Supplement to

A THEORY ON CONSTRUCTING 2^{n-m} DESIGNS WITH GENERAL MINIMUM LOWER ORDER CONFOUNDING

Pengfei Li[1], Shengli Zhao[2] and Runchu Zhang[*,3,4]

[1] *University of Alberta,* [2] *Qufu Normal University,*
[3] *Northeast Normal University and* [4] *Nankai University*

Appendix: Proof of Theorem 1

The global line of proving the theorem is that, firstly we prove Part (a) and then use the result of Part (a) to prove Part (b), finally use the result of Part (b) to prove Part (c).

For convenience of presentation below, we introduce the notation $Q_1 \times Q_2 = \{d_1d_2 : d_1 \in Q_1, d_2 \in Q_2\}$, where $Q_1, Q_2 \subset H_q$. Particularly, denote $dQ = \{d\} \times Q$ for $d \in H_q$ and $Q \subset H_q$.

Proof of Part (a)

Note that, when $r = q$, Part (a) of the theorem is obviously valid, since any design S with s factors from H_q, satisfying $2^{q-1} \le s \le 2^q - 1$, has exactly q independent factors and $S \subset H_q$. So, we only need to consider the case $r \le q - 1$.

Suppose that $S_1 \subset H_q$ is a design with s factors, where $2^{r-1} \le s \le 2^r - 1$ for some $r \le q-1$, and has $h+1$ ($r \le h \le q-1$) independent factors. Let a denote the factor q. Under isomorphism, we can assume $a \in S_1$ and S_1 can be represented as

$$S_1 = Q \cup \{a, ab_1, ab_2, \ldots, ab_l\}, \tag{1}$$

where Q is a subset of H_h and has h independent factors, and $\{b_1, \ldots, b_l\} \subset H_h$. Without loss of generality, we assume that $\{b_1, \ldots, b_t\} \subset Q$ and $\{b_{t+1}, \ldots, b_l\} \subset H_h \backslash Q$, and consider another set

$$S_2 = Q \cup \{a, ab_1, \ldots, ab_t\} \cup \{b_{t+1}, \ldots, b_l\}. \tag{2}$$

We have the following lemma.

Lemma 6. *Suppose that S_1 and S_2 are defined in (1) and (2) respectively, then $\bar{g}(S_2) \le \bar{g}(S_1)$.*

Proof. Denote $Q_1 = \{a, ab_1, ab_2, \ldots, ab_t\}$ and $Q_2 = \{ab_{t+1}, \ldots, ab_l\}$. Then we have $S_1 = Q \cup Q_1 \cup Q_2$ and $S_2 = Q \cup Q_1 \cup aQ_2$. Let $P = H_q \backslash (S_1 \cup S_2)$, where $S_1 \cup S_2 = Q \cup Q_1 \cup Q_2 \cup aQ_2$ in which the four sets are mutually exclusive. According to the definitions of $\bar{g}(S_1)$ and $\bar{g}(S_2)$, we get

$$\bar{g}(S_1) = \#\{\gamma : \gamma \in P, B_2(S_1, \gamma) > 0\} + \#\{\gamma : \gamma \in aQ_2, B_2(S_1, \gamma) > 0\} \stackrel{\triangle}{=} g_{11} + g_{12}$$

[*] Corresponding author, Emails: zhrch@nankai.edu.cn, rczhang@nenu.edu.cn.

and

$$\bar{g}(S_2) = \#\{\gamma : \gamma \in P, B_2(S_2,\gamma) > 0\} + \#\{\gamma : \gamma \in Q_2, B_2(S_2,\gamma) > 0\} \overset{\triangle}{=} g_{21} + g_{22}.$$

For any $\gamma \in Q_2$, $\gamma = a(a\gamma)$, where $a \in Q_1 \subset S_2$ and $a\gamma \in aQ_2 \subset S_2$, we have $B_2(S_2,\gamma) > 0$. From the definition of g_{22}, we get $g_{22} = \#\{Q_2\}$. Similarly, $g_{12} = \#\{aQ_2\}$ follows. We can check that $\#\{Q_2\} = \#\{aQ_2\}$, which leads to $g_{12} = g_{22}$.

