

Cyclicly constructed $E(s^2)$ -optimal supersaturated designs

Dursun A. Bulutoglu*

Air Force Institute of Technology, 2950 Hobson Way, Wright Patterson AFB 45433, USA

Received 17 August 2005; received in revised form 6 June 2006; accepted 10 September 2006

Available online 17 November 2006

Abstract

Nguyen [1996. An algorithmic approach to constructing supersaturated designs. *Technometrics* 38, 69–73] and Tang and Wu [1997. $E(s^2)$ -optimality of supersaturated designs. *Statist. Sinica* 7, 929–939] independently derived a lower bound for the $E(s^2)$ value of an N run, m factor supersaturated design (SSD). This bound can be achieved only if m is a multiple of $N - 1$ when $N \equiv 0 \pmod{4}$ or if m is an even multiple of $N - 1$ when $N \equiv 2 \pmod{4}$. One important question is whether Nguyen–Tang–Wu bound can be achieved in all of these cases. In this paper, based on a construction method by Bulutoglu and Cheng (2004), we present a theoretical method for finding as many positive integers t as possible such that there is an $E(s^2)$ -optimal SSD achieving the Nguyen–Tang–Wu bound with N runs and $t(N - 1)$ factors when $N \equiv 0 \pmod{4}$ and $2t(N - 1)$ factors when $N \equiv 2 \pmod{4}$. This method is applied to the $N = 12, 14, 18, 20, 24, 26, 28, 30, 32, 38, 42, 44, 48, 50, 54$ cases.

© 2006 Elsevier B.V. All rights reserved.

Keywords: Balanced incomplete block designs; Difference vector; Lower bound; Minimax criterion; Orbit; Primitive element

1. Introduction

A supersaturated design (SSD) is a factorial design that does not have enough runs to estimate all main effects. Booth and Cox (1962) proposed the $E(s^2)$ criterion as a way to order such designs. Due to their applications in factor screening experiments, there is a renewed interest in constructing SSDs. Applications and theories in which the $E(s^2)$ criterion is used to discriminate between two-level SSDs are abundant in the recent literature; see Lin (1993, 1995), Wu (1993), Nguyen (1996), Tang and Wu (1997), Cheng (1997), Li and Wu (1997), Butler et al. (2001), Eskridge et al. (2004), Liu and Dean (2004), Bulutoglu and Cheng (2004), Ryan and Bulutoglu (2006) and Nguyen and Cheng (2006).

A two-level SSD with N runs and m factors is represented by an $N \times m$ matrix X , where every entry is ± 1 and every column has an equal number of $+1$ s and -1 s. It is also assumed that no two columns of X are completely aliased (i.e., for all pairs of columns x and y of X , $x \neq y$ and $x \neq -y$) implying that

$$N - 1 < m \leq \binom{N - 1}{\frac{N}{2} - 1}. \quad (1)$$

* Tel.: +1 937 2553636x4704.

E-mail address: dursun.bulutoglu@afit.edu.

The $E(s^2)$ value of an SSD is

$$E(s^2) = \frac{\sum_{i < j} s_{ij}^2}{\binom{m}{2}},$$

where s_{ij} is the dot product between the i th and j th columns of X . The $E(s^2)$ criterion is used to discriminate among N run, m factor SSDs by selecting designs with smaller $E(s^2)$ values. Nguyen (1996) and Tang and Wu (1997) independently proved that

$$E(s^2) \geq \frac{m - N + 1}{(m - 1)(N - 1)} N^2 \quad (2)$$

for any N run, m factor SSD. Bound (2) can be achieved only if $m = t(N - 1)$ and $N \equiv 0 \pmod{4}$ or if $m = 2t(N - 1)$ and $N \equiv 2 \pmod{4}$ for some positive integer t . Even though it is easy to construct $t(N - 1)$ factor, N run designs achieving Nguyen–Tang–Wu bound when $N \equiv 0 \pmod{4}$ by concatenating saturated designs obtained from Hadamard matrices (see Ryan and Bulutoglu, 2006; Tang and Wu, 1997) there is no guarantee that such designs have no aliased columns and qualify as SSDs. Similarly it is easy to construct $t(N - 1)$ factor, N run designs achieving Nguyen–Tang–Wu bound when $N \equiv 2 \pmod{4}$ by concatenating SSDs with N runs and $2(N - 1)$ factors, but such designs may have aliased columns disqualifying them from being SSDs. An interesting and difficult question is whether Nguyen–Tang–Wu bound can be achieved by SSDs for every multiple of $N - 1$ when $N \equiv 0 \pmod{4}$ and for every even multiple of $N - 1$ when $N \equiv 2 \pmod{4}$ assuming (1) holds.

Bulutoglu and Cheng (2004) (Theorems 2.1–2.3) provided a method based on balanced incomplete block designs (BIBDs) for constructing SSDs achieving the Nguyen–Tang–Wu bound. However, they never investigated for which multiples $t(N - 1)$ of $N - 1$ their method yielded an SSD with N runs and $t(N - 1)$ factors. Hence, for given N for which the construction of Bulutoglu and Cheng (2004) applies, it is not possible to know the set of positive integers t such that the construction of Bulutoglu and Cheng (2004) yields an N run $t(N - 1)$ factor SSD without implementing the construction and counting the number of columns in the resulting designs. The goal of this paper is first to extend the construction method of Bulutoglu and Cheng (2004) by constructing N run, $(N - 2)(N - 1)$ factor or $(N - 2)(N - 1)/2$ factor, $E(s^2)$ -optimal SSD and second to provide an efficient theoretical method for finding as many positive integers t as possible such that there is an $E(s^2)$ -optimal, N run, $t(N - 1)$ factor SSD obtained by using the construction of Bulutoglu and Cheng (2004). The novelty of this theoretical method is that the construction of Bulutoglu and Cheng (2004) does not need to be implemented and that the method can be implemented with little computational power. On the other hand, computing all $t(N - 1)$ factor SSDs obtained by using the construction of Bulutoglu and Cheng (2004) to determine the values t for which their construction yields a $t(N - 1)$ factor SSD is computationally expensive.

Booth and Cox (1962) also proposed the minimax criterion for selecting a two-level SSD. This criterion was studied by Tang and Wu (1997) when $m = t(N - 1)$ for some positive integer t . The minimax criterion ranks designs by

$$s_{\max} = \max_{i < j} |s_{ij}|$$

and then by

$$f_{s_{\max}} = \sum_{i < j} I_{s_{\max}}(|s_{ij}|),$$

where the indicator function $I_a(b) = 1$ if $a = b$ and is 0 otherwise. The minimax criterion can most often distinguish between designs with the same $E(s^2)$ value.

In Section 2, Theorem 2.2 of Bulutoglu and Cheng (2004) is generalized. It is also proven that when $N - 1$ is a prime power the construction of Bulutoglu and Cheng (2004) yields an $E(s^2)$ -optimal SSD with N runs and $(N - 1)(N - 2)$ factors. Furthermore, a theorem which provides insight about the design characteristic $f_{s_{\max}}$ of SSDs constructed by the method of Bulutoglu and Cheng (2004) is stated and proven. Finally, $E(s^2)$ -optimal SSDs constructed by the method of Bulutoglu and Cheng (2004) are compared using the minimax criterion with those constructed by the NOA_k algorithm in Ryan and Bulutoglu (2006).

Ryan and Bulutoglu (2006) designed the SRS_4 algorithm based on concatenating saturated designs obtained from Hadamard matrices when $N \equiv 0 \pmod{4}$ or $E(s^2)$ -optimal SSDs with N runs and $2(N - 1)$ factors when $N \equiv 2 \pmod{4}$.

The minimax properties of the best $E(s^2)$ -optimal SSDs produced by this algorithm are inferior to those constructed by the method of Bulutoglu and Cheng (2004). Hence this makes it even more important to determine for which multiples t the method of Bulutoglu and Cheng (2004) yields an $E(s^2)$ -optimal N run, $t(N - 1)$ factor SSD. In Section 3 new theorems are proven to determine the values of t for which the method of Bulutoglu and Cheng (2004) yields an $E(s^2)$ -optimal, N run, $t(N - 1)$ factor SSD. Based on these new theorems, a method for finding all possible such t is given. A heuristic based on this method for finding as many positive such t as possible is described and applied to the $N = 12, 14, 18, 20, 24, 26, 28, 30, 32, 38, 42, 44, 48, 50, 54$ cases. For easy reference, below is a list of some definitions and conventions used throughout this paper.

