2^{\#} C_2^{(1)}(\mathbf{D}^*), \dots, \#_2^{\#} C_2^{(p_1-1)}(\mathbf{D}^*)), \quad (3.4)$$

and

$$\#_2^{\#} C_2^{(p_1)}(\mathbf{D}^*) > \#_2^{\#} C_2^{(p_1)}(\mathbf{D}). \quad (3.5)$$

Recall the definitions of $\#_2^{\#} C_2^{(p)}(\mathbf{D})$ and $\#_2^{\#} C_2^{(p)}(\mathbf{D}_t)$, we have

$$\begin{aligned} \frac{1}{p+1} \#_2^{\#} C_2^{(p)}(\mathbf{D}) &= \#\{\gamma \in \mathbf{H}_q : \gamma \notin U(\mathbf{D}_b), B_2(\mathbf{D}_t, \gamma) = p+1\} \\ &= \#\{\gamma \in \mathbf{H}_{q-1} : B_2(\mathbf{D}_t, \gamma) = p+1\} \\ &\quad - \#\{\gamma \in \mathbf{H}_k : B_2(\mathbf{D}_t, \gamma) = p+1\}, \end{aligned} \quad (3.6)$$

where the second equality is due to $B_2(\mathbf{D}_t, \gamma) = 0$ for any $\gamma \in \mathbf{F}_{qq}$. From (3.6), it is obtained that

$$\begin{aligned} \sum_{p=0}^P \frac{1}{p+1} \#_2^{\#} C_2^{(p)}(\mathbf{D}) &= \sum_{p=0}^P \#\{\gamma \in \mathbf{H}_{q-1} : B_2(\mathbf{D}_t, \gamma) = p+1\} \\ &\quad - \sum_{p=0}^P \#\{\gamma \in \mathbf{H}_k : B_2(\mathbf{D}_t, \gamma) = p+1\} \\ &= \#\{\mathbf{H}_{q-1} \setminus \mathbf{H}_k\} = 2^{q-1} - 2^k. \end{aligned} \quad (3.7)$$

By (3.2), (3.3) and (3.7), it is obtained that

$$\sum_{p=0}^P \frac{1}{p+1} \#_2^{\#} C_2^{(p)}(\mathbf{D}) = \sum_{p=0}^{p_0-2} \frac{1}{p+1} \#_2^{\#} C_2^{(p)}(\mathbf{D}) + \frac{1}{p_0} \#_2^{\#} C_2^{(p_0-1)}(\mathbf{D}) = 2^{q-1} - 2^k. \quad (3.8)$$

Similarly, for \mathbf{D}^* we have

$$\sum_{p=0}^P \frac{1}{p+1} \#_2^{\#} C_2^{(p)}(\mathbf{D}^*) = \sum_{p=0}^P \#\{\gamma \in \mathbf{H}_{q-1} : B_2(\mathbf{D}_t^*, \gamma) = p+1\}$$

$$\begin{aligned}
& - \sum_{p=0}^P \#\{\boldsymbol{\gamma} \in U(\mathbf{D}_b^*) \cap \mathbf{H}_{q-1} : B_2(\mathbf{D}_t^*, \boldsymbol{\gamma}) = p + 1\} \\
& = 2^{q-1} - 1 - \#(U(\mathbf{D}_b^*) \cap \mathbf{H}_{q-1}).
\end{aligned} \tag{3.9}$$

From (3.2)–(3.5), we obtain

$$\begin{aligned}
\sum_{p=0}^P \frac{1}{p+1} {}^2C_2^{(p)}(\mathbf{D}) & = \sum_{p=0}^{p_1-1} \frac{1}{p+1} {}^2C_2^{(p)}(\mathbf{D}) + \frac{1}{p_1+1} {}^2C_2^{(p_1)}(\mathbf{D}) \\
& < \sum_{p=0}^{p_1-1} \frac{1}{p+1} {}^2C_2^{(p)}(\mathbf{D}^*) + \frac{1}{p_1+1} {}^2C_2^{(p_1)}(\mathbf{D}^*) \\
& \leq \sum_{p=0}^{p_1-1} \frac{1}{p+1} {}^2C_2^{(p)}(\mathbf{D}^*) + \sum_{p=p_1}^P \frac{1}{p+1} {}^2C_2^{(p)}(\mathbf{D}^*) \\
& = \sum_{p=0}^P \frac{1}{p+1} {}^2C_2^{(p)}(\mathbf{D}^*).
\end{aligned}$$

Then it leads to $\#(U(\mathbf{D}_b^*) \cap \mathbf{H}_{q-1}) < 2^k - 1$ from Eqs (3.8) and (3.9). This contradicts Lemma 2 (ii) and completes the proof of (i).

For (ii). From Lemma 1, if $\mathbf{D}_b^* \cap \mathbf{F}_{qq} \neq \emptyset$, then $\#(U(\mathbf{D}_b^*) \cap \mathbf{F}_{qq}) \geq 2^k \geq 2^{r+1}$ which implies $U(\mathbf{D}_b^*) \cap \mathbf{D}_t^* \neq \emptyset$. This is not allowed as has been pointed out. Therefore, if $r+1 \leq k \leq q-2$, there should be $\mathbf{D}_b^* \subset \mathbf{H}_{q-1}$. According to Lemma 2 (iii), if \mathbf{D}_b is an s -projection of \mathbf{H}_{k+1} , then $U(\mathbf{D}_b) = \mathbf{H}_{k+1}$. The remainder of the proof is similar to that of (i) and omitted. This completes the proof. \square

In the following, an example is provided to illustrate the constructions of B²-GMC $2^{n-m} : 2^s$ designs with $\frac{5N}{16} + 1 \leq n \leq \frac{N}{2}$.

Example 1. Consider constructing B²-GMC $2^{12-7} : 2^2$ and $2^{12-7} : 2^9$ designs. For both B²-GMC designs to be constructed, we have $q = n - m = 5$, $N = 32$ and $r = 2$ as $2^2 \leq \frac{N}{2} - n \leq 2^3 - 1$. The values of the parameters N and n satisfy $\frac{5N}{16} + 1 \leq n \leq \frac{N}{2}$. Therefore, to construct these two B²-GMC designs, \mathbf{D}_t should be the last 12 columns of \mathbf{F}_{55} .

For the case $2^{12-7} : 2^2$, we have $s = 2$ which gives $k = 1$. Therefore, we should choose 2 block columns according to Theorem 1 (i) as $k < r$. Without loss of generality, let $\mathbf{D}_{b1} = \{\mathbf{1}, \mathbf{5}\}$ be the 2-projection of $\mathbf{H}_1 \cup \mathbf{F}_{52}$. Then $\mathbf{D} = (\mathbf{D}_t, \mathbf{D}_{b1})$ is a B²-GMC $2^{12-7} : 2^2$ design.