Now we pick-up the three sets:

$$\begin{aligned}
P_1 &= \{\gamma : \gamma \in P, B_2(S_1,\gamma) > 0 \text{ and } B_2(S_2,\gamma) > 0\},\\
P_2 &= \{\gamma : \gamma \in P, B_2(S_1,\gamma) > 0 \text{ and } B_2(S_2,\gamma) = 0\},\\
P_3 &= \{\gamma : \gamma \in P, B_2(S_1,\gamma) = 0 \text{ and } B_2(S_2,\gamma) > 0\}.
\end{aligned}$$

Then, P_1, P_2 and P_3 are mutually exclusive and we have $g_{11} = \#\{P_1\} + \#\{P_2\}$ and $g_{21} = \#\{P_1\} + \#\{P_3\}$. So, to finish the proof, it suffices to show the result $\#\{P_2\} \geq \#\{P_3\}$ or a stronger result: if $\gamma \in P_3$ then $a\gamma \in P_2$.

To do this, we note that, if $\gamma \in P_3$, then γ must not be an interaction of any two factors in $Q \cup Q_1 \cup Q_2$ but an interaction of some two factors in $Q \cup Q_1 \cup aQ_2$. Therefore, γ must be an interaction of two factors with one coming from aQ_2 and the other coming from Q or Q_1. If $\gamma \in aQ_2 \times Q_1 = Q_2 \times aQ_1 \subset Q_2 \cup (Q_2 \times Q)$ or $\gamma \in aQ_2 \times \{b_1,\ldots,b_t\} = Q_2 \times \{ab_1,\ldots,ab_t\} \subset Q_2 \times Q_1$, where $\{b_1,\ldots,b_t\} \subset Q$, then $\gamma \notin P$ or $B_2(S_1,\gamma) > 0$, which contradicts the assumption $\gamma \in P_3$. So, we must have $\gamma \in aQ_2 \times (Q\backslash\{b_1,\ldots,b_t\}) \subset H_h$. Because of this, we get $a\gamma \in Q_2 \times (Q\backslash\{b_1,\ldots,b_t\})$, which implies $B_2(S_1,a\gamma) > 0$. The remainder is to prove that, for the $a\gamma$, we have $a\gamma \in P$ and $B_2(S_2,a\gamma) = 0$. For the former, it is easy to be validated. We only show $B_2(S_2,a\gamma) = 0$ below.

We use the reduction to absurdity to prove the point. Suppose $B_2(S_2,a\gamma) > 0$. Since $\gamma \in H_h$, we have $a\gamma \in aH_h$ and $a\gamma \in Q_1 \times (Q \cup aQ_2)$. Thus, there are only the following two possibilities: $a\gamma \in Q_1 \times Q$ or $a\gamma \in Q_1 \times aQ_2$. However, if $a\gamma \in Q_1 \times Q$, then $\gamma \in aQ_1 \times Q \subset Q \cup (Q \times Q)$, or if $a\gamma \in Q_1 \times aQ_2$, then $\gamma \in Q_1 \times Q_2$. Any one of the two cases implies that $\gamma \notin P$ or $B_2(S_1,\gamma) > 0$, which contradicts the assumption $\gamma \in P_3$. Lemma 6 is proved. $\square$

Lemma 6 indicates that, if the design S_1 is transformed into the design S_2, i.e. the elements $ab_{t+1},\ldots,ab_l$ in S_1, which are out of H_h, are substituted by the elements $b_{t+1},\ldots,b_l$, which are in H_h, then $\bar{g}(S_2) \leq \bar{g}(S_1)$.