- \mathbb{Z}^+ is the set of positive integers.
- \mathbb{Z} is the set of integers.
- Let $A = \{a_1, a_2, \dots, a_n\}$ be a set of integers and let $y \in \mathbb{Z}$. Define

$$yA = \{ya_1, ya_2, \dots, ya_n\}.$$

- $\text{GF}(s)$ denotes a finite field with s elements. The multiplicative group consisting of the non-zero elements of $\text{GF}(s)$ is cyclic, and a generator of this group is called a primitive element of the field.
- $\mathbb{Z}_q = \{0, 1, \dots, q - 1\}$ is the commutative ring of order q with addition and multiplication modulo q .
- Products and sums in \mathbb{Z}_q are reduced modulo q when needed.
- For each $T = \{a_1, a_2, \dots, a_t\} \subset \mathbb{Z}_q$ and $b \in \mathbb{Z}_q$,

$$T + b = \{a_1 + b, a_2 + b, \dots, a_t + b\} \pmod{q}.$$

2. SSDs based on BIBDs

Cheng (1997) showed that for $t \in \mathbb{Z}^+$ constructing an N run, $m = t(N - 1)$ factor optimal SSD is equivalent to constructing a $\text{BIBD}(N - 1, t(N - 1), N/2 - 1)$, a BIBD with $N - 1$ treatments and $q(N - 1)$ distinct blocks each having size $N/2 - 1$. Using this result when $N - 1$ is an odd prime power, Bulutoglu and Cheng (2004) constructed optimal SSDs with N runs and $e(N - 1)$ factors, where e is defined in Theorem 2.2 Bulutoglu and Cheng (2004). It is not hard to show that the SSDs constructed by Bulutoglu and Cheng (2004) belong to the class of k -circulant SSDs defined by Liu and Dean (2004). For quick reference, Theorems 2.2 and 2.3 in Bulutoglu and Cheng (2004) are stated respectively.

Theorem 1 (Bulutoglu and Cheng, 2004). *Suppose $N - 1$ is an odd prime power, q is an even divisor of $N - 2$ with $q \neq N - 2$, x is a primitive element of $\text{GF}(N - 1)$, and T is a subset of \mathbb{Z}_q of size $q/2$. Let e be the smallest positive integer such that $T + e = T$. Then the $e(N - 1)$ sets $\{S_{r,a} : r = 0, \dots, e - 1, a \in \text{GF}(N - 1)\}$, where $S_{r,a} = \{x^{jq+i} + a : 0 \leq j \leq (N - 2)/q - 1, i \in T + r\}$, are distinct and constitute a $\text{BIBD}(N - 1, e(N - 1), N/2 - 1)$. Furthermore, if $(N - 2)/q$ is odd and U is a subset of size $e/2$ of $\{0, \dots, e - 1\}$ such that $U^* = U + (q/2)$, where U^* is the complement of U in $\{0, \dots, e - 1\}$ and the addition is reduced modulo q , then the $e(N - 1)/2$ sets $\{S_{r,a} : r \in U, a \in \text{GF}(N - 1)\}$ constitute a BIBD with distinct blocks.*

Theorem 2 (Bulutoglu and Cheng, 2004). *Let q be an even divisor of $N - 2$ such that $q \neq N - 2$. Let T and T' be subsets of size $q/2$ of \mathbb{Z}_q such that $T' \neq T + a$ for all elements a of \mathbb{Z}_q . If d_1 and d_2 are BIBDs constructed by applying Theorem 2.2 of Bulutoglu and Cheng (2004) to T and T' , respectively, then d_1 and d_2 have no blocks in common; therefore their union is also a BIBD with distinct blocks.*

The following lemma is used to generalize Theorem 1.

Lemma 1. *Let $N - 1$ be an odd prime power, q be an even divisor of $N - 2$, U be a size $e/2$ subset of $\{0, 1, \dots, e - 1\}$ and U^* be the complement of U in $\{0, 1, \dots, e - 1\}$. Also, let $u_i \in \{i, i + q/2\}$ for $i = 0, 1, \dots, q/2 - 1$.*

1. *If $T \subset \mathbb{Z}_q$ has size $q/2$ and e is the smallest positive integer such that $T + e = T$, then e is an even divisor of q .*
2. *If e is any even divisor of q , then there exists a size $q/2$ set $T \subset \mathbb{Z}_q$ such that e is the smallest positive integer satisfying $T + e = T$.*

3. If $U^* = U + (q/2)$, then $e = q$ and U has the form

$$U = \bigcup_{i=0}^{q/2-1} \{u_i\}.$$

4. If $e = q$ and U has the form

$$U = \bigcup_{i=0}^{q/2-1} \{u_i\},$$

then $U^* = U + (q/2)$. A particular such U is $U = \{0, 1, \dots, q/2 - 1\}$.

Proof.

1. Clearly, e is a divisor of q . Also, since $T + e = T$, the set T has the form

$$T = \bigcup_{i=1}^{\alpha} \bigcup_{j=0}^{q/e-1} \{x_i + je\}$$

for some $\alpha \in \mathbb{Z}^+$ and $x_i \in \mathbb{Z}_q$. Since $T \subset \mathbb{Z}_q$ is of order $q/2$,

$$\frac{q}{2} = \frac{\alpha q}{e}.$$

Hence, e is divisible by 2.

2. Assume that e is an even divisor of q and consider the set

$$T = \bigcup_{j=0}^{q/e-1} \bigcup_{i=1}^{e/2} \{i + je\}.$$

Clearly, $T \subset \mathbb{Z}_q$ has size $q/2$, and it is easy to see that e is the smallest integer such that $T + e = T$.

3. If $q \neq e$, then $q/e \geq 2$, since e is a divisor of q . Hence, $2e - 2 < q$ implying $e - 1 + q/2 < q$ and $e/2 + q/2 > e - 1$. Therefore, for any $y \in \{e/2, e/2 + 1, \dots, e - 1\}$, $e - 1 < y + q/2 < q$. Thus, there does not exist $y \in U$ such that $y \in \{e/2, e/2 + 1, \dots, e - 1\}$. So $U = \{0, 1, \dots, e/2 - 1\}$, but this cannot happen because $e - 1 < e/2 - 1 + q/2 < q$. To prove the second part of the statement, observe that since $U^* = U + (q/2)$, there are no two elements $x, y \in U$ with $x - y \equiv q/2 \pmod{q}$, so U must have the form

$$U = \bigcup_{i=0}^{q/2-1} \{u_i\}.$$

4. This part is easy to see.

Lemma 1 and Theorem 1 imply the following, more general result.

Theorem 3. Let $N - 1$ be an odd prime power and q be an even divisor of $N - 2$ with $q \neq N - 2$. Then there exist an $E(s^2)$ -optimal SSD with N runs and $m = q(N - 1)$ factors achieving the Nguyen–Tang–Wu bound (2) constructed by Theorem 1. Furthermore, if $(N - 2)/q$ is odd, then there are $E(s^2)$ -optimal SSDs with N runs and $m = q/2(N - 1)$ factors achieving the Nguyen–Tang–Wu bound (2) constructed by Theorem 1 by taking

$$U = \bigcup_{i=0}^{q/2-1} \{u_i\},$$

where $u_i \in \{i, i + q/2\}$.

Conversely for any $E(s^2)$ -optimal SSD with N runs and $m = e(N - 1)$ factors constructed by the first part of Theorem 1, e must be an even divisor of $N - 2$. Furthermore, for any $E(s^2)$ -optimal SSD with N runs and $m = e/2(N - 1)$ factors constructed by the second part of Theorem 1 $e = q$, and

$$U = \bigcup_{i=0}^{q/2-1} \{u_i\}$$

for some $u_i \in \{i, i + q/2\}$.

The following group action is needed in the next Example and Theorem 4. Let \mathcal{F}_q denote the set of all size $q/2$ subsets of \mathbb{Z}_q . Let \mathbb{Z}_q act on \mathcal{F}_q by

$$T \rightarrow T + a \pmod{q}$$

for $a \in \mathbb{Z}_q$ and $T \in \mathcal{F}_q$. This group action partitions \mathcal{F}_q into orbits. Next, we discuss an example for Theorem 3 and demonstrate the gain in generalizing Theorem 1.

Example 1. Let $N = 14$. Then $N - 2 = 12$ has three even divisors not equal to 12: 6, 4, and 2. Hence, by Theorem 3 there exists an $E(s^2)$ -optimal SSD achieving the Nguyen–Tang–Wu bound for $q \in \{2, 4, 6\}$. (For example to construct a BIBD(13, 72, 6), let $q = 6$, set $T = \{0, 1, 2\}$ and use the six initial blocks $\{2^0, 2^1, 2^2, 2^6, 2^7, 2^8\}$, $\{2^1, 2^2, 2^3, 2^7, 2^8, 2^9\}$, $\{2^2, 2^3, 2^4, 2^8, 2^9, 2^{10}\}$, $\{2^3, 2^4, 2^5, 2^9, 2^{10}, 2^{11}\}$, $\{2^4, 2^5, 2^6, 2^{10}, 2^{11}, 2^{12}\}$ and $\{2^5, 2^6, 2^7, 2^{11}, 2^{12}, 2^{13}\}$. Adding the integers $0, 1, 2, \dots, 12 \pmod{13}$ to all elements in the initial blocks yields a BIBD(13, 72, 6). Let X be the treatment-block incidence matrix in which (i, j) th entry is equal to 1 if the i th treatment appears in the j th block and is equal to -1 otherwise. Then appending a row of 1s to X , yields an $E(s^2)$ -optimal SSD achieving the Nguyen–Tang–Wu bound with 14 runs and 72 factors.