For the case $2^{12-7} : 2^9$, we have $s = 9$ which gives $k = 3$. Therefore, we should choose 9 block columns according to Theorem 1 (ii) as $k > r$. Without loss of generality, let $\mathbf{D}_{b2} = \{\mathbf{1}, \mathbf{2}, \mathbf{12}, \mathbf{3}, \mathbf{13}, \mathbf{23}, \mathbf{123}, \mathbf{4}, \mathbf{14}\}$ be the 9-projection of \mathbf{H}_4 . Then $\mathbf{D} = (\mathbf{D}_t, \mathbf{D}_{b2})$ is a B²-GMC $2^{9-4} : 2^9$ design.

3.2. B²-GMC designs with $n > \frac{N}{2}$

Similar to the discussion in the first paragraph of Section 3.1, when constructing B²-GMC designs with $n > \frac{N}{2}$, we should also first maximize ${}^2C_2(\mathbf{D}_t)$. Suppose the number of columns in $\mathbf{H}_q \setminus \mathbf{D}_t$ satisfies $2^r \leq N - 1 - n \leq 2^{r+1} - 1$ for some $r \leq q - 2$. According to the first paragraph of Section 3.2 in [22],

when $n > \frac{N}{2}$, if \mathbf{D}_t maximizes ${}^{\#}C_2(\mathbf{D}_t)$, then $\mathbf{H}_q \setminus \mathbf{D}_t \subset \mathbf{H}_{r+1}$ up to isomorphism. This implies that $\mathbf{D}_b \subset \mathbf{H}_{r+1}$.

Suppose $2^k \leq s \leq 2^{k+1} - 1$ for some $k \leq q - 2$. According to Lemma 2 (i) and (ii) combined with Lemma 1, we have $\#U(\mathbf{D}_b) \geq 2^{k+1} - 1$ no matter $\mathbf{D}_b \cap \mathbf{F}_{qq} = \emptyset$ or $\mathbf{D}_b \cap \mathbf{F}_{qq} \neq \emptyset$. Therefore, there should be $k = r$ with $N - 1 - n = 2^{k+1} - 1$ or $k < r$, otherwise $U(\mathbf{D}_b) \cap \mathbf{D}_t \neq \emptyset$. For the case of $k = r$ with $N - 1 - n = 2^{k+1} - 1$, it is trivial since $\mathbf{D}_t = \mathbf{H}_q \setminus \mathbf{H}_{k+1}$ and thus $\mathbf{D}_b \subset \mathbf{H}_{k+1}$. This obtains that the design $\mathbf{D} = (\mathbf{D}_t, \mathbf{D}_b)$ with $\mathbf{D}_t = \mathbf{H}_q \setminus \mathbf{H}_{k+1}$ and \mathbf{D}_b being any s -projection of \mathbf{H}_{k+1} is a B^2 -GMC design. The following theorem considers the constructions of B^2 -GMC designs for the case of $k < r$.

Theorem 2. Suppose $\mathbf{D} = (\mathbf{D}_t, \mathbf{D}_b)$ is a $2^{n-m} : 2^s$ design with $2^r \leq N - 1 - n \leq 2^{r+1} - 1$ for some $r \leq q - 2$ and $2^k \leq s \leq 2^{k+1} - 1$ for some $k < r$. The design $\mathbf{D} = (\mathbf{D}_t, \mathbf{D}_b)$ is a B^2 -GMC design if \mathbf{D}_t consists of the last n columns of \mathbf{H}_q and \mathbf{D}_b is any s -projection of \mathbf{H}_{k+1} .

Proof. Let $\mathbf{D}^* = (\mathbf{D}_t^*, \mathbf{D}_b^*)$ be a $2^{n-m} : 2^s$ design with $\mathbf{H}_q \setminus \mathbf{D}_t^* \subset \mathbf{H}_{r+1}$. Then we have $U(\mathbf{D}_b^*) \subset \mathbf{H}_q \setminus \mathbf{D}_t^*$. From Lemma 3 of [22],

$$B_2(\mathbf{D}_t^*, \gamma) = \begin{cases} n - N/2, & \text{if } \gamma \in \mathbf{H}_q \setminus \mathbf{H}_{r+1}, \\ B_2(\bar{\mathbf{D}}_t^*, \gamma) + \frac{N}{2} - 2^r, & \text{if } \gamma \in \mathbf{H}_{r+1}, \end{cases}$$

where $\bar{\mathbf{D}}_t^* = \mathbf{H}_q \setminus \mathbf{D}_t^*$.

By Lemma 2 (iv), if \mathbf{D}_b is any s -projection of \mathbf{H}_{k+1} , then $U(\mathbf{D}_b) = \mathbf{H}_{k+1}$. Suppose γ_0 is the last column of \mathbf{H}_{k+1} in Yates order and $B_2(\mathbf{D}_t, \gamma_0) = p_0$, where $p_0 \geq \frac{N}{2} - 2^r > n - \frac{N}{2} \geq 1$. From Lemma 3, if $\gamma \in \mathbf{H}_{k+1}$, then $B_2(\mathbf{D}_t, \gamma) \geq p_0$. By the definition of ${}^{\#}C_2^{(p)}(\mathbf{D})$, when $p \leq p_0 - 2$, we have $1 \leq p + 1 \leq p_0 - 1$ and

$$\begin{aligned} {}^{\#}C_2^{(p)}(\mathbf{D}) &= (p+1)\#\{\gamma \in \mathbf{H}_q : \gamma \notin U(\mathbf{D}_b), B_2(\mathbf{D}_t, \gamma) = p+1\} \\ &= (p+1)\#\{\gamma \in \mathbf{H}_q : B_2(\mathbf{D}_t, \gamma) = p+1\} \\ &= {}^{\#}C_2^{(p)}(\mathbf{D}_t). \end{aligned} \quad (3.10)$$

From Lemma 3, for any $\gamma \in \mathbf{H}_q \setminus \mathbf{H}_{k+1}$, we have $B_2(\mathbf{D}_t, \gamma) \leq p_0$. Therefore, when $p \geq p_0$, we have

$${}^{\#}C_2^{(p)}(\mathbf{D}) = (p+1)\#\{\gamma \in \mathbf{H}_q : \gamma \notin U(\mathbf{D}_b), B_2(\mathbf{D}_t, \gamma) = p+1\} = 0. \quad (3.11)$$

Since \mathbf{D}_t consists of the last n columns of \mathbf{H}_q , from Theorem 3 of [22], \mathbf{D}_t is a GMC 2^{n-m} design. Then \mathbf{D}_t sequentially maximizes (2.2). Recall that ${}^{\#}C_2^{(p)}(\mathbf{D}) = {}^{\#}C_2^{(p)}(\mathbf{D}_t)$ for $p = 0, 1, \dots, P$. Thus, (3.10) implies that \mathbf{D} maximizes

$$({}^{\#}C_2^{(0)}(\mathbf{D}), {}^{\#}C_2^{(1)}(\mathbf{D}), \dots, {}^{\#}C_2^{(P)}(\mathbf{D}), {}^{\#}C_2^{(0)}(\mathbf{D}), {}^{\#}C_2^{(1)}(\mathbf{D}), \dots, {}^{\#}C_2^{(p_0-2)}(\mathbf{D}))$$

among all \mathbf{D}^* .