In the following study, we join Q and aQ_2 together and still denote it by Q. Without loss of generality, we assume that S_2 has the form

$$S_2 = Q \cup \{a, ab_1,\ldots,ab_t\}, \tag{3}$$

where $Q \subset H_h$ and has h independent factors, and $\{b_1,\ldots,b_t\} \subset Q$. When $2^{r-1} \leq s \leq 2^r - 1$, the number of factors in Q is smaller than $2^r - 1$. Therefore there are at least two factors c_1 and c_2 in Q such that $c = c_1c_2 \notin Q$. Under isomorphism, we can assume that there is some t_0

such that

$$\{c, cb_1, cb_2, \ldots, cb_{t_0}\} \subset H_h \backslash Q \text{ and } \{cb_{t_0+1}, \ldots, cb_t\} \subset Q.$$

Denote

$$S_3 = Q \cup \{c, cb_1, cb_2, \ldots, cb_{t_0}\} \cup \{ab_{t_0+1}, \ldots, ab_t\}. \tag{4}$$

We have one more result as follows.

Lemma 7. *Suppose that S_2 and S_3 are defined in (3) and (4) respectively. Then $\bar{g}(S_3) \le \bar{g}(S_2)$. Especially, if $t_0 = t$ the strict inequality $\bar{g}(S_3) < \bar{g}(S_2)$ is valid.*

Proof. Let $Q_1 = \{a, ab_1, ab_2, \ldots, ab_{t_0}\}$ and $Q_2 = \{ab_{t_0+1}, \ldots, ab_t\}$. Then $S_2 = Q \cup Q_1 \cup Q_2$ and $S_3 = Q \cup acQ_1 \cup Q_2$. Also denote $P = H_q \backslash (S_2 \cup S_3)$, where $S_2 \cup S_3 = Q \cup Q_1 \cup acQ_1 \cup Q_2$ in which the four parts are mutually exclusive. According to the definitions of $\bar{g}(S_2)$ and $\bar{g}(S_3)$, we have

$$\bar{g}(S_2) = \#\{\gamma : \gamma \in P, B_2(S_2, \gamma) > 0\} + \#\{\gamma : \gamma \in acQ_1, B_2(S_2, \gamma) > 0\} \stackrel{\triangle}{=} g_{21} + g_{22}$$

and

$$\bar{g}(S_3) = \#\{\gamma : \gamma \in P, B_2(S_3, \gamma) > 0\} + \#\{\gamma : \gamma \in Q_1, B_2(S_3, \gamma) > 0\} \stackrel{\triangle}{=} g_{31} + g_{32}.$$

Now let

$$\begin{aligned}
P_1 &= \{\gamma : \gamma \in P, B_2(S_2, \gamma) > 0 \text{ and } B_2(S_3, \gamma) > 0\}, \\
P_2 &= \{\gamma : \gamma \in P, B_2(S_2, \gamma) > 0 \text{ and } B_2(S_3, \gamma) = 0\}, \\
P_3 &= \{\gamma : \gamma \in P, B_2(S_2, \gamma) = 0 \text{ and } B_2(S_3, \gamma) > 0\}.
\end{aligned}$$

Then, P_1, P_2 and P_3 are mutually exclusive, $g_{21} = \#\{P_1\} + \#\{P_2\}$, and $g_{31} = \#\{P_1\} + \#\{P_3\}$.

If $t_0 = t$, then $Q_2 = \emptyset$, the empty set, and $S_3 \subset H_h$. As a result, for any $\gamma \in Q_1$, we have $B_2(S_3, \gamma) = 0$ and hence $g_{32} = 0$. On the other hand, because there is $c \in acQ_1$ such that $B_2(S_2, c) > 0$, it leads to $g_{22} \ge 1$. Thus, to prove $\bar{g}(S_3) < \bar{g}(S_2)$, it suffices to show that $\#\{P_2\} \ge \#\{P_3\}$ or a stronger result: if $\gamma \in P_3$ then $ac\gamma \in P_2$. By the same argument as in proving Lemma 6, we can show that if $\gamma \in P_3$ then $\gamma \in acQ_1 \times Q \subset H_h$. From this, it directly follows that $ac\gamma \in Q_1 \times Q$, then we can verify $B_2(S_2, ac\gamma) > 0$ and $ac\gamma \in P$. Note that, $B_2(S_3, ac\gamma) = 0$ is straightforward since $S_3 \subset H_h$ and $ac\gamma \notin H_h$. In this way, the second half result of Lemma 7 follows.