Note that the existence of a 14 run 72 factor SSD achieving the Nguyen–Tang–Wu bound follows directly from Theorem 3 without requiring the computation of all orbits in \mathcal{F}_q for some even divisor q of $N - 2$. On the other hand, Bulutoglu and Cheng (2004) had to compute all orbits of \mathcal{F}_6 to derive the same result.

By the converse of Theorem 3, we deduce that only $e(N - 2)$, $e \in \{2, 4, 6\}$ factor SSDs can be constructed using Theorem 1. Furthermore, if for example, $e = q = 4$ then U must be $\{0, 1\}$, $\{0, 3\}$, $\{2, 1\}$ or $\{2, 3\}$.

The next theorem simplifies the problem of finding all $E(s^2)$ -optimal SSDs with N runs constructed by Theorems 1 and 2.

Theorem 4. Let $N - 1$ be an odd prime power, let q be an even divisor of $N - 2$, and let x be a primitive element of $\text{GF}(N - 1)$.

1. Let T be in \mathcal{F}_q and e be the orbit length of T . Also, let

$$S_{r,a} = \{x^{jq+i} + a : 0 \leq j \leq (N - 2)/q - 1, i \in T + r\},$$

where $\{S_{r,a} : r = 0, 1, \dots, e - 1, a \in \text{GF}(N - 1)\}$ is the BIBD($N - 1, e(N - 1), N/2 - 1$) in Theorem 1. Then there exists some $T' \in \mathcal{F}_{N-2}$ with orbit length e such that $\{S_{r,a} : r = 0, 1, \dots, e - 1, a \in \text{GF}(N - 1)\} = \{S'_{r,a} : r = 0, 1, \dots, e - 1, a \in \text{GF}(N - 1)\}$, where $S'_{r,a} = \{x^i + a : i \in T' + r\}$.

2. Conversely, let $T' \in \mathcal{F}_{N-2}$ have orbit length e , let $q \in \mathbb{Z}^+$ be such that e divides q and q divides $(N - 2)$, and let $S'_{r,a} = \{x^i + a : i \in T' + r\}$ for $r = 0, 1, \dots, e - 1$ and $a \in \text{GF}(N - 1)$. Then there exists some $T \in \mathcal{F}_q$ with orbit length e such that $\{S'_{r,a} : r = 0, 1, \dots, e - 1, a \in \text{GF}(N - 1)\} = \{S_{r,a} : r = 0, 1, \dots, e - 1, a \in \text{GF}(N - 1)\}$, where $S_{r,a} = \{x^{jq+i} + a : 0 \leq j \leq (N - 2)/q - 1, i \in T + r\}$.

Proof.

1. Set $T' = \{jq + i : 0 \leq j \leq (N - 2)/q - 1, i \in T\}$. Then $T' \in \mathcal{F}_{N-2}$, and $T' + r = \{jq + i + r : 0 \leq j \leq (N - 2)/q - 1, i \in T\} = \{jq + i : 0 \leq j \leq (N - 2)/q - 1, i \in T + r\}$ for $r = 0, 1, \dots, e - 1$. Clearly, $T' + r \in \mathcal{F}_{N-2}$, and the orbit of T' in \mathcal{F}_{N-2} is $O_{T'} = \{T' + 0, T' + 1, \dots, T' + e - 1\}$.

2. Since T' has orbit length e , T' has the form

$$T' = \bigcup_{i=1}^{\alpha} \bigcup_{j=0}^{(N-2)/e-1} \{x_i + je\}$$

for $\alpha = e/2$ and some $x_1, x_2, \dots, x_{\alpha} \in \mathbb{Z}_{N-2}$. Since e divides q and q divides $(N - 2)$, $\beta e = q$, and $\gamma \beta e = N - 2$ for some $\beta, \gamma \in \mathbb{Z}^+$. Set

$$T = \bigcup_{i=1}^{\alpha} \bigcup_{j=0}^{\beta-1} \{x_i + je\}.$$

From this, $|T| = \alpha\beta = \beta e/2 = q/2$; thus, $T \in \mathcal{F}_q$. Finally, since

$$T' + r = \bigcup_{k=0}^{(N-2)/q-1} \{kq + T + r\},$$

the orbit length of T is e . \square

Example 1. 1. (For part 1) Setting $T' = \{0, 1, 2, 6, 7, 8\} \in \mathcal{F}_{12}$ yields the six initial blocks $\{2^0, 2^1, 2^2, 2^6, 2^7, 2^8\}$, $\{2^1, 2^2, 2^3, 2^7, 2^8, 2^9\}$, $\{2^2, 2^3, 2^4, 2^8, 2^9, 2^{10}\}$, $\{2^3, 2^4, 2^5, 2^9, 2^{10}, 2^{11}\}$, $\{2^4, 2^5, 2^6, 2^{10}, 2^{11}, 2^{12}\}$ and $\{2^5, 2^6, 2^7, 2^{11}, 2^{12}, 2^{13}\}$. Hence the BIBD(13, 72, 6) constructed from $T' \in \mathcal{F}_{12}$ is the same as the BIBD(13, 72, 6) constructed from $T \in \mathcal{F}_6$.

2. (For part 2) Let $T' = \{0, 2, 4, 6, 8, 10\} \in \mathcal{F}_{12}$ has orbit length 2 and 2 divides 4. Let $T = \{0, 2\} \in \mathcal{F}_4$ then T has orbit length 2 and the BIBD(13, 26, 6) constructed from $T' \in \mathcal{F}_{12}$ is the same as the BIBD(13, 26, 6) constructed from $T = \{0, 1, 2\} \in \mathcal{F}_6$.

Remark 1.

- (a) Note that in Theorem 1, it is assumed that q is an even divisor of $N - 2$ with $q \neq N - 2$. When $q = N - 2$, the construction still yields a BIBD($N - 1, e(N - 1), N/2 - 1$). When $e \neq q = N - 2$ by Theorem 4, this BIBD has distinct blocks and yields an N run $e(N - 1)$ factor optimal SSD. When $e = q = N - 2$ on the other hand, there is no guarantee that this BIBD has distinct blocks.
- (b) $E(s^2)$ -optimal SSDs with N runs and $(N - 2)(N - 1)/2$ factors can be constructed provided that the BIBD($N - 1, (N - 2)(N - 1)/2, N/2 - 1$) constructed using the second part of Theorem 1 has distinct blocks. These designs are constructed by setting

$$U = \bigcup_{i=0}^{(N-2)/2-1} \{u_i\}$$

for $u_i \in \{i, i + (N - 2)/2\}$.

The following theorem provides a choice for T which yields a BIBD($N - 1, (N - 2)(N - 1), N/2 - 1$) with distinct blocks. The resulting BIBD($N - 1, (N - 2)(N - 1), N/2 - 1$) corresponds to an $E(s^2)$ -optimal SSD with N runs and $(N - 2)(N - 1)$ factors.

Theorem 5. Let $N - 1 = p^n$, where $n \in \mathbb{Z}^+$ and where p is an odd prime such that $p > 7$ if $n = 1$ or $p > 2$ if $n = 2$. Let x be a primitive element of $\text{GF}(N - 1)$. If $p = N - 1$, then let $1 < x \leq (p - 1)/4$ or $p - (p + 1)/4 \leq x \leq p - 1$. Such an x exists for all primes smaller than 10^{14} . Also, let $T = \{0, 1, \dots, N/2 - 2\}$ and $S_{r,a} = \{x^i + a : i \in T + r\}$. Then the $(N - 2)(N - 1)$ sets $\{S_{r,a} : r=0, 1, \dots, N - 3, a \in \text{GF}(N - 1)\}$ are the distinct blocks of a BIBD($N - 1, (N - 2)(N - 1), N/2 - 1$).

Furthermore, if $U = \bigcup_{i=0}^{N/2-2} \{u_i\}$ for $u_i \in \{i, i + (N - 2)/2\}$, then the $(N - 1)(N - 2)/2$ sets $\{S_{r,a} : r \in U, a \in \text{GF}(N - 1)\}$ form the blocks of a BIBD($N - 1, (N - 2)(N - 1)/2, N/2 - 1$) with distinct blocks.

Proof. First, $\{S_{r,a} : r=0, 1, \dots, N - 3, a \in \text{GF}(N - 1)\}$ constitutes a BIBD($N - 1, (N - 2)(N - 1), N/2 - 1$) by the first part of Theorem 2.1 of Bulutoglu and Cheng (2004). To arrive at a contradiction, assume $\{S_{r,a} : r=0, 1, \dots, N - 3, a \in \text{GF}(N - 1)\}$ has two identical blocks. Then there exists sets $A = \{x^i + a : i \in T\}$ and $B = \{x^i : i \in T + r\}$, where $a \in \text{GF}(N - 1)$ and $0 \leq r \leq N - 3$ with either $r \neq 0$ or $a \neq 0$ such that $A = B$.