Suppose \mathbf{D} is not a B^2 -GMC design, then there exists a \mathbf{D}^* and some $p_1 \geq p_0 - 1$ such that

$$\begin{aligned} &({}^{\#}C_2^{(0)}(\mathbf{D}), {}^{\#}C_2^{(1)}(\mathbf{D}), \dots, {}^{\#}C_2^{(P)}(\mathbf{D}), {}^{\#}C_2^{(0)}(\mathbf{D}), {}^{\#}C_2^{(1)}(\mathbf{D}), \dots, {}^{\#}C_2^{(p_1-1)}(\mathbf{D})) \\ &= ({}^{\#}C_2^{(0)}(\mathbf{D}^*), {}^{\#}C_2^{(1)}(\mathbf{D}^*), \dots, {}^{\#}C_2^{(P)}(\mathbf{D}^*), {}^{\#}C_2^{(0)}(\mathbf{D}^*), {}^{\#}C_2^{(1)}(\mathbf{D}^*), \dots, {}^{\#}C_2^{(p_1-1)}(\mathbf{D}^*)) \end{aligned}$$

and ${}^{\#}C_2^{(p_1)}(\mathbf{D}^*) > {}^{\#}C_2^{(p_1)}(\mathbf{D})$. With a similar argument to the proof of Theorem 1 (i), such a \mathbf{D}^* results in $\#\{U(\mathbf{D}_b^*) \cap \mathbf{H}_{q-1}\} < 2^{k+1} - 1$ which contradicts Lemma 2 (i). This completes the proof. \square

In the following, an example is provided to illustrate the constructions of B^2 -GMC $2^{n-m} : 2^s$ designs with $n > \frac{N}{2}$.

Example 2. Consider constructing B^2 -GMC $2^{9-5} : 2^2$ and $2^{12-8} : 2^3$ designs.

For the case $2^{9-5} : 2^2$, we have $q = n - m = 4$, $N = 16$ and $r = 2$ as $2^2 \leq N - n - 1 \leq 2^3 - 1$. Since $s = 2$, we obtain $k < r$ as $k = 1$. According to Theorem 2, let \mathbf{D}_{t1} be the last 9 columns of \mathbf{H}_4 , and $\mathbf{D}_{b1} = \{\mathbf{1}, \mathbf{2}\}$ be a 2-projection of \mathbf{H}_2 . Then $\mathbf{D} = (\mathbf{D}_{t1}, \mathbf{D}_{b1})$ is a B^2 -GMC $2^{9-5} : 2^2$ design.

For the case $2^{12-8} : 2^3$, we have $q = n - m = 4$, $N = 16$ and $r = 1$ as $2^1 \leq N - n - 1 \leq 2^2 - 1$. Since $s = 3$, we obtain $k = r$ as $k = 1$. As discussed in the second paragraph in Section 3.2, let \mathbf{D}_{t2} be the last 12 columns of \mathbf{H}_4 , and $\mathbf{D}_{b2} = \{\mathbf{1}, \mathbf{2}, \mathbf{12}\} = \mathbf{H}_2$. Then $\mathbf{D} = (\mathbf{D}_{t2}, \mathbf{D}_{b2})$ is a B^2 -GMC $2^{12-8} : 2^3$ design.

4. Concluding remarks

Regular two-level factorial designs are widely used in factorial experiments. Inhomogeneity of the units has bad influences on estimating the treatment effects when size of experimental units is large. To reduce such bad influences, a useful way is to block the experimental units into categories. As has been pointed out in [1], there are two types of blocking problems. One is the single block variable problem and the other is the multi block variables problem. In the last decades, the single block variable problem was maturely investigated in the literature.

As has been exemplified in Section 1, multi block variables problem is more widely encountered in practice compared to the blocking problem with a single block variable. However, the studies on multi block variables problem are relatively primitive. The GMC criterion is welcome in the situations where the importance ordering of treatment effects is present. Zhang et al. [18] proposed the B^2 -GMC criterion for choosing optimal blocked regular two-level designs. Construction methods on B^2 -GMC designs can only be found in [19] in which the B^2 -GMC designs of some n from $\frac{5N}{16} + 1 \leq n \leq \frac{N}{2}$ are constructed. In this paper, the B^2 -GMC designs of n all over $\frac{5N}{16} + 1 \leq n \leq N - 1$ are systematically constructed. The structures of the constructed B^2 -GMC designs are concise and easy to implement.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 11801331).

Conflict of interest

The authors declare that there is no conflict of interest.

References

1. S. Bisgaard, A note on the definition of resolution for blocked s^{n-p} designs, *Technometrics*, **36** (1994), 308–311.
2. C. F. J. Wu, M. S. Hamada, *Experiments: Planning, analysis, and optimization*, 2 Eds., New Jersey: Wiley, 2009.
3. R. R. Sitter, J. H. Chen, M. Feder, Fractional resolution and minimum aberration in blocked s^{n-k} designs, *Technometrics*, **39** (1997), 382–390.