In the following let us consider the case $t_0 < t$. Actually the proof for this case is very similar to that for $t_0 = t$. It only needs one more condition $acQ_2 \subset Q$, however it is just a simple fact from the definition of S_3.

To make it clear, let us take two steps. Firstly, we show the fact: for any $\gamma \in Q_1$, if $B_2(S_3, \gamma) > 0$ then $B_2(S_2, ac\gamma) > 0$ and hence $g_{32} \le g_{22}$.

Note that, if $\gamma \in Q_1$ and $B_2(S_3, \gamma) > 0$, then $\gamma \in Q_2 \times (Q \cup acQ_1)$. Based on this, the above fact immediately follows, since we have that, if $\gamma \in Q_2 \times Q$ then $ac\gamma \in acQ_2 \times Q \subset Q \times Q$, or if $\gamma \in Q_2 \times acQ_1$ then $ac\gamma \in Q_2 \times Q_1$, both lead to $B_2(S_2, ac\gamma) > 0$.

Next, let us show the fact: for any $\gamma \in P_3$, then $ac\gamma \in P_2$ and hence $g_{31} \leq g_{21}$.

Again, note that for any $\gamma \in P_3$ we have $\gamma \in acQ_1 \times (Q \cup Q_2)$. From this, we can first conclude $\gamma \notin acQ_1 \times Q_2 = Q_1 \times acQ_2 \subset Q_1 \times Q$, it is because if not then $B_2(S_2, \gamma) > 0$, but under given $\gamma \in P_3$ it is impossible. So, we must have $\gamma \in acQ_1 \times Q \subset H_h$. On the other hand, we can validate $ac\gamma \in P$ and $ac\gamma \in Q_1 \times Q$, or more precisely, $B_2(S_2, ac\gamma) > 0$. Therefore, it is sufficient to show $B_2(S_3, ac\gamma) = 0$.

We use the reduction to absurdity to prove the point above. Suppose $B_2(S_3, ac\gamma) > 0$. Since $\gamma \in H_h$ and $ac\gamma \in P$, we have $ac\gamma \in aH_h$ and $ac\gamma \in Q_2 \times (Q \cup acQ_1)$, which yields $ac\gamma \in Q_2 \times Q$ or $ac\gamma \in Q_2 \times acQ_1$. However, if $ac\gamma \in Q_2 \times Q$ then $\gamma \in acQ_2 \times Q \subset Q \times Q$, or if $ac\gamma \in Q_2 \times acQ_1$ then $\gamma \in Q_2 \times Q_1$. Both cases lead to $B_2(S_2, \gamma) > 0$, contradicting the assumption $\gamma \in P_3$.

From the above two steps, the two inequalities $g_{31} \leq g_{21}$ and $g_{32} \leq g_{22}$ are proved and hence we get $\bar{g}(S_3) \leq \bar{g}(S_2)$. □

Lemma 7 tells us that, when we substitute design S_2 by design S_3, i.e. the elements $a, ab_1, \ldots, ab_{t_0}$ in design S_2, which are out of H_h, are substituted by the elements $c, cb_1, \ldots, cb_{t_0}$, which are in H_h, the $\bar{g}(\cdot)$ value will be reduced. Especially, this procedure can continuously go on till that $t_0 = t$, i.e. $S_3 \subset H_h$, then S_3 has h independent factors and $\bar{g}(S_3) < \bar{g}(S_2)$. If $h > r$, applying Lemma 6 to go the procedure in Lemma 6 but the H_{h-1} in this case has one less independent factor than the previous one. We can repeatedly and alternately go through the procedures of Lemmas 6 and 7 till we construct a design $S_3^* \subset H_r$. Then $\bar{g}(S_3^*) < \bar{g}(S_3)$ and S_3^* has exact r independent factors.

Now, let us return to the proof of Part (a) for the case $r \leq q - 1$.