B is mapped into itself by $z \rightarrow z/x$ except for one element, and A is mapped into itself by $z \rightarrow xz + (a - ax)$ except for one element. Thus, the composite map $z \rightarrow z + (a - ax)$ maps $A = B$ into itself except for at most two elements. W.l.o.g. assume that $a - ax \neq 0$. Otherwise $x = 1$, resulting in a contradiction. Then there exists $x_0, x_1 \in A = B$ such that

$$A = \bigcup_{i=0}^{r_0} \{x_0 + i(a - ax)\}, \tag{3}$$

where $r_0 + 1 = N/2 - 1$, or

$$A = \left[\bigcup_{i=0}^{r_0} \{x_0 + i(a - ax)\} \right] \cup \left[\bigcup_{j=0}^{r_1} \{x_1 + j(a - ax)\} \right], \tag{4}$$

where $r_0 + r_1 + 2 = N/2 - 1$ and $r_0, r_1 \in \{0, 1, \dots, p - 1\}$.

Case 1: $N - 1 = p^n$ for some $n > 1, n \in \mathbb{Z}^+$. The maximum number of elements $A = B$ can have is $2p$, and $N - 1 = p^n \geq p^2$. Thus, $|A| = |B| = N/2 - 1 \geq (p^2 + 1)/2 - 1 = (p^2 - 1)/2 > 2p$ for $p \geq 5$. Therefore, there is a contradiction for $p \geq 5$. When $p = 3$, the same argument leads to a contradiction if $n \geq 3$. Finally, the $p = 3$ and $n = 2$ case was checked by computer; the resulting BIBD had distinct blocks.

Case 2: $N - 1 = p$. Let $g(p)$ be the smallest primitive element in \mathbb{Z}_p . It has been numerically observed that $g(p) < 0.3(4 + \log(p))^2$ for all primes smaller than 10^{14} . See <http://www.ieeta.pt/~tos/p-roots.html> for details. It is also clear from tables at <http://mathworld.wolfram.com/PrimitiveRoot.html> that $1 < g(p) \leq (p - 1)/4$ for all primes $p \in [11, 223]$. By these two results, one can pick a primitive element x such that $1 < x \leq (p - 1)/4$ if $p < 10^{14}$.

Let $x_0 = \alpha(a - ax)$ and $x_1 = \beta(a - ax)$ for some $\alpha, \beta \in \mathbb{Z}_p$. Then Eqs. (3) and (4) lead to the following cases:

(a)

$$A = \bigcup_{i=0}^{r_0} \{(\alpha + i)(a - ax)\},$$

where $r_0 + 1 = N/2 - 1$.

(b)

$$A = \left[\bigcup_{i=0}^{r_0} \{(\alpha + i)(a - ax)\} \right] \cup \left[\bigcup_{j=0}^{r_1} \{(\beta + j)(a - ax)\} \right],$$

where $r_0 + r_1 + 2 = N/2 - 1$ and $r_0, r_1 \in \{0, 1, \dots, p - 1\}$.

W.l.o.g. assume that $\alpha = 1$. Let $x^{r'} = a - ax$ for some $0 < r' < p - 1$. Let A' and B' be the elements of A and B divided by $(a - ax)$, respectively. $A = B$ implies that $A' = \{x^t, x^{t+1}, \dots, x^{t+(p-3)/2}\} = B'$, where $t = r - r'$. Since $1 \in A'$ in both cases, $1 \in B'$, and this implies that either $x \in B'$ or $1/x \in B'$. Let $y \in \{x, 1/x\}$. Then the map $z \rightarrow yz$ maps $A' = B'$ into itself except for one element.

Case 2(a):

- i. $1 < y \leq (p - 1)/4$. Let θ be the smallest positive integer such that $\theta y > (p - 1)/2$ then $\theta \in [2, (p - 1)/4]$, $(p - 1)/2 < \theta y < p - 1$, and $(p - 1)/2 < (\theta + 1)y \leq p - 1$. Therefore, in this case, the map $z \rightarrow yz$ cannot map A' into itself except for one element, so $A \neq B$, a contradiction.

ii. $(p - 1)/4 < y \leq (p - 1)/2$. Let $y = (p - 1)/4 + s$. Then $0 < s \leq (p - 1)/4$ and $s \in \mathbb{Z}^+$. Observe that $y \in A$, $2y = (p - 1)/2 + 2s \notin A$, $3y = (p - 3)/4 + 3s \in A$, and $4y = p - 1 + 4s \notin A$. Therefore, if A' has more than three elements the map $z \rightarrow yz$ does not map A' into itself except for 1 element. It follows that if $p > 7$, then $A \neq B$, a contradiction.

Case 2(b): Also, $A = \{x^r, x^{r+1}, \dots, x^{r+N/2-2}\}$, and

$$\begin{aligned} -A &= \{-x^r, -x^{r+1}, \dots, -x^{r+N/2-2}\} \\ &= \{x^{(p-1)/2+r}, x^{(p-1)/2+r+1}, \dots, x^{(p-1)/2+r+N/2-2}\}. \end{aligned}$$

Hence, $A \cup -A = \mathbb{Z}_p - \{0\}$, and $A \cap -A = \emptyset$. This implies that

$$\left[\bigcup_{i=0}^{r_0} \{(\alpha + i)(a - ax)\} \right] \cup \left[\bigcup_{j=0}^{r_1} \{-(\beta + j)(a - ax)\} \right] = \bigcup_{i=1}^{(p-1)/2} \{i(a - ax)\},$$

where either $\alpha = 1$ or $\beta = 1$.

Let $A'_1 = \{1, 2, \dots, \gamma\}$ and $A'_2 = \{-(\gamma + 1), -(\gamma + 2), \dots, (p + 1)/2\}$, where $\gamma = 1 + r_0$. Then $A' = A'_1 \cup A'_2$. Observe that the map $z \rightarrow 1/z$ maps element 1 to 1 and maps $(p + 1)/2$ to 2. Since $A' = B'$, the map $z \rightarrow 1/z$ maps at least two elements of B' into B' . This implies that both x and $1/x$ are in B' .

Let the elements of A'_1 and A'_2 be ordered from smallest to largest using their non-negative integer representation in $[0, p - 1]$. Let \mathbb{Z}_p^0 be the elements of \mathbb{Z}_p represented by p equally spaced points on a circle.

i. $1 < x \leq (p - 1)/4$.

A. $|A'_1| \leq |A'_2|$. First, observe that $|A'_1| \leq (p - 1)/4$ and $(p - 1)/4 \leq |A'_2|$. Then for any $x \in A'_1$, there exists $\theta \in A'_1$ such that $\gamma + 1 \leq x\theta \leq (p - 1)/2$. Therefore, $x A'_1$ has at least one element not in A' . If (for $i = 1, 2, \dots, \gamma$) $\{xi\}$ traverses the circle \mathbb{Z}_p^0 more than once, then $\{xi\}$ passes through the arc $[\gamma + 1, \gamma + 2, \dots, (p - 1)/2]$ more than once. This forces $x A'_1$ to have two elements not in A' . Hence, the elements in $x A'_1$ can traverse the arc $[\gamma + 1, \gamma + 2, \dots, (p - 1)/2]$ at most once. This implies that the elements in $x A'_1$ cover at most $\lceil \gamma/x \rceil + \lfloor \gamma/x \rfloor$ elements in A'_1 and $\lceil [(p - 1)/2 - \gamma]/x \rceil$ elements in A'_2 . If $x[(p + 1)/2] \in A'_1$, then $x A'_2$ traverses through $[\gamma + 1, \gamma + 2, \dots, (p - 1)/2]$ at least once implying that $x A'_2$ has an element not in A' . Therefore, one can assume that $x[(p + 1)/2] \in A'_2$ and that $x A'_2$ does not traverse through $[\gamma + 1, \gamma + 2, \dots, (p - 1)/2]$. Then $x A'_2$ can cover at most $\lceil [(p - 1)/2 - \gamma]/x \rceil + \lceil \gamma/x \rceil$ elements in A' . Also, observe that $x A'_1$ traverses through $[1, 2, \dots, \gamma]$ at most once as $|A'_1| \leq |A'_2|$; this forces the maximum possible number of elements of A'_1 covered by elements of $x A'_1$ to be $\lfloor \gamma/x \rfloor$.