4. H. G. Chen, C. S. Cheng, Theory of optimal blocking of s^{n-m} designs. *Ann. Stat.*, **27** (1999), 1948–1973.
5. R. C. Zhang, D. K. Park, Optimal blocking of two-level fractional factorial designs, *J. Stat. Plan. Infer.*, **91** (2000), 107–121.
6. S. W. Cheng, C. F. J. Wu, Choice of optimal blocking schemes in two-level and three-level designs, *Technometrics*, **44** (2002), 269–277.
7. H. Q. Xu, Blocked regular fractional factorial designs with minimum aberration, *Ann. Stat.*, **34** (2006), 2534–2553.
8. H. Q. Xu, R. W. Mee, Minimum aberration blocking schemes for 128-run designs, *J. Stat. Plan. Infer.*, **140** (2010), 3213–3229.
9. S. L. Zhao, P. F. Li, R. Karunamuni, Blocked two-level regular factorial designs with weak minimum aberration, *Biometrika*, **100** (2013), 249–253.
10. R. C. Zhang, P. Li, S. L. Zhao, M. Y. Ai, A general minimum lower-order confounding criterion for two-level regular designs, *Stat. Sinica*, **18** (2008), 1689–1705.
11. R. C. Zhang, R. Mukerjee, General minimum lower-order confounding in block designs using complementary sets, *Stat. Sinica*, **19** (2009), 1787–1802.
12. J. L. Wei, P. Li, R. C. Zhang, Blocked two-level regular designs with general minimum lower-order confounding, *J. Stat. Theory Pract.*, **8** (2014), 46–65.
13. S. L. Zhao, P. F. Li, R. C. Zhang, R. Karunamuni, Construction of blocked two-level regular factorial designs with general minimum lower-order confounding, *J. Stat. Plan. Infer.*, **143** (2013), 1082–1090.
14. Y. N. Zhao, S. L. Zhao, M. Q. Liu, A theory on constructing blocked two-level designs with general minimum lower-order confounding, *Front. Math. China*, **11** (2016), 207–235.
15. X. F. Zhang, Z. B. Zhu, C. Q. Zhang, Multi-stage differential evolution algorithm for constrained D-optimal design, *AIMS Mathematics*, **6** (2021), 2956–2969.
16. M. Gashi, On the symmetric block design with parameters $(280, 63, 14)$ admitting a Frobenius group of order 93, *AIMS Mathematics*, **4** (2019), 1258–1273.
17. S. L. Zhao, Q. Q. Zhao, Minimum aberration blocked designs with multiple block variables, *Metrika*, **84** (2021), 121–140.
18. R. C. Zhang, P. Li, J. L. Wei, Optimal two-level regular designs with multi block variables, *J. Stat. Theory Pract.*, **5** (2011), 161–178.
19. Y. N. Zhao, S. L. Zhao, M. Q. Liu, On constructing optimal two-level designs with multi block variables, *J. Syst. Sci. Complex*, **31** (2018), 773–786.
20. B. X. Tang, C. F. J. Wu, Characterization of minimum aberration 2^{n-k} designs in terms of their complementary designs, *Ann. Statist.*, **24** (1996), 2549–2559.
21. G. E. P. Box, J. S. Hunter, The 2^{k-p} fractional factorial designs, *Technometrics*, **3** (1961), 311–351.
22. P. F. Li, S. L. Zhao, R. C. Zhang, A theory on constructing 2^{n-m} designs with general minimum lower-order confounding, *Stat. Sinica*, **21** (2011), 1571–1589.

23. Q. Zhou, N. Balakrishnan, R. C. Zhang, The factor aliased effect number pattern and its application in experimental planning, *Can. J. Statist.*, **41** (2013), 540–555.

24. J. Chen, M. Q. Liu, Some theory for constructing general minimum lower order confounding designs, *Stat. Sinica*, **21** (2011), 1541–1555.

Appendix: Proof of Lemma 1.

We only need to prove $\#\{U(\mathbf{D}_b) \cap \mathbf{F}_{qq}\} \geq 2^k$ for the case of $s = 2^k$. Recall that

$$U(\mathbf{D}_b) = \mathbf{D}_b \cup \{\boldsymbol{\gamma} \in \mathbf{H}_q : \boldsymbol{\gamma} = \mathbf{a}\mathbf{b}, \mathbf{a}, \mathbf{b} \in \mathbf{D}_b\}.$$

We have

$$U(\mathbf{D}_b) \cap \mathbf{F}_{qq} = (\mathbf{D}_b \cap \mathbf{F}_{qq}) \cup (\{\boldsymbol{\gamma} \in \mathbf{H}_q : \boldsymbol{\gamma} = \mathbf{a}\mathbf{b}, \mathbf{a}, \mathbf{b} \in \mathbf{D}_b\} \cap \mathbf{F}_{qq}).$$

Denote $\mathbf{A} = \mathbf{D}_b \cap \mathbf{F}_{qq}$ and $\mathbf{E} = \mathbf{D}_b \cap \mathbf{H}_{q-1}$. Then $\mathbf{D}_b = \mathbf{A} \cup \mathbf{E}$, $\mathbf{A} \cap \mathbf{E} = \emptyset$,

$$\{\boldsymbol{\gamma} \in \mathbf{H}_q : \boldsymbol{\gamma} = \mathbf{a}\mathbf{b}, \mathbf{a}, \mathbf{b} \in \mathbf{D}_b\} \cap \mathbf{F}_{qq} = \mathbf{A} \otimes \mathbf{E},$$

and

$$U(\mathbf{D}_b) \cap \mathbf{F}_{qq} = \mathbf{A} \cup \mathbf{A} \otimes \mathbf{E},$$

where $\mathbf{A} \otimes \mathbf{E} = \{\boldsymbol{\gamma} \in \mathbf{H}_q : \boldsymbol{\gamma} = \mathbf{a}\mathbf{b}, \mathbf{a} \in \mathbf{A}, \mathbf{b} \in \mathbf{E}\}$. Thus, it suffices to prove

$$\#\{\mathbf{A} \cup \mathbf{A} \otimes \mathbf{E}\} \geq 2^k \quad (\text{A.1})$$

for $\#\mathbf{A} + \#\mathbf{E} = 2^k$.

Regarding to the columns in \mathbf{A} and \mathbf{E} , there are two cases:

(B1) $\#\mathbf{A} > \#\mathbf{E}$, or
(B2) $\#\mathbf{A} \leq \#\mathbf{E}$.

The global line of the remaining proof for Lemma 1 is as follows. In Lemma A.1, we first show that if (A.1) holds for the case (B1), then (A.1) holds for the case (B2). Afterwards, with Lemmas A.2–A.5, we prove that (A.1) indeed holds for the case (B1).

Lemma A.1. *Suppose that (A.1) holds for the case (B1), then (A.1) holds for the case (B2).*

Proof. For the \mathbf{A} and \mathbf{E} in the case (B2), without loss of generality, we suppose $\mathbf{q} \in \mathbf{A}$. Then,

$$\begin{aligned} \#\{\mathbf{A} \cup \mathbf{A} \otimes \mathbf{E}\} &= \#\{\mathbf{A} \otimes (\{\mathbf{I}_N\} \cup \mathbf{E})\} \\ &= \#((\mathbf{q}\mathbf{A}) \otimes (\{\mathbf{q}\} \cup \mathbf{q}\mathbf{E})) \\ &= \#\{(\{\mathbf{I}_N\} \cup \tilde{\mathbf{A}}) \otimes \tilde{\mathbf{E}}\} \\ &= \#\{\tilde{\mathbf{E}} \cup \tilde{\mathbf{E}} \otimes \tilde{\mathbf{A}}\}, \end{aligned}$$

where $\tilde{\mathbf{A}} = \mathbf{q}(\mathbf{A} \setminus \mathbf{q}) \subset \mathbf{H}_{q-1}$ and $\tilde{\mathbf{E}} = \{\mathbf{q}\} \cup \mathbf{q}\mathbf{E} \subset \mathbf{F}_{qq}$.

Note that $\#\tilde{\mathbf{A}} = \#\mathbf{A} - 1 \leq 2^{k-1} - 1$, $\#\tilde{\mathbf{E}} = \#\mathbf{E} + 1 \geq 2^{k-1} + 1$ and $\#\tilde{\mathbf{A}} + \#\tilde{\mathbf{E}} = 2^k$, then $\#\tilde{\mathbf{E}} > \#\tilde{\mathbf{A}}$ and the case (B2) converts into the case (B1). Therefore, if (A.1) holds for the case (B1), then (A.1) holds for the case (B2). This completes the proof. \square

In the following, we only need to prove that (A.1) holds for the case (B1).