Suppose that S is a design with $2^{r-1} \leq s \leq 2^r - 1$ factors and $\bar{g}(S)$ is minimized. Obviously, the S has at least r independent factors. If the S has $h\,(> r)$ independent factors, just like the statement in the paragraph after the proof of Lemma 7, we can construct a design S^* such that $\bar{g}(S^*) < \bar{g}(S)$ which contradicts the condition that $\bar{g}(S)$ is minimized. Therefore the S exactly has r independent factors. Noting that $S \subset H_r$ is obvious, the proof of Part (a) is then completed.

Proof of Part (b)

To prove Part (b) of Theorem 1, we need two more lemmas in the following.

Suppose that $S_4 \subset H_q$ is a resolution IV or higher design with s factors, where $2^{r-2} + 1 \leq s \leq 2^{r-1}$. With a suitable relabelling, we can assume $a \in S_4$. If S_4 has $h + 1$ $(r \leq h \leq q - 1)$ independent factors, then S_4 has the form

$$S_4 = Q \cup \{a, ab_1, \ldots, ab_t\}, \tag{5}$$

where $Q \subset H_h$ and has h independent factors, and $\{b_1, \ldots, b_t\} \subset H_h$. Since S_4 has resolution at least IV, aQ and $\{a, ab_1, \ldots, ab_t\}$ are mutually exclusive. Let

$$S_5 = aQ \cup \{a, ab_1, \ldots, ab_t\}. \tag{6}$$

Then we have the following result.

Lemma 8. *Suppose that S_4 and S_5 are defined in (5) and (6), respectively. Then $\bar{g}(S_5) \le \bar{g}(S_4)$.*

Proof. Let $Q_1 = \{a, ab_1, \ldots, ab_t\}$, then $S_4 = Q \cup Q_1$ and $S_5 = aQ \cup Q_1$. From $S_5 \subset \{a, aH_h\}$ and the definition of $\bar{g}(S_5)$, we have

$$\bar{g}(S_5) = \#\{\gamma : \gamma \in H_h, B_2(S_5, \gamma) > 0\}.$$

So, by the definition of $\bar{g}(S_4)$, it suffices to prove that, if $\gamma \in H_h$ and $B_2(S_5, \gamma) > 0$, then $B_2(S_4, \gamma) > 0$ and $\gamma \notin S_4$ or $B_2(S_4, a\gamma) > 0$ and $a\gamma \notin S_4$.

Remind that, if $\gamma \in H_h$ and $B_2(S_5, \gamma) > 0$, then we have $\gamma \in aQ \times aQ$, or $\gamma \in Q_1 \times Q_1$, or $\gamma \in aQ \times Q_1$. Since S_4 has resolution at least IV, when $\gamma \in aQ \times aQ\,(= Q \times Q)$ or $\gamma \in Q_1 \times Q_1$, then $B_2(S_4, \gamma) > 0$, which causes $\gamma \notin S_4$, and when $\gamma \in aQ \times Q_1$, then $a\gamma \in Q \times Q_1$ and $B_2(S_4, a\gamma) > 0$, which causes $a\gamma \notin S_4$. □

Lemma 8 tells us that, when we substitute design S_4 by design S_5, i.e., the elements of part Q in design S_4, which is out of $F_{q(h+1)}$, are substituted by the elements aQ, which are in $F_{q(h+1)}$, the $\bar{g}(\cdot)$ value will be reduced.

The following lemma examines the structure of the design that has s factors, resolution IV or higher, and r independent factors, where $2^{r-2} + 1 \le s \le 2^{r-1}$.

Lemma 9. *Let $S \subset H_r$ be a design having s factors and resolution IV or higher with $2^{r-2}+1 \le s \le 2^{r-1}$, in which there are r independent factors. Then, if $A_i(S) > 0$ for some odd number i, it must have that $A_5(S) > 0$.*

Proof. Suppose that i_0 is the smallest odd number such that $A_{i_0}(S) > 0$. Without loss of generality, we assume $b_1 b_2 \cdots b_{i_0} = I$, where $\{b_1, \ldots, b_{i_0}\} \subset S$ and I is the identity element.