Thus, the maximum number of elements in A' covered by elements of $x A'_1 \cup x A'_2$ is $2\lceil [(p - 1)/2 - \gamma]/x \rceil + \lfloor \gamma/x \rfloor + \lceil \gamma/x \rceil - 1$. Since all elements of A' except one are covered by $x A'_1 \cup x A'_2$,

$$2 \left\lceil \frac{(p - 1)/2 - \gamma}{x} \right\rceil + \left\lceil \frac{\gamma}{x} \right\rceil + \left\lfloor \frac{\gamma}{x} \right\rfloor - 1 \geq \frac{(p - 1)}{2} - 1.$$

This implies that $x = 2$ as $p \geq 11$, but then $x(p + 1)/2 = 2(p + 1)/2 = p + 1 \in A'_1$. Therefore, $x A'_1 \cup x A'_2$ has more than one element not in A' , a contradiction.

B. $|A'_2| \leq |A'_1|$. The proof is similar to that of Case A.

ii. $-(p + 1)/4 \leq x < -1$. The proof is similar to that of Case i. \square

The following is a simple example for the construction in Theorem 5.

Example 1. (continued) By Theorem 5 there exists a 14 run, 156 factor $E(s^2)$ -optimal SSD achieving the Nguyen–Tang–Wu bound. The corresponding BIBD(13, 156, 6) is constructed by taking $T = \{0, 1, 2, 3, 4, 5\}$ and using the following 12 initial blocks: $B_{i+1} = \{2^{0+i}, 2^{1+i}, 2^{2+i}, 2^{3+i}, 2^{4+i}, 2^{5+i}\}$ for $i = 0, 1, 2, \dots, 11$.

Theorem 5 does not hold for any size $(N - 2)/2$ subset T of \mathbb{Z}_{N-2} . The following is a counterexample.

Example 1. (continued) Let $T = \{0, 1, 2, 3, 4, 10\}$ then the blocks of the corresponding BIBD(13, 156, 6) are $S_{i,a} = \{2^{0+i} + a, 2^{1+i} + a, 2^{2+i} + a, 2^{3+i} + a, 2^{4+i} + a, 2^{10+i} + a\}$, where $i = 0, 1, 2, \dots, 11, a = 0, 1, 2, \dots, 12$ and addition is reduced modulo 13. Observe that $S_{0,0} = S_{6,5} = \{2^0, 2^1, 2^2, 2^3, 2^4, 2^{10}\}$. Hence the design constructed from the treatment-block incidence matrix has aliased columns and does not qualify as an 156 factor, 14 run SSD.

It is clear from Theorem 1 that if T_1 and T_2 belong to the same orbit they yield the same BIBD($N - 1, e(N - 1), N/2 - 1$). When $q \neq N - 2$, by Theorem 2, if T_1 and T_2 belong to different orbits, then the BIBDs constructed by using Theorem 1 with T_1 and T_2 , respectively, have no common blocks. The following remark concerns the case when $q = N - 2$.

Remark 2. When $q = N - 2$, if there are two subsets T_1 and T_2 in \mathcal{F}_q such that the resulting BIBDs obtained by applying Theorem 1 to T_1 and T_2 have no repeated blocks and such that these two BIBDs have no common blocks, then these two BIBDs can be combined to get a larger BIBD without repeated blocks. This larger BIBD can be converted to an $E(s^2)$ -optimal SSD.

One might think that using different generators for $GF(N - 1)$ in Theorem 1 yields new BIBDs. The following lemma shows that this is not the case.

Lemma 2. Let x_1 and x_2 be distinct primitive elements of $GF(N - 1)$. Also, let q be an even divisor of $N - 2$ and T be a size $q/2$ subset of \mathbb{Z}_q . Then

$$\begin{aligned} S_{r,a} &= \{x_2^{jq+i} + a : 0 \leq j \leq (N - 2)/q - 1, i \in T + r\} \\ &= \{x_1^{jq+i} + a : 0 \leq j \leq (N - 2)/q - 1, i \in T' + r'\} \end{aligned}$$

for some $T' \in \mathcal{F}_q$ and $r' \in \mathbb{Z}_q$.

Proof. Since x_1 is a primitive element of $GF(N - 1)$, $x_1^\alpha = x_2$ for some $\alpha \in \mathbb{Z}_{N-2}$ such that α and $N - 2$ are relatively prime. Hence,

$$\{jq \pmod{(N - 2)} : 0 \leq j \leq (N - 2)/q - 1\} = \{j\alpha q \pmod{(N - 2)} : 0 \leq j \leq (N - 2)/q - 1\}.$$

Therefore,

$$\begin{aligned} S_{r,a} &= \{x_2^{jq+i} + a : 0 \leq j \leq (N - 2)/q - 1, i \in T + r\} \\ &= \{x_1^{\alpha jq+i} + a : 0 \leq j \leq (N - 2)/q - 1, i \in T + r\} \\ &= \{x_1^{jq+i} + a : 0 \leq j \leq (N - 2)/q - 1, i \in \alpha T + \alpha r\} \\ &= \{x_1^{jq+i} + a : 0 \leq j \leq (N - 2)/q - 1, i \in T' + r'\}, \end{aligned}$$

where $T' = \alpha T$ and $r' = \alpha r$. \square

The following theorem gives information about $f_{s_{\max}}$ for $E(s^2)$ -optimal SSDs constructed by Theorem 1 or Remark 1.

Theorem 6. Let X be an N , run $e(N - 1)$ factor $E(s^2)$ -optimal SSD constructed by the first part of Theorem 1 or Remark 1. Then the frequency of every distinct entry in $X^T X$ is a multiple of $e(N - 1)$. In particular, $f_{s_{\max}}$ appears a multiple of $e(N - 1)$ times. Furthermore, if X is an N run, $e(N - 1)/2$ factor optimal SSD constructed by the second part of Theorem 1 or the second part of Remark 1, then every distinct entry in $X^T X$ appears a multiple of $(N - 1)$ times.

Proof. For simplicity, the theorem is proved when $N - 1 = p$. The proof of the general case is similar. Let x be a primitive element in \mathbb{Z}_p . Order the elements of \mathbb{Z}_p as $\mathbb{Z}_p = \{0, 1, x, x^2, \dots, x^{(p-2)}\}$. Let σ and h be defined as

$\sigma(y) = y + 1$ and $h(y) = xy$ for any $y \in \mathbb{Z}_p$. Both σ and h act on \mathbb{Z}_p by permuting the elements of \mathbb{Z}_p . Based on the above ordering of the elements of \mathbb{Z}_p , let σ_p and h_p be the permutation representations of σ and h , respectively. Then $\sigma_p = (1, \sigma_p(1), \sigma_p^2(1), \dots, \sigma_p^{(p-1)}(1))$ and $h_p = (2, 3, \dots, p)$ are the cycle notations for σ and h , respectively. Let S_0 be the first initial block in the BIBD($N - 1, e(N - 1), N/2 - 1$) from Theorem 1. Then by Theorem 4, $S_0 = \{x^i : i \in T\}$ for some $T \in \mathcal{F}_{N-2}$.

Define the first initial block vector $v_0 \in \{1, -1\}^{N-1}$ as

$$v_{0i} = \begin{cases} -1 & \text{if } i = 1, \\ 1 & \text{if } x^{i-2} \in S_0, \\ -1 & \text{otherwise.} \end{cases}$$

If the permutations in A act on $\{+1, -1\}^{N-1}$ by permuting the coordinates, then e is the smallest integer such that $h_p^e v_0 = v_0$.

Let the $e(N - 1)$ vectors in the set $\{\sigma_p^i h_p^j v_0 : i = 0, 1, \dots, (p - 1) \text{ and } j = 0, 1, \dots, (e - 1)\}$ be the columns of the matrix X_0 . Also, let

$$X = \begin{bmatrix} X_0 \\ \mathbf{1}_{e(N-1)}^T \end{bmatrix}.$$

Then X is the $E(s^2)$ -optimal SSD constructed by the first part of Theorem 1.

Let $\sigma_p^{i_1} h_p^{j_1} v_0$ and $\sigma_p^{i_2} h_p^{j_2} v_0$ be the k_1 th and k_2 th columns of X_0 , respectively, where $k_1, k_2 \in \{1, 2, \dots, e(N - 1)\}$. Also, for $l = 1, 2$, let

$$\begin{aligned} C_l &= \{(\sigma_p^{i_l} h_p^{j_l} v_0)^T \sigma_p^i h_p^j v_0 : i = 0, 1, \dots, (p - 1) \text{ and } j = 0, 1, \dots, (p - 2)\} \\ &= \{(v_0)^T h_p^{-j_l} \sigma_p^{i_l - i} h_p^j v_0 : i = 0, 1, \dots, (p - 1) \text{ and } j = 0, 1, \dots, (p - 2)\} \\ &= \{(v_0)^T h_p^{-j_l} \sigma_p^i h_p^j v_0 : i = 0, 1, \dots, (p - 1) \text{ and } j = 0, 1, \dots, (p - 2)\}, \end{aligned}$$

let $A = \bigcup_{i=0}^{p-1} \bigcup_{j=0}^{p-2} \{\sigma_p^i h_p^j\} = \bigcup_{i=0}^{p-1} \bigcup_{j=0}^{p-2} \{\sigma^i h^j(y)\} = \bigcup_{i=0}^{p-1} \bigcup_{j=0}^{p-2} \{x^j y + i\}$, and let $h_p^k A$ be the set obtained by applying h_p^k to each element of A for any $k \in \mathbb{Z}^+$. Then $h_p^k A = \bigcup_{i=0}^{p-1} \bigcup_{j=0}^{p-2} \{x^k(x^j(y) + i)\} = \bigcup_{i=0}^{p-1} \bigcup_{j=0}^{p-2} \{(x^{(j+k)}(y) + ix^k)\} = \bigcup_{i=0}^{p-1} \bigcup_{j=0}^{p-2} \{x^j(y) + i\} = A$. This shows that $C_1 = C_2$ as multisets.