For \mathbf{A} in the case (B1), we have $\#\mathbf{A} \geq 2^{k-1} + 1$. Then, \mathbf{A} has at least $k + 1$ independent columns. We suppose \mathbf{A} has $h + 1 (\geq k + 1)$ independent columns. Let \mathbf{e} denote the h th independent column in \mathbf{H}_q in Yates order. Up to isomorphism, \mathbf{A} can be expressed as

$$\mathbf{A} = \mathbf{A}_1 \cup \{\mathbf{e}\mathbf{a}_1, \mathbf{e}\mathbf{a}_2, \dots, \mathbf{e}\mathbf{a}_v\}, \quad (\text{A.2})$$

where \mathbf{A}_1 has h independent columns with $\mathbf{A}_1 \subset \mathbf{F}_{qh}$ and $\{\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_v\} \subset \mathbf{F}_{qh}$.

For \mathbf{E} in the case (B1), if $\#\mathbf{E} = 0$, then $\#\mathbf{A} = 2^k$ and (A.1) holds. In the following, we consider only $1 \leq \#\mathbf{E} \leq 2^{k-1} - 1$. Up to isomorphism, there are three cases for the columns in \mathbf{E} :

- (C1) all the columns are from \mathbf{H}_{h-1} ;
- (C2) some columns are from \mathbf{H}_{h-1} and the others are from $\mathbf{H}_h \setminus \mathbf{H}_{h-1}$;
- (C3) some columns are from \mathbf{H}_{h-1} , some are from $\mathbf{H}_h \setminus \mathbf{H}_{h-1}$ and the others are from $\mathbf{H}_q \setminus \mathbf{H}_h$.

We first consider the case (C2) with $h > k$. Note that $\mathbf{A} \cup \mathbf{A} \otimes \mathbf{E} = \mathbf{A} \otimes (\{\mathbf{I}_N\} \cup \mathbf{E})$. Denote $\mathbf{B} = \{\mathbf{I}_N\} \cup \mathbf{E}$. Then \mathbf{B} can be represented as

$$\mathbf{B} = \mathbf{B}_1 \cup \{\mathbf{e}\mathbf{b}_1, \mathbf{e}\mathbf{b}_2, \dots, \mathbf{e}\mathbf{b}_w\}, \quad (\text{A.3})$$

where $\mathbf{I}_N \in \mathbf{B}_1$, $\mathbf{B}_1 \setminus \{\mathbf{I}_N\} \subset \mathbf{H}_{h-1}$ and $\{\mathbf{b}_1, \dots, \mathbf{b}_w\} \subset \mathbf{H}_{h-1}$.

Recall that $2^{k-1} < \#\mathbf{A} \leq 2^k - 1 < 2^{h-1}$, we can always find a column $\mathbf{r} \in \mathbf{H}_{h-1}$ or $\mathbf{r} = \mathbf{I}_N$ such that at least one column in $\{\mathbf{e}\mathbf{a}_1, \mathbf{e}\mathbf{a}_2, \dots, \mathbf{e}\mathbf{a}_v\}$, say $\mathbf{e}\mathbf{a}_1$, satisfies $(\mathbf{r}\mathbf{e})(\mathbf{e}\mathbf{a}_1) = \mathbf{r}\mathbf{a}_1 \in \mathbf{F}_{qh} \setminus \mathbf{A}_1$. Without loss of generality, we assume that there is some $t_1 (1 \leq t_1 \leq v)$ such that $\mathbf{r}\mathbf{e}\{\mathbf{e}\mathbf{a}_1, \dots, \mathbf{e}\mathbf{a}_{t_1}\} \subset \mathbf{F}_{qh} \setminus \mathbf{A}_1$ and $\mathbf{r}\mathbf{e}\{\mathbf{e}\mathbf{a}_{t_1+1}, \dots, \mathbf{e}\mathbf{a}_v\} \subset \mathbf{A}_1$. Meanwhile, there is some $t_2 (0 \leq t_2 \leq w)$ such that $\mathbf{r}\mathbf{e}\{\mathbf{e}\mathbf{b}_1, \dots, \mathbf{e}\mathbf{b}_{t_2}\} \subset \mathbf{H}_{h-1} \setminus \mathbf{B}_1$ and $\mathbf{r}\mathbf{e}\{\mathbf{e}\mathbf{b}_{t_2+1}, \dots, \mathbf{e}\mathbf{b}_w\} \subset \mathbf{B}_1$.

Let $\mathbf{A}_2 = \{\mathbf{e}\mathbf{a}_{t_1+1}, \dots, \mathbf{e}\mathbf{a}_v\}$ and $\mathbf{A}_3 = \{\mathbf{e}\mathbf{a}_1, \dots, \mathbf{e}\mathbf{a}_{t_1}\}$. Then,

$$\mathbf{A} = \mathbf{A}_1 \cup \mathbf{A}_2 \cup \mathbf{A}_3. \quad (\text{A.4})$$

Let $\mathbf{B}_2 = \{\mathbf{e}\mathbf{b}_{t_2+1}, \dots, \mathbf{e}\mathbf{b}_w\}$ and $\mathbf{B}_3 = \{\mathbf{e}\mathbf{b}_1, \dots, \mathbf{e}\mathbf{b}_{t_2}\}$. Then,

$$\mathbf{B} = \mathbf{B}_1 \cup \mathbf{B}_2 \cup \mathbf{B}_3. \quad (\text{A.5})$$

Let

$$\mathbf{A}^* = \mathbf{A}_1 \cup \mathbf{A}_2 \cup \mathbf{A}_3^* \quad (\text{A.6})$$

and

$$\mathbf{B}^* = \mathbf{B}_1 \cup \mathbf{B}_2 \cup \mathbf{B}_3^*, \quad (\text{A.7})$$

where $\mathbf{A}_3^* = \mathbf{r}\mathbf{e}\mathbf{A}_3$ and $\mathbf{B}_3^* = \mathbf{r}\mathbf{e}\mathbf{B}_3$.

Lemma A.2. Suppose \mathbf{A} , \mathbf{B} , \mathbf{A}^* and \mathbf{B}^* are defined as in (A.4)–(A.7), respectively, then $\#\{\mathbf{A}^* \otimes \mathbf{B}^*\} \leq \#\{\mathbf{A} \otimes \mathbf{B}\}$.