Since S has resolution IV or higher, we have $i_0 \ge 5$. We use the reduction to absurdity to prove that surely $i_0 = 5$. Suppose $i_0 \ne 5$, it implies $i_0 \ge 7$, thus we can define the four sets

$$Q_1 = (b_1 b_2 b_3) \times (S \backslash \{b_1, \ldots, b_{i_0}\}), \quad Q_2 = (b_1 b_4 b_5) \times (S \backslash \{b_1, \ldots, b_{i_0}\}),$$
$$Q_3 = (b_2 b_4 b_6) \times (S \backslash \{b_1, \ldots, b_{i_0}\}), \quad Q_4 = \{b_j b_k,\ 1 \le j < k \le i_0\}.$$

We firstly prove that S, Q_1, Q_2, Q_3 and Q_4 are mutually exclusive. If not, let us suppose that among the five sets there are some two of them the intersection of which is nonempty, say $S \cap Q_1 \ne \emptyset$. Assume $b \in S \cap Q_1$, then there exists some $b' \in S \backslash \{b_1, \ldots, b_{i_0}\}$ such that $b = b_1 b_2 b_3 b'$, which leads that $b b_1 b_2 b_3 b'$ is a defining word of S with length 3 (if $b = b'$ or b_1 or b_2 or b_3) or 5. However, this is impossible under the given assumption for i_0. If there are other two of them whose intersection is nonempty, similarly, we can also find a defining word the length of which is an odd number and smaller than i_0, which is still impossible. By the above arguments, we get

$$\#\{S\} + \sum_{j=1}^{4} \#\{Q_j\} = s + 3(s - i_0) + i_0(i_0 - 1)/2 = 4s + i_0(i_0 - 7)/2 \ge 4s \ge 2^r + 4,$$

where the third and forth inequalities are from the assumptions $i_0 \geq 7$ and $s \geq 2^{r-2}+1$, respectively. On the other hand, since $S \subset H_r$, $Q_j \subset H_r$ for $j = 1,2,3,4$, and the five sets are mutually exclusive, we have $\#\{S\} + \sum_{j=1}^{4} \#\{Q_j\} < 2^r$, the contradiction completing the proof of Lemma 9. $\square$

With the preparations above, we come to prove Part (b) of the theorem.

Suppose that S is a resolution at least IV design with s factors and $\bar{g}(S)$ is minimized, where $2^{r-2}+1 \leq s \leq 2^{r-1}$ for some $r \leq q$. Firstly, we prove the first half of Part (b). Since any design $S \subset H_q$ satisfying $2^{q-2}+1 \leq s \leq 2^{q-1}$ and having resolution at least IV has exactly q independent factors, the first half of Part (b) holds when $r = q$. We only need to consider $r \leq q-1$.

It is obvious that S has at least r independent factors. If S has $h+1$ independent factors with $r \leq h \leq q-1$, we assume that S has the form in (5). That is,

$$S = Q \cup \{a, ab_1, \ldots, ab_t\},$$

where Q and $\{a, b_1, \ldots, b_t\}$ satisfy the conditions as in (5). Let $Q_1 = \{a, ab_1, \ldots, ab_t\}$ and define $S^* = aQ \cup Q_1$, then $S^* \subset F_{q(h+1)}$. Further let $S^{**} = Q \cup \{b_1, \ldots, b_t\}$, then $S^* = \{a, aS^{**}\}$ and $S^{**} \subset H_h$. It leads that, S^{**} has $s-1$ factors with $2^{r-2} \leq s-1 \leq 2^{r-1}-1$ and among them there are h ones to be independent. Note that, when the range of S is over all the designs with resolution at least IV, then the range of S^{**} is over all the designs with $s-1$ factors. By the structure of $F_{q(h+1)}$, Lemma 8 and the condition of $\bar{g}(S)$ being minimized, we have

$$\begin{aligned}
\bar{g}(S) &= \bar{g}(S^*) = \#\{\gamma : \gamma \in H_q \backslash S^*, B_2(S^*, \gamma) > 0\} \\
&= \#\{\gamma : \gamma \in H_h, B_2(S^*, \gamma) > 0\} \\
&= \#\{\gamma : \gamma \in H_h \backslash S^{**}, B_2(S^*, \gamma) > 0\} + \#\{\gamma : \gamma \in S^{**}, B_2(S^*, \gamma) > 0\} \\
&= \#\{\gamma : \gamma \in H_h \backslash S^{**}, B_2(S^{**}, \gamma) > 0\} + (s-1) \\
&= \bar{g}(S^{**}) + (s-1).
\end{aligned}$$