Let $C'_l = \{(v_0)^T h_p^{-j_l} \sigma_p^i h_p^j v_0 : i = 0, 1, \dots, (p - 1) \text{ and } j = 0, 1, \dots, (e - 1)\}$ for $l = 1, 2$. Since $h_p^e v_0 = v_0$ and $C_1 = C_2, C'_1 = C'_2$. The fact that $C'_1 = C'_2$ implies that the frequency of each element on the k_1 th row of $X^T X$ must be the same as the frequency of each element on the k_2 th row of $X^T X$. Since there are $e(N - 1)$ rows in $X^T X$, each element that appears as an entry in $X^T X$ must appear a multiple of $e(N - 1)$ times.

Let the $e/2(N - 1)$ vectors in the set $\{\sigma_p^i h_p^j v_0 : i = 0, 1, \dots, (p - 1) \text{ and } j \in U\}$ be the columns of the matrix X_0 , where U is the subset of $\{0, 1, \dots, e - 1\}$ specified in Theorem 3. Also, let

$$X = \begin{bmatrix} X_0 \\ \mathbf{1}_{e(N-1)}^T \end{bmatrix}.$$

Then X is the $E(s^2)$ -optimal SSD constructed by the second part of Theorem 1. Now, it is easy to see that each entry in $X^T X$ must appear a multiple of $(N - 1) = p$ times. \square

In Table 1, $E(s^2)$ -optimal SSDs with the best minimax properties found by NOA_k algorithms of Ryan and Bulutoglu (2006), constructed by Theorem 1 or Remark 1, and constructed by Theorem 2 or Remark 2 are listed. (The listed SSDs were obtained by using all orbits in \mathcal{F}_{N-2} and retaining SSDs that had the best minimax properties.) The letter h denotes that an SSD was constructed by the second part of Remark 1 or by applying Remark 2 to two SSDs constructed by the second part of Remark 1. All the SSDs corresponding to the last two sets of columns in Table 1 were constructed using GAP.

Table 1
 Properties of $E(s^2)$ -optimal SSDs constructed by NOA_k algorithms of Ryan and Bulutoglu (2006), Theorems 1 and 2 and Remarks 1 and 2

N	m	$E(s^2)$	NOA ₂		NOA ₄		NOA ₈		Thm. 1 or Remark 1.		Thm. 2 or Remark 2.		
			s_{\max}	$f_{s_{\max}}$	s_{\max}	$f_{s_{\max}}$	s_{\max}	$f_{s_{\max}}$	s_{\max}	$f_{s_{\max}}$	s_{\max}	$f_{s_{\max}}$	
10	18	5.8824	6	9	6	9	6	9	6	9	—	—	
10	36	8.5714	6	90	6	90	6	90	6	90	h	—	—
10	72	9.8592	6	468	6	468	6	468	6	468	—	—	—
12	22	6.8571	4	99	4	99	4	99	8	11	—	—	
12	55	10.6667	8	53	4	990	4	990	4	990	h	—	—
12	66	11.0769	8	96	4	1485	4	1485	—	—	8	55	h
12	110	11.8899	8	372	8	273	8	270	8	275	8	275	
12	132	12.0916	—	—	8	396	8	396	—	—	8	396	
12	220	12.4932	—	—	—	—	8	1589	—	—	8	1650	
14	13	4.0000	2	78	2	78	2	78	—	—	—	—	
14	26	7.8400	6	39	6	39	6	39	6	39	h	—	—
14	52	11.5294	10	9	6	312	6	312	10	26	—	—	
14	78	12.7273	10	35	—	—	—	—	6	819	h	10	39
14	104	13.3204	10	91	—	—	—	—	—	—	6	1560	h
14	130	13.6744	10	165	—	—	—	—	—	—	10	65	
14	156	13.9097	10	263	—	—	—	—	10	156	10	52	
14	182	14.0774	—	—	—	—	—	—	—	—	10	325	
14	208	14.2029	—	—	—	—	—	—	—	—	10	260	
14	234	14.3004	—	—	—	—	—	—	—	—	10	351	
14	312	14.4952	—	—	—	—	—	—	—	—	10	858	
18	34	9.8182	—	—	—	—	—	—	14	17	—	—	
18	68	14.5075	—	—	—	—	—	—	14	34	—	—	
18	102	16.0396	—	—	—	—	—	—	—	—	14	51	
18	136	16.8000	—	—	—	—	—	—	6	3672	h	—	—
18	170	17.2544	—	—	—	—	—	—	—	—	14	17	
18	204	17.5567	—	—	—	—	—	—	—	—	14	34	
18	272	17.9336	—	—	—	—	—	—	10	1496	10	1054	h
18	306	18.0590	—	—	—	—	—	—	—	—	14	17	
18	340	18.1593	—	—	—	—	—	—	—	—	14	34	
18	408	18.3100	—	—	—	—	—	—	—	—	10	3400	
18	544	18.4972	—	—	—	—	—	—	—	—	10	7072	
20	38	10.8108	—	—	—	—	—	—	16	19	—	—	
20	57	14.2857	—	—	—	—	—	—	8	95	h	—	—
20	76	16.0000	—	—	—	—	—	—	—	—	8	304	h
20	114	17.6991	—	—	—	—	—	—	8	1083	8	1083	h
20	171	18.8235	—	—	—	—	—	—	8	1710	h	—	—
20	190	19.0476	—	—	—	—	—	—	—	—	8	2394	h
20	228	19.3833	—	—	—	—	—	—	—	—	12	57	h
20	342	19.9414	—	—	—	—	—	—	12	513	12	171	h

NOA_k algorithms tend to produce SSDs having better minimax properties when k is increased. However, the NOA_k algorithms fail to find $E(s^2)$ -optimal SSDs as N and m get large. On the other hand it is possible to construct $E(s^2)$ -optimal SSDs for large values of N and m by Theorem 1 or Remark 1 or by Theorem 2 or Remark 2. By Theorem 6, the $E(s^2)$ -optimal SSDs constructed by Theorem 2 or Remark 1 have a certain structure. (In fact this structure is possessed by all k -circulant SSDs.) This structure may keep these SSDs from having the best minimax properties. This provides an explanation for the pattern in Table 1 as SSDs found via NOA_8 do not necessarily have this structure. Nonetheless, the theoretically constructed SSDs have very good minimax properties. For example, for many cases they still have better minimax properties than the $E(s^2)$ -optimal SSDs found by the NOA_2 algorithm or those constructed by SRS_4 algorithm of Ryan and Bulutoglu (2006).

3. Determining the number of factors

When $N - 1$ is an odd prime power, it is of theoretical and practical interest to determine the number of factors of all $E(s^2)$ -optimal SSDs that can be constructed using Theorems 1 and 2 or Remarks 1 and 2. By Theorem 4 and Lemma 2, this can be done by computing the number of size e orbits in \mathcal{F}_{N-2} for every even divisor e of $N - 2$. A brute force algorithm can be implemented to find all orbits of \mathcal{F}_{N-2} , but this becomes intangible as $N - 2$ gets larger. Next, a computationally efficient method is developed for determining the number of size e orbits in \mathcal{F}_q . First, represent each element of \mathcal{F}_q by ordering its elements from smallest to largest (mod q) (i.e., for $T = \{x_1, x_2, \dots, x_{q/2}\} \in \mathcal{F}_q$ and $x_1 < x_2 < \dots < x_{q/2} \pmod{q}$).

Definition 1. Let $T = \{x_1, x_2, \dots, x_{q/2}\}$ be a size $q/2$ subset of \mathbb{Z}_q such that $x_1 < x_2 < \dots < x_{q/2} \pmod{q}$. If $d_i = x_{i+1} - x_i \pmod{q}$ for $i = 1, 2, \dots, q/2$ and $x_{q/2+1} = x_1$, then the vector

$$d = \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_{q/2} \end{bmatrix}$$

is called the *difference vector* of T .

Let T and d be as in Definition 1. Then $\sum_{i=1}^{q/2} d_i = q$, the x_i , and the d_i completely determine T .