Proof. Let

$$\begin{aligned} \mathbf{Q}_1 &= (\mathbf{A}_1 \otimes \mathbf{B}_2) \cup (\mathbf{A}_2 \otimes \mathbf{B}_1), \\ \mathbf{Q}_2 &= (\mathbf{A}_1 \otimes \mathbf{B}_1) \cup (\mathbf{A}_3 \otimes \mathbf{B}_3), \end{aligned}$$

$$\begin{aligned}
Q_3 &= (A_1 \otimes B_3) \cup (A_3 \otimes B_1), \\
Q_4 &= (A_2 \otimes B_3) \cup (A_3 \otimes B_2), \\
Q_3^* &= (A_3^* \otimes B_2) \cup (A_2 \otimes B_3^*), \\
Q_4^* &= (A_1 \otimes B_3^*) \cup (A_3^* \otimes B_1).
\end{aligned}$$

Since $reA_2 \subset A_1$ and $reB_2 \subset B_1$, we have $A_2 \otimes B_2 \subset Q_2$. Thus

$$\begin{aligned}
A \otimes B &= Q_1 \cup Q_2 \cup (A_2 \otimes B_2) \cup Q_3 \cup Q_4 \\
&= Q_1 \cup Q_2 \cup Q_3 \cup Q_4.
\end{aligned}$$

Since $Q_1 \cup Q_3 \subset F_{q(h+1)} \setminus F_{qh}$ and $Q_2 \cup Q_4 \subset F_{qh}$ are mutually exclusive, thus

$$\begin{aligned}
\#\{A \otimes B\} &= \#\{Q_1 \cup Q_3\} + \#\{Q_2 \cup Q_4\} \\
&= \#Q_1 + \#Q_2 + \#Q_3 + \#Q_4 - \#\{Q_1 \cap Q_3\} - \#\{Q_2 \cap Q_4\}.
\end{aligned}$$

Note that $A_3^* \otimes B_3^* = A_3 \otimes B_3$, then

$$A^* \otimes B^* = Q_1 \cup Q_2 \cup (A_2 \otimes B_2) \cup Q_3^* \cup Q_4^* = Q_1 \cup Q_2 \cup Q_3^* \cup Q_4^*.$$

Since $Q_1 \cup Q_3^* \subset F_{q(h+1)} \setminus F_{qh}$ and $Q_2 \cup Q_4^* \subset F_{qh}$ are mutually exclusive, thus

$$\begin{aligned}
\#\{A^* \otimes B^*\} &= \#\{Q_1 \cup Q_3^*\} + \#\{Q_2 \cup Q_4^*\} \\
&= \#Q_1 + \#Q_2 + \#Q_3^* + \#Q_4^* - \#\{Q_1 \cap Q_3^*\} - \#\{Q_2 \cap Q_4^*\} \\
&= \#Q_1 + \#Q_2 + \#Q_3 + \#Q_4 - \#\{Q_1 \cap Q_3^*\} - \#\{Q_2 \cap Q_4^*\},
\end{aligned}$$

where the third equality is due to $reQ_3^* = Q_4$ and $reQ_4^* = Q_3$. Therefore, to prove Lemma A.2, it suffices to prove

$$\#\{Q_1 \cap Q_3^*\} + \#\{Q_2 \cap Q_4^*\} \geq \#\{Q_1 \cap Q_3\} + \#\{Q_2 \cap Q_4\}$$

or equivalently

$$\#\{Q_2 \cap Q_4^*\} - \#\{Q_2 \cap Q_4\} \geq \#\{Q_1 \cap Q_3\} - \#\{Q_1 \cap Q_3^*\}. \quad (\text{A.8})$$

Note that $A_2 \subset reA_1$ and $B_2 \subset reB_1$, then

$$A_2 \otimes B_3 \subset (reA_1) \otimes B_3 = A_1 \otimes B_3^*$$

and

$$A_3 \otimes B_2 \subset A_3 \otimes (reB_1) = (reA_3) \otimes B_1 = A_3^* \otimes B_1$$

which implies that $Q_4 \subset Q_3^*$. Similarly, we can obtain $Q_3^* \subset Q_3$. Therefore, (A.8) is equivalent to

$$\#\{(Q_2 \cap Q_4^*) \setminus (Q_2 \cap Q_4)\} \geq \#\{(Q_1 \cap Q_3) \setminus (Q_1 \cap Q_3^*)\}. \quad (\text{A.9})$$

Thus, we only need to prove (A.9).

For the left hand side of (A.9), we have

$$\#\{(Q_2 \cap Q_4^*) \setminus (Q_2 \cap Q_4)\} = \#\{Q_2 \cap (Q_4^* \setminus Q_4)\}.$$

For the right hand side of (A.9), we have

$$\begin{aligned}\#\{(\mathbf{Q}_1 \cap \mathbf{Q}_3) \setminus (\mathbf{Q}_1 \cap \mathbf{Q}_3^*)\} &= \#\{\mathbf{Q}_1 \cap (\mathbf{Q}_3 \setminus \mathbf{Q}_3^*)\} \\ &= \#\{(\mathbf{reQ}_1) \cap (\mathbf{reQ}_3 \setminus \mathbf{reQ}_3^*)\} \\ &= \#\{(\mathbf{reQ}_1) \cap (\mathbf{Q}_4^* \setminus \mathbf{Q}_4)\}.\end{aligned}$$

Since $\mathbf{reQ}_1 = (\mathbf{A}_1 \otimes (\mathbf{reB}_2)) \cup ((\mathbf{reA}_2) \otimes \mathbf{B}_1) \subset \mathbf{A}_1 \otimes \mathbf{B}_1$, we have $\mathbf{reQ}_1 \subset \mathbf{Q}_2$. Then (A.9) holds. This completes the proof of Lemma A.2. \square

Remark 1. Lemma A.2 indicates that for any \mathbf{A} defined in (A.2) and \mathbf{B} defined in (A.3), we can always find \mathbf{A}^* , which has less columns out of \mathbf{F}_{qh} than \mathbf{A} , and \mathbf{B}^* , which has no more columns out of \mathbf{H}_{h-1} than \mathbf{B} , such that $\#\{\mathbf{A}^* \otimes \mathbf{B}^*\} \leq \#\{\mathbf{A} \otimes \mathbf{B}\}$. Repeatedly applying Lemma A.2, we can finally find $\mathbf{A}^{**} \subset \mathbf{F}_{qh}$ and \mathbf{B}^{**} , which has no more columns out of \mathbf{H}_{h-1} than \mathbf{B} , such that $\#\{\mathbf{A}^{**} \otimes \mathbf{B}^{**}\} \leq \#\{\mathbf{A} \otimes \mathbf{B}\}$.