Thus, $\bar{g}(S^{**})$ is minimized too. According to Part (a) of the theorem, S^{**} can only have $r-1$ independent factors, contradicting to it having $h\,(\geq r)$ independent factors. This contradiction finishes the proof of the first half of Part (b).

Next, we consider the proof of the second half of Part (b). Now the S has r independent factors. Suppose the S has the form of (5) with $h = r-1$, and define S^* as above. Butler (2003) noticed that if $A_i(S) = 0$ for all odd numbers i's, then $S \subset F_{qr}$. Therefore, to finish the proof of the second half, it is sufficient to prove that $A_i(S) = 0$ for all odd numbers i's. If not, according to Lemma 9 and the assumption that S has resolution at least IV, we have $A_5(S) > 0$. In the following we prove that if $A_5(S) > 0$, then $\bar{g}(S^*) < \bar{g}(S)$ which is a contradiction to the assumption that $\bar{g}(S)$ is minimized. By Lemma 8 and its proof, it suffices to show that there exists a $\gamma \in H_{r-1}$ such that $B_2(S^*, \gamma) > 0$, $\gamma \notin S$ with $B_2(S, \gamma) > 0$ and $a\gamma \notin S$ with $B_2(S, a\gamma) > 0$.

Without loss of generality, we assume the factor a appears in the defining word with length 5. By the structure of S, there are two possibilities for this defining word with length 5: one is that, besides a one more factor is from Q_1 and the other three factors are from Q, and the other is that, besides a three more factors are from Q_1 and the other one factor is from Q. After a suitable relabelling, we denote these two possibilities as

$$I = a(ab_1)d_1d_2d_3, \quad \text{where } ab_1 \in Q_1,\ \{d_1, d_2, d_3\} \subset Q$$

and

$$I = a(ab_1)(ab_2)(ab_3)d_1, \quad \text{where } \{ab_1, ab_2, ab_3\} \subset Q_1,\ d_1 \in Q.$$

For the first case, let $\gamma = b_1d_1 = d_2d_3$. We can verify that $B_2(S^*, \gamma) > 0$ and $B_2(S, \gamma) > 0$. Note that $a\gamma = (ab_1)d_1$, where $ab_1 \in Q_1 \subset S$ and $d_1 \in Q \subset S$. Therefore, we have $B_2(S, a\gamma) > 0$. Since the S has resolution IV, $\gamma \notin S$ and $a\gamma \notin S$. For the second case, let $\gamma = (ab_1)(ab_2) = b_3d_1$ and the proof is similar as the first case. Hence the claim that $S \subset F_{qr}$ is proved. Noting that F_{qr} and T_r are isomorphic, then the second half of Part (b) follows.

Proof of Part (c)

We first prove that the four designs consisting of the first or last s columns of F_{qr} or T_r are isomorphic. Suppose that F'_{qr} consists of the 2^{r-1} columns in F_{qr} in a contrary order. Then we can easily validate

$$F_{qr} = \{q, qH_{r-1}\} \text{ and } F'_{qr} = \{12\cdots(r-1)q, 12\cdots(r-1)qH_{r-1}\},$$

which mean that, the design consisting of the first s columns of F_{qr} and the one consisting of the last s columns of F_{qr} are isomorphic. Similarly, the design consisting of the first s columns of T_r and the one consisting of the last s columns of T_r are isomorphic. When F_{qr} and T_r are written in Yates order, from the structures of F_{qr} and T_r, we have that the design consisting of the first s columns of T_r and the one consisting of the first s columns of F_{qr} are isomorphic. Therefore the four designs consisting of the first or last s columns of F_{qr} or T_r are isomorphic.