Lemma 3. Let $T = \{x_1, x_2, \dots, x_{q/2}\}$ and $T + r = \{y_1, y_2, \dots, y_{q/2}\}$ such that $x_1 < x_2 < \dots < x_{q/2}$ and $y_1 < y_2 < \dots < y_{q/2}$. Also, let d and d' be the difference vectors of T and $T + r$, respectively. Then

$$g^l \begin{bmatrix} x_1 + r \\ x_2 + r \\ \vdots \\ x_{q/2} + r \end{bmatrix} \equiv \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{q/2} \end{bmatrix} \pmod{q}$$

and $g^l d \equiv d' \pmod{q}$ for some $l \in \{0, 1, \dots, q/2 - 1\}$, where

$$g \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{q/2} \end{bmatrix} = \begin{bmatrix} x_{q/2} \\ x_1 \\ \vdots \\ x_{q/2-1} \end{bmatrix}$$

(i.e., g is the cyclic shift operator on the indices).

Proof. If r_i is the smallest integer such that $x_{q/2-i+1} + r_i \equiv 0 \pmod{4}$ for $i = 1, 2, \dots, q/2$, then

$$g^i \begin{bmatrix} x_1 + r_i \\ x_2 + r_i \\ \vdots \\ x_{q/2} + r_i \end{bmatrix} \equiv \begin{bmatrix} y'_1 \\ y'_2 \\ \vdots \\ y'_{q/2} \end{bmatrix} \pmod{q}$$

and $T + r_i + s = \{y'_1, y'_2, \dots, y'_{q/2}\}$, where $s < r_{i+1} - r_i$, $r_{q/2+1} = r_1$, and $y_1 < y_2 < \dots < y_{q/2}$. It is also clear that $g^i d \equiv d' \pmod{q}$. \square

Lemma 4. Let $T \in \mathcal{F}_q$ and g be the cyclic shift operator on the indices of a $q/2$ tuple. Let O_T be the orbit of T under the action of the group \mathbb{Z}_q^+ . Also, let \mathbf{d} be the difference vector of T and k be the smallest integer such that $g^k \mathbf{d} = \mathbf{d}$. Then, there exists $T_1, T_2, \dots, T_k \in O_T$ with difference vectors $g^0 \mathbf{d}, g^1 \mathbf{d}, \dots, g^{k-1} \mathbf{d}$, respectively, such that the first element of each T_i is 0. Furthermore, the difference vector of any $T' \in O_T$ is of the form $g^j \mathbf{d}$ for some $j \in \{0, 1, \dots, k-1\}$.

Proof. Note that for any $T = \{x_1, x_2, \dots, x_{q/2}\} \subset \mathbb{Z}_q, \bigcup_{i=1}^q \{x_1 + i, x_2 + i, \dots, x_{q/2} + i\} = \mathbb{Z}_q$. W.l.o.g. assume $x_1 = 0$ and $x_1 < x_2 < \dots < x_{q/2}$. If r_i is the smallest integer such that $x_{q/2-i+1} + r_i \equiv 0 \pmod{q}$ for $i = 1, 2, \dots, q/2$, then $\{T, T + r_1, T + r_2, \dots, T + r_{k-1}\}$, where $r_1 < r_2 < \dots < r_{k-1}$ is the desired $\{T_1, T_2, \dots, T_k\}$. The second part follows immediately from Lemma 3. \square

To find the number of length e orbits in \mathcal{F}_q for each even divisor e of q , start with

$$\sum_{i=1}^{q/2} d_i = q \quad \text{and} \quad d_i > 0. \tag{5}$$

Then the number of integer solutions to Eq. (5) is $\binom{q-1}{q/2-1}$. If \mathbf{d}_1 and \mathbf{d}_2 are two solutions to Eq. (5) such that $g^l \mathbf{d}_1 = \mathbf{d}_2$ for some $l \in \{0, 1, \dots, q/2-1\}$, then call \mathbf{d}_1 and \mathbf{d}_2 equivalent. Now, by Lemma 4, the number of orbits in \mathcal{F}_q is the same as the number of non-equivalent integer solutions to Eq. (5). Before describing a method to find all non-equivalent solutions to Eq. (5), the following definitions are needed.

Definition 2. Let $\Phi : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ be defined recursively by $\Phi(1) = 1$ and

$$\Phi(n) = \binom{2n-1}{n-1} - \sum_{n/d \in \mathbb{Z}^+, d \neq 1} \Phi(n/d). \tag{6}$$

Definition 3. Let g be cyclic shift operator on the indices of solutions to Eq. (5). The *period* of a solution \mathbf{d} to Eq. (5) is the smallest positive integer k such that $g^k \mathbf{d} = \mathbf{d}$.

Note that the period of a solution to Eq. (5) divides $q/2$. Using the function Φ and the period of a solution, a method for finding all non-equivalent solutions to Eq. (5) is provided in the next theorem.

Theorem 7. If α is a divisor of $q/2$, then the number of period α non-equivalent solutions to Eq. (5) is $\Phi(\alpha)/\alpha$. Furthermore, $\Phi(\alpha)/\alpha$ is the number of length 2α orbits in \mathcal{F}_q under the action of \mathbb{Z}_q .

Proof. If \mathbf{d} is a solution of period α or a divisor of α , then \mathbf{d} has the form

$$\mathbf{d} = \mathbf{1}_{q/(2\alpha)}^T \otimes (d_1, d_2, \dots, d_\alpha),$$

where $\mathbf{1}_{q/(2\alpha)}^T$ is a length $q/(2\alpha)$ row vector of +1s. Then the number of solutions that are either period α or a divisor of α is $\binom{2\alpha-1}{\alpha-1}$. Arguing the same way for all divisors of α shows that the number of solutions of period α is $\Phi(\alpha)$. Since there are $\alpha-1$ distinct equivalent solutions to a given period α solution, the number of non-equivalent period α solutions is $\Phi(\alpha)/\alpha$. The second part of the theorem can be proven by observing that a solution of the form

$$\mathbf{d} = \mathbf{1}_{q/(2\alpha)}^T \otimes (d_1, d_2, \dots, d_\alpha)$$

is the difference vector of some $T \in \mathcal{F}_q$ with $|O_T| = \sum_{i=1}^\alpha d_i = 2\alpha$. \square

Remark 3. Observe that the number of length 2α orbits in \mathcal{F}_q is $\Phi(\alpha)/\alpha$ which does not depend on q . Therefore, for any even divisor q of $N-2$ and any divisor α of $q/2$, the number of length 2α orbits in \mathcal{F}_{N-2} is the same as the number of length 2α orbits in \mathcal{F}_q .

By Theorems 4 and 7, Lemma 2, and the equivalence of an $E(s^2)$ -optimal SSD with N runs and $q(N - 1)$ factors for $q \in \mathbb{Z}^+$ to a BIBD($N - 1, q(N - 1), N/2 - 1$), the number of factors for N run $E(s^2)$ -optimal SSDs constructed by Theorems 1 and 2 and Remarks 1 and 2 can be determined by the following steps:

1. Factor $N - 2$.
2. Using Eq. (6) and starting with the prime divisors of $N - 2$, compute $\Phi(\alpha)$ and $\Phi(\alpha)/\alpha$ for all divisors α of $(N - 2)/2$. $\Phi(\alpha)/\alpha$ is the number of distinct length 2α orbits in \mathcal{F}_{N-2} .
3. For each divisor α of $(N - 2)/2$, by Theorem 1 each orbit of length 2α in \mathcal{F}_{N-2} corresponds to an $E(s^2)$ -optimal SSD with N runs and $2\alpha(N - 1)$ factors if $2\alpha \neq N - 2$. When $2\alpha = N - 2$, one needs to make sure that the design obtained is an SSD; $E(s^2)$ -optimality is guaranteed.
4. Let $\alpha_1 < \alpha_2 < \dots < \alpha_{t_1} = (N - 2)/2$ be all divisors of $(N - 2)/2$ such that $(N - 2)/(2\alpha_i)$ is odd, and let $\beta_1 < \beta_2 < \dots < \beta_{t_2}$ be all divisors of $(N - 2)/2$ such that $(N - 2)/(2\beta_i)$ is even. Let $\gamma_i = \phi(\alpha_i)/\alpha_i$ (for $i = 1, 2, \dots, t_1 - 1$) and $\theta_i = \phi(\beta_i)/\beta_i$ (for $i = 1, 2, \dots, t_2$) be the number of length $2\alpha_i$ and $2\beta_i$ orbits in \mathcal{F}_{N-2} , respectively. Let b be the number of length $N - 2$ orbits in \mathcal{F}_{N-2} and $\{B_l : l = 1, 2, \dots, b\}$ be the BIBD($N - 1, (N - 2)(N - 1), N/2 - 1$)s constructed by Theorem 1 by using length $N - 2$ orbits in \mathcal{F}_{N-2} . By second part of Remark 1, each B_l can be written as $B_l = B_l^1 \cup B_l^2$, where B_l^i are BIBD($N - 1, (N - 2)(N - 1)/2, N/2 - 1$)s. Let $\mathcal{E} = \{B_l^i : l = 1, 2, \dots, b, i = 1, 2\}$ be the collection of all such BIBD($N - 1, (N - 2)(N - 1)/2, N/2 - 1$)s. Let \mathcal{C} be a subset of \mathcal{E} with the maximum number of elements such that the BIBD obtained by taking the union of all elements of \mathcal{C} has distinct blocks. Let $\gamma_{t_1} = |\mathcal{C}|$. By Theorem 5, $\gamma_{t_1} \geq 2$. (it was empirically observed that $\gamma_{t_1} \geq 4$ for $N = 8, 10, 12, 14, 18$, and 20 .) Then the set