For simplicity of notation, we still denote \mathbf{A}^{**} as \mathbf{A} and \mathbf{B}^{**} as \mathbf{B} . Then we can assume that $\mathbf{A} \subset \mathbf{F}_{qh}$. Note that there might be $t_2 = 0$ in the procedure above. Then, following Remark 1, \mathbf{B} has the following cases:

(D1) $\mathbf{B} \setminus \{\mathbf{I}_N\} \subset \mathbf{H}_{h-1}$, or
(D2) $(\mathbf{B} \setminus \{\mathbf{I}_N\}) \cap (\mathbf{H}_h \setminus \mathbf{H}_{h-1}) \neq \emptyset$,

For the case (D2), we write \mathbf{B} as $\mathbf{B} = \mathbf{B}_1 \cup \{\mathbf{eb}_1, \dots, \mathbf{eb}_{t_3}\}$, where $\mathbf{I}_N \in \mathbf{B}_1$, $\mathbf{B}_1 \setminus \{\mathbf{I}_N\} \subset \mathbf{H}_{h-1}$ and $\{\mathbf{b}_1, \dots, \mathbf{b}_{t_3}\} \subset \mathbf{H}_{h-1}$. Note that $1 \leq \#(\mathbf{B} \setminus \{\mathbf{I}_N\}) \leq 2^{k-1} - 1 < 2^{h-1} - 1$. We can always find a column $\mathbf{r}_1 \in \mathbf{H}_{h-1}$ or $\mathbf{r}_1 = \mathbf{I}_N$ such that at least one column in $\{\mathbf{eb}_1, \dots, \mathbf{eb}_{t_3}\}$, say \mathbf{eb}_1 , satisfies $(\mathbf{r}_1 \mathbf{e})(\mathbf{eb}_1) = \mathbf{r}_1 \mathbf{b}_1 \in \mathbf{H}_{h-1} \setminus \mathbf{B}_1$. Without loss of generality, suppose there is some t_4 with $1 \leq t_4 \leq t_3$ such that $\mathbf{r}_1 \mathbf{e} \{\mathbf{eb}_1, \dots, \mathbf{eb}_{t_4}\} \subset \mathbf{H}_{h-1} \setminus \mathbf{B}_1$ and $\mathbf{r}_1 \mathbf{e} \{\mathbf{eb}_{t_4+1}, \dots, \mathbf{eb}_{t_3}\} \subset \mathbf{B}_1$. Denote $\mathbf{B}_2 = \{\mathbf{eb}_{t_4+1}, \dots, \mathbf{eb}_{t_3}\}$ and $\mathbf{B}_3 = \{\mathbf{eb}_1, \dots, \mathbf{eb}_{t_4}\}$, then

$$\mathbf{B} = \mathbf{B}_1 \cup \mathbf{B}_2 \cup \mathbf{B}_3. \quad (\text{A.10})$$

Denote

$$\mathbf{B}^* = \mathbf{B}_1 \cup \mathbf{B}_2 \cup \mathbf{B}_3^*, \quad (\text{A.11})$$

where $\mathbf{B}_3^* = \mathbf{r}_1 \mathbf{e} \mathbf{B}_3$.

Lemma A.3. Suppose $\mathbf{A} \subset \mathbf{F}_{qh}$, \mathbf{B} and \mathbf{B}^* are defined as in (A.10) and (A.11), respectively, then $\#\{\mathbf{A} \otimes \mathbf{B}^*\} \leq \#\{\mathbf{A} \otimes \mathbf{B}\}$.

Proof. Note that $\mathbf{A} \otimes \mathbf{B}_1 \subset \mathbf{F}_{qh}$ and $(\mathbf{A} \otimes \mathbf{B}_2) \cup (\mathbf{A} \otimes \mathbf{B}_3) \subset \mathbf{F}_{q(h+1)} \setminus \mathbf{F}_{qh}$. Therefore,

$$\begin{aligned}\#\{\mathbf{A} \otimes \mathbf{B}\} &= \#\{\mathbf{A} \otimes \mathbf{B}_1\} + \#\{(\mathbf{A} \otimes \mathbf{B}_2) \cup (\mathbf{A} \otimes \mathbf{B}_3)\} \\ &= \#\{\mathbf{A} \otimes \mathbf{B}_1\} + \#\{\mathbf{A} \otimes \mathbf{B}_2\} + \#\{\mathbf{A} \otimes \mathbf{B}_3\} - \#\{(\mathbf{A} \otimes \mathbf{B}_2) \cap (\mathbf{A} \otimes \mathbf{B}_3)\}.\end{aligned}$$

Since $(\mathbf{A} \otimes \mathbf{B}_1) \cup (\mathbf{A} \otimes \mathbf{B}_3^*) \subset \mathbf{F}_{qh}$ and $\mathbf{A} \otimes \mathbf{B}_2 \subset \mathbf{F}_{q(h+1)} \setminus \mathbf{F}_{qh}$, we have

$$\begin{aligned}\#\{\mathbf{A} \otimes \mathbf{B}^*\} &= \#\{(\mathbf{A} \otimes \mathbf{B}_1) \cup (\mathbf{A} \otimes \mathbf{B}_3^*)\} + \#\{\mathbf{A} \otimes \mathbf{B}_2\} \\ &= \#\{\mathbf{A} \otimes \mathbf{B}_1\} + \#\{\mathbf{A} \otimes \mathbf{B}_2\} + \#\{\mathbf{A} \otimes \mathbf{B}_3^*\} - \#\{(\mathbf{A} \otimes \mathbf{B}_1) \cap (\mathbf{A} \otimes \mathbf{B}_3^*)\} \\ &= \#\{\mathbf{A} \otimes \mathbf{B}_1\} + \#\{\mathbf{A} \otimes \mathbf{B}_2\} + \#\{\mathbf{A} \otimes \mathbf{B}_3\} - \#\{(\mathbf{A} \otimes \mathbf{B}_1) \cap (\mathbf{A} \otimes \mathbf{B}_3^*)\},\end{aligned}$$

where the third equality is due to $\mathbf{r}_1\mathbf{e}(\mathbf{A} \otimes \mathbf{B}_3^*) = \mathbf{A} \otimes \mathbf{B}_3$. On one hand,

$$\begin{aligned}\#\{(\mathbf{A} \otimes \mathbf{B}_1) \cap (\mathbf{A} \otimes \mathbf{B}_3^*)\} &= \#\{\mathbf{r}_1\mathbf{e}((\mathbf{A} \otimes \mathbf{B}_1) \cap (\mathbf{A} \otimes \mathbf{B}_3^*))\} \\ &= \#\{(\mathbf{A} \otimes (\mathbf{r}_1\mathbf{e}\mathbf{B}_1)) \cap (\mathbf{A} \otimes \mathbf{B}_3)\}.\end{aligned}\quad (\text{A.12})$$

On the other hand, $\mathbf{B}_2 \subset \mathbf{r}_1\mathbf{e}\mathbf{B}_1$, which leads to

$$(\mathbf{A} \otimes \mathbf{B}_2) \cap (\mathbf{A} \otimes \mathbf{B}_3) \subset (\mathbf{A} \otimes (\mathbf{r}_1\mathbf{e}\mathbf{B}_1)) \cap (\mathbf{A} \otimes \mathbf{B}_3). \quad (\text{A.13})$$

From (A.12) and (A.13), we obtain that

$$\#\{(\mathbf{A} \otimes \mathbf{B}_1) \cap (\mathbf{A} \otimes \mathbf{B}_3^*)\} \geq \#\{(\mathbf{A} \otimes \mathbf{B}_2) \cap (\mathbf{A} \otimes \mathbf{B}_3)\}.$$