Suppose that S is a design with s factors and maximizes the sequence (2.4) among all the designs with resolution at least IV and s factors, where $2^{r-2}+1 \le s \le 2^{r-1}$ for some $r \le q$. By the above analysis, proving Part (c) is equivalent to showing that the unique choice of such S is the design consisting of the first s columns of F_{qr}. In the following we use the mathematical induction to prove this point.

Firstly, we show it holds for $r \le 3$. According to the result of Part (b) just proved, we have $S \subset F_{qr}$. When $s = 1, 2, 3$, under isomorphism, the unique choices of such S are $\{a\}$, $\{a, 1a\}$ and $\{a, 1a, 2a\}$, respectively. Here we remind the mention in Section 2 about resolution at least IV when all the s factors are independent even $s \le 3$. When $s = 4$, according to Part (b) proved above, the number of independent factors in such S is 3 and the choice of S is only $\{a, 1a, 2a, 12a\}$. So, for the four cases of s, such design S is the only one that consists of the first s columns of F_{qr}. Thus the result follows for $r \le 3$.

Next, assume that, for $r \leq k$, the fact that the design maximizing (2.4) in all the designs with s factors and resolution at least IV uniquely consists of the first s columns in F_{qr} is true, and come to prove that for $r = k+1$ the fact is true too. By Part (b) of the theorem, we have $S \subset F_{q(k+1)}$. Note that, by Lemma 1 (a) with q being taken as $k+1$ and the condition $2^{k-1}+1 \leq s \leq 2^k$, for any $\gamma \in H_k$, we have

$$B_2(S, \gamma) = B_2(F_{q(k+1)} \backslash S, \gamma) + s - 2^{k-1} \geq 1$$

and hence $\bar{g}(S) = 2^k - 1$, which is a constant. Therefore, maximizing (2.4) is equivalent to maximizing ${}^{\#}_{2}C_2(S)$. By Lemma 1 (c) with q being taken as $k+1$, we know that maximizing ${}^{\#}_{2}C_2(S)$ is equivalent to maximizing the sequence

$$\Big\{ -\bar{g}(F_{q(k+1)} \backslash S),\ {}^{\#}_{2}C_2(F_{q(k+1)} \backslash S) \Big\}. \tag{7}$$

Note that, when $r = k+1$, by the assumptions in Part (c) we have $2^{k-1}+1 \leq s \leq 2^k$ and the number of factors in $F_{q(k+1)} \backslash S$ is smaller than 2^{k-1}. Applying the inductive assumption for $r \leq k$, if $F_{q(k+1)} \backslash S$ consists of the first $2^k - s$ columns in $F_{q(k+1)}$, it uniquely maximizes the sequence (7). As we already proved at the beginning of this part, the design consisting of the last $2^k - s$ columns in $F_{q(k+1)}$ columns and the one consisting the first $2^k - s$ columns in $F_{q(k+1)}$ columns are isomorphic. Therefore if we choose $F_{q(k+1)} \backslash S$ to be the one consisting of the last $2^k - s$ columns in $F_{q(k+1)}$, then it also maximizes the sequence (7). In this way, the unique choice of such S is the set of the first s columns in $F_{q(k+1)}$, which means that, the result is true for $r = k+1$ and hence it is true for all $r \leq q$ by the mathematical induction. This completes the proof of Part (c).

Up to now, the proofs of all the three parts of Theorem 1 are finished.

References

Butler, N. A. (2003). Some theory for constructing minimum aberration fractional factorial designs. *Biometrika* **90**, 233-238.

Department of Mathematical and Statistical Sciences, University of Alberta Edmonton, AB T6G 2G1, Canada

E-mail: pengfei@stat.ualberta.ca

School of Mathematical Sciences, Qufu Normal University, Qufu 273165, China

E-mail: zhaoshli758@126.com

LPMC and School of Mathematical Sciences, Nankai University, Tianjin 300071, China

KLAS and School of Mathematics and Statistics, Northeast Normal University, Changchun 130024, China

E-mail: zhrch@nankai.edu.cn, rczhang@nenu.edu.cn