$$M = \left[\bigcup_{j=1}^{t_1} \bigcup_{0 \leq a_j \leq \gamma_j} \left\{ \sum_{i=1}^{t_1} \alpha_i a_i (N - 1) \right\} \right] \cup \left[\bigcup_{j=1}^{t_2} \bigcup_{0 \leq a_j \leq \theta_j} \left\{ \sum_{i=1}^{t_2} 2\beta_i a_i (N - 1) \right\} \right]$$

is all possible number of factors for N run $E(s^2)$ -optimal SSDs constructed by Theorems 1 and 2 and Remarks 1 and 2.

Note that the computation of γ_{t_1} requires taking the union of all subcollections of the B_l and checking if the resulting BIBD has distinct blocks. This is computationally expensive even for small values of N . However, if γ_{t_1} is replaced by a known lower bound for γ_{t_1} , then the union in Step 4 can be easily computed. If S is this set, then $M \supseteq S$. Hence, this method yields non-trivial subsets of M . Next, for $N = 14$ the set S is computed using the lower bound 4 for γ_{t_1} .

Example 1. (continued) First, $N - 2 = 12 = 2^2 \cdot 3$, and $\alpha_1 = 2, \alpha_2 = 6$ are all the divisors of $(N - 2)/2 = 6$ such that $(N - 2)/2\alpha_i$ is odd and $\beta_1 = 1, \beta_2 = 3$ are all the divisors of $(N - 2)/2 = 6$ such that $(N - 2)/2\beta_i$ is even. Note that $t_1 = t_2 = 2$. It is clear from Eq. (6) that $\phi(1) = 1, \phi(2) = \binom{3}{1} - 1 = 2$ and $\phi(3) = \binom{5}{2} - 1 = 9$; hence, $\gamma_1 = \phi(2)/2 = 1, 4 \leq \gamma_2, \theta_1 = \phi(1)/1 = 1$ and $\theta_2 = \phi(3)/3 = 3$. Then $S = S_1 \cup S_2$, where

$$S_1 = \left[\bigcup_{0 \leq a_1 \leq 1} \left\{ \sum_{i=1}^2 \alpha_i a_i (N - 1) \right\} \right] \cup \left[\bigcup_{0 \leq a_2 \leq 4} \left\{ \sum_{i=1}^2 \alpha_i a_i (N - 1) \right\} \right] \tag{7}$$

and

$$S_2 = \left[\bigcup_{0 \leq a_1 \leq 1} \left\{ \sum_{i=1}^2 \beta_i a_i (N - 1) \right\} \right] \cup \left[\bigcup_{0 \leq a_2 \leq 3} \left\{ \sum_{i=1}^2 \beta_i a_i (N - 1) \right\} \right]. \tag{8}$$

Hence, $S = \bigcup_{t=1}^{24} \{26t\}$.

The set S was computed using GAP for $N = 12, 14, 18$ and 20 by replacing γ_{t_1} with 4 and for the remaining values of N by replacing γ_{t_1} with 2 (see The GAP group, 2002). The results are summarized in Table 2. The last column $\binom{N-1}{N/2-1}$ is the maximum number of columns an N run SSD can have. The sequences $\{a_i\}_{i=0}^{992}, \{b_i\}_{i=0}^{1600103}$ in Table 2 are defined

Table 2
The elements of the set S

N	γ_{r_i}	S	$\binom{N-1}{N/2-1}$
10	2	$\bigcup_{t=1}^7 \{18t\}$	126
12	4	$\{11, 22, 55, 66, 77, 110, 121, 165, 176, 187, 220, 231, 242\}$	462
14	4	$\bigcup_{t=1}^{24} \{26t\}$	1716
18	4	$\bigcup_{t=1}^{51} \{34t\}$	24310
20	4	$\bigcup_{t=1}^{56} \{19t\}$	92378
24	2	$\{23, 46, 253, 276, 299, 506, 529, 552\}$	1352078
26	2	$\bigcup_{t=1}^{506} \{50t\}$	5200300
28	2	$\{27, 54, 351, 378, 702, 729, 756\}$	20058300
30	2	$\bigcup_{t=1}^{992} \{29a_t\}$	77558760
32	2	$\bigcup_{t=1}^{300} \{31t\}$	300540195
38	2	$\bigcup_{t=1}^{24780} \{74t\}$	17672631900
44	2	$\bigcup_{t=1}^{3492} \{43t\}$	1052049481860
48	2	$\{47, 94, 1081, 1128, 1175, 2162, 2209, 2256\}$	16123801841550
50	2	$\bigcup_{t=1}^{1358503} \{98t\}$	63205303218876
54	2	$\bigcup_{t=1}^{1600103} \{53b_t\}$	973469712824056

by $a_0 = 0, b_0 = 0,$

$$a_i - a_{i-1} = 2 \quad \text{if } i \text{ is not divisible by } 4,$$

$$a_i - a_{i-1} = 8 \quad \text{otherwise,}$$

$$b_i - b_{i-1} = 2 \quad \text{if } i \text{ is not divisible by } 4,$$

$$b_i - b_{i-1} = 20 \quad \text{otherwise.}$$

The results in Table 2 were obtained with little computational power. On the other hand obtaining these results by applying the construction in Theorem 1 would have been infeasible for $N \geq 20$ as this would have required computation of all orbits in \mathcal{F}_q for every even divisor q of $N - 2$ such that $q \neq N - 2$ for several modestly large N . Hence the theoretical results in this paper make it feasible to construct the set S in Table 2.

Acknowledgments

The author thanks Professor Bjorn Poonen for suggesting the initial step to prove Theorem 5, Professor John D. Dixon for providing GAP support that helped construct Table 2, and Professor Kenneth Ryan for helping during the preparation of this document. The author also thanks two anonymous referees for careful reading of the paper and suggestions that improved the presentation.

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the US Government.

References

Booth, E.H., Cox, D.R., 1962. Some systematic supersaturated designs. *Technometrics* 4, 489–495.
 Bulutoglu, D.A., Cheng, C.S., 2004. Construction of $E(s^2)$ -optimal supersaturated designs. *Ann. Statist.* 32, 1662–1678.
 Butler, N.A., Mead, R., Eskridge, K.M., Gilmour, S.G., 2001. A general method of constructing $E(s^2)$ -optimal supersaturated designs. *J. R. Stat. Soc. Ser. B Stat. Methodol.* 63, 621–632.
 Cheng, C.S., 1997. $E(s^2)$ -optimality of supersaturated designs. *Statist. Sinica* 7, 929–939.
 Eskridge, K.M., Gilmour, S.G., Mead, R., Butler, N., Travniccek, D.A., 2004. Large supersaturated designs. *J. Stat. Comput. Simulation* 74, 525–542.
 Li, W.W., Wu, C.F.J., 1997. Columnwise-pairwise algorithms with applications to the construction of supersaturated designs. *Technometrics* 39, 171–179.
 Lin, D.K.J., 1993. A new class of supersaturated designs. *Technometrics* 35, 28–31.

- Lin, D.K.J., 1995. Generating systematic supersaturated designs. *Technometrics* 37, 213–225.
- Liu, Y., Dean, A.M., 2004. k -circulant supersaturated designs. *Technometrics* 46, 32–43.
- Nguyen, N.K., 1996. An algorithmic approach to constructing supersaturated designs. *Technometrics* 38, 69–73.
- Nguyen, N.K., Cheng, C.S., 2006. New $E(s^2)$ -optimal supersaturated designs constructed from incomplete block designs. Preprint.
- Ryan, K.J., Bulutoglu, D.A., 2006. $E(s^2)$ -optimal supersaturated designs with good minimax properties. Preprint.
- Tang, B., Wu, C.F.J., 1997. A method for constructing supersaturated designs and its $E(s^2)$ -optimality. *Canad. J. Statist.* 25, 191–201.
- The GAP Group, 2002. GAP—Groups, algorithms, and programming, version 4.3. (<http://www.gap-system.org>).
- Wu, C.F.J., 1993. Construction of supersaturated designs through partially aliased interactions. *Biometrika* 80, 661–669.