This implies $\#\{\mathbf{A} \otimes \mathbf{B}^*\} \leq \#\{\mathbf{A} \otimes \mathbf{B}\}$ and completes the proof. \square

Remark 2. By repeatedly applying Lemma A.3, we can finally find $\mathbf{B}^* \subset \mathbf{H}_{h-1}$ such that $\#\{\mathbf{A} \otimes \mathbf{B}^*\} \leq \#\{\mathbf{A} \otimes \mathbf{B}\}$. This result is also true for the cases (C1) and (C3) with $h > k$ due to the following reasons. When $\{\mathbf{e}\mathbf{a}_1, \mathbf{e}\mathbf{a}_2, \dots, \mathbf{e}\mathbf{a}_v\} = \emptyset$, the case (C2) reduce to the case (C1). For the case (C3), with a similar argument to Lemma A.3, we can find a \mathbf{T} with $\mathbf{I}_N \subset \mathbf{T}$ and $(\mathbf{T} \setminus \mathbf{I}_N) \subset \mathbf{H}_h$ such that $\#\{\mathbf{A} \otimes \mathbf{T}\} \leq \#\{\mathbf{A} \otimes \mathbf{B}\}$. Then the case (C3) reduces to case (C2).

The following remark considers the case of $h = k$.

Remark 3. For $h = k$, up to isomorphism, $\mathbf{A} \subset \mathbf{F}_{q(k+1)}$. In this situation, h should equal to k in the cases (C1), (C2) and (C3). Especially, in the cases (C1) and (C2), \mathbf{E} is already a subset of \mathbf{H}_k . By repeatedly applying Lemma A.3 to \mathbf{E} in the case (C3), we can find a set, say \mathbf{P} , such that $\mathbf{P} \subset \mathbf{H}_k$ and $\#\{\mathbf{A} \otimes (\{\mathbf{I}_N\} \cup \mathbf{P})\} \leq \#\{\mathbf{A} \otimes (\{\mathbf{I}_N\} \cup \mathbf{E})\}$.

In summary, for any \mathbf{A} and \mathbf{B} defined in (A.2) and (A.3), by repeatedly applying Lemmas A.2 and A.3, we can always find $\mathbf{A}^* \subset \mathbf{F}_{q(k+1)}$ and $\mathbf{B}^* \setminus \{\mathbf{I}_N\} \subset \mathbf{H}_k$ with $\mathbf{I}_N \in \mathbf{B}^*$, such that $\#\{\mathbf{A}^* \otimes \mathbf{B}^*\} \leq \#\{\mathbf{A} \otimes \mathbf{B}\}$. Next, we denote \mathbf{A}^* as \mathbf{A} and \mathbf{B}^* as \mathbf{B} and prove that $\#\{\mathbf{A} \otimes \mathbf{B}\} = 2^k$ for any $\mathbf{A} \subset \mathbf{F}_{q(k+1)}$, $\mathbf{B} \setminus \{\mathbf{I}_N\} \subset \mathbf{H}_k$ with $\mathbf{I}_N \in \mathbf{B}$ and $\#\mathbf{A} + \#\mathbf{B} = 2^k$. We first introduce a useful lemma from [24].

Denote I_S as the set consisting of the distinct columns generated by taking component-wise products of any two columns of \mathbf{S} .

Lemma A.4. Let \mathbf{S} be an s -subset of \mathbf{F}_{qq} , $s = 2^{k-1} + \delta \geq 3$ and $0 < \delta \leq 2^{k-1}$, then $\#I_S \geq 2^k - 1$, where the equality holds when the number of independent columns of \mathbf{S} is $k + 1$.

Lemma A.5. Suppose $\mathbf{A} \subset \mathbf{F}_{q(k+1)}$, $\mathbf{I}_N \in \mathbf{B}$, $\mathbf{B} \setminus \mathbf{I}_N \subset \mathbf{H}_k$ with $\#\mathbf{A} + \#\mathbf{B} = 2^k + 1$ and $k \leq q - 2$, then $\#\{\mathbf{A} \otimes \mathbf{B}\} = 2^k$.

Proof. Without loss of generality, suppose \mathbf{e} is the $(k + 1)$ th independent column in \mathbf{H}_q . Then $\#\{\mathbf{A} \otimes \mathbf{B}\} = \#\{\mathbf{A} \otimes (\mathbf{e}\mathbf{q}\mathbf{B})\}$ and $\mathbf{e}\mathbf{q}\mathbf{B} \subset \mathbf{F}_{q(k+2)} \setminus \mathbf{F}_{q(k+1)}$. Next, we show $\#\{\mathbf{A} \otimes (\mathbf{e}\mathbf{q}\mathbf{B})\} = 2^k$. Since $\mathbf{A} \cap \mathbf{e}\mathbf{q}\mathbf{B} = \emptyset$, we have $\#\{\mathbf{A} \cup \mathbf{e}\mathbf{q}\mathbf{B}\} = \#\mathbf{A} + \#\{\mathbf{e}\mathbf{q}\mathbf{B}\} = 2^k + 1$ and $\mathbf{A} \cup \mathbf{e}\mathbf{q}\mathbf{B}$ has $k + 2$ independent columns. By Lemma A.4, we have

$$\#I_{\mathbf{A} \cup \mathbf{e}\mathbf{q}\mathbf{B}} = \#\{I_{\mathbf{A}} \cup I_{\mathbf{e}\mathbf{q}\mathbf{B}} \cup (\mathbf{A} \otimes (\mathbf{e}\mathbf{q}\mathbf{B}))\} = 2^{k+1} - 1. \quad (\text{A.14})$$

Note that $I_{\mathbf{A}} \cup I_{\mathbf{e}\mathbf{q}\mathbf{B}} \subset \mathbf{H}_k$ then $\#\{I_{\mathbf{A}} \cup I_{\mathbf{e}\mathbf{q}\mathbf{B}}\} \leq 2^k - 1$, and $\mathbf{A} \otimes (\mathbf{e}\mathbf{q}\mathbf{B}) \subset \mathbf{H}_{k+1} \setminus \mathbf{H}_k$ then $\#\{\mathbf{A} \otimes (\mathbf{e}\mathbf{q}\mathbf{B})\} \leq 2^k$. From (A.14), there should be $\#\{I_{\mathbf{A}} \cup I_{\mathbf{e}\mathbf{q}\mathbf{B}}\} = 2^k - 1$ and $\#\{\mathbf{A} \otimes (\mathbf{e}\mathbf{q}\mathbf{B})\} = 2^k$. This completes the proof. \square

Proof of Lemma 1. According to the proofs of Lemmas A.2, A.3 and A.5, we can immediately obtain that $\#\{U(\mathbf{D}_b) \cap \mathbf{F}_{qq}\} \geq 2^k$. This completes the proof. \square



AIMS Press

© 2021 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0>)