Construction of sliced space-filling designs based on balanced sliced orthogonal arrays

Mingyao Ai[1], Bochuan Jiang[1,2], Kang Li[1]

[1]*Peking University and* [2]*Science and Technology on Complex Land Systems Simulation Laboratory*

Appendix: Proofs of Lemmas and Theorems

Proof of Lemma 2

Since $\boldsymbol{A}$ is a balanced $D(s_1, \lambda, s_1)$ and $\boldsymbol{C}_{(l_1,\ldots,l_\lambda)}(:, j) = \boldsymbol{A}(:, j) + \Gamma(1, l_j)$ for $j = 1, \ldots, \lambda$, we know that $\boldsymbol{C}_{(l_1,\ldots,l_\lambda)}$ is also a balanced $D(s_1, \lambda, s_1)$. From the formula (2.1), the label of the i-th row of $\boldsymbol{A}$ can be uniquely represented as $(b_{i0}, b_{i1}, \ldots, b_{i,\lambda-1})\boldsymbol{u}$ for $i = 1, \ldots, s_1$. Let $\boldsymbol{B}$ be the $s_1 \times \lambda$ matrix with $(b_{i0}, b_{i1}, \ldots, b_{i,\lambda-1})$ as the i-th row. Clearly, $\boldsymbol{A} = \boldsymbol{B}\boldsymbol{u}\boldsymbol{u}'$. By using Lemma 1 in Qian and Wu (2009), we have $\phi(\boldsymbol{A}) = \boldsymbol{B}\phi(\boldsymbol{u}\boldsymbol{u}')$.

Next we are ready to prove that $\phi(\boldsymbol{u}\boldsymbol{u}')$ has full rank over G. Note that $\phi(\alpha^i) = \beta^i$ for $i = 0, 1, \ldots, \lambda - 1$. By performing some row transformations, the matrix $\phi(\boldsymbol{u}\boldsymbol{u}')$ can be transfered to

$$\begin{pmatrix} 1 & \beta & \cdots & \beta^{\lambda-2} & \beta^{\lambda-1} \\ 0 & 0 & \cdots & 0 & \phi(\alpha^\lambda) - \beta^\lambda \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \phi(\alpha^\lambda) - \beta^\lambda & \cdots & \phi(\alpha^{2\lambda-3}) - \beta^{2\lambda-3} & \phi(\alpha^{2\lambda-2}) - \beta^{2\lambda-2} \end{pmatrix},$$

which has the same rank as $\phi(\boldsymbol{u}\boldsymbol{u}')$ over G. Suppose that α^λ is uniquely represented as $b_0 + b_1\alpha + \cdots + b_{\lambda-1}\alpha^{\lambda-1}$, where $b_i \in G$, $0 \le i \le \lambda - 1$. If $\phi(\alpha^\lambda) = \beta^\lambda$, then $\phi(\alpha^{\lambda+1}) = \phi(b_0\alpha + b_1\alpha^2 + \cdots + b_{\lambda-1}\alpha^\lambda) = b_0\beta + b_1\beta^2 + \cdots + b_{\lambda-1}\beta^\lambda = \beta\phi(\alpha^\lambda) = \beta^{\lambda+1}$. It can be further shown that $\phi(\alpha^j) = \beta^j$ for any j, which implies that ϕ only projects the element zero of F to zero of G, a contradiction. Hence, $\phi(\alpha^\lambda) \neq \beta^\lambda$ and $\phi(\boldsymbol{u}\boldsymbol{u}')$ has full rank over G. Note that $\boldsymbol{B}$ has no repeated rows. Thus, $\phi(\boldsymbol{A})$ also has no repeated rows and consists of all the s_2^λ possible λ-tuples from G, i.e., $\phi(\boldsymbol{A})$ is an $OA(s_2^\lambda, s_2^\lambda, \lambda)$. The part (ii) of Lemma 2 follows by noting

$\phi(\boldsymbol{v}_{(l_1,\ldots,l_\lambda)}) = \boldsymbol{0}$ for any $(l_1, \ldots, l_\lambda) \in Q^\lambda$.

Pick any two distinct λ-tuples $(l_1, \ldots, l_\lambda), (l'_1, \ldots, l'_\lambda) \in Q^\lambda$. Obviously, the i-th rows of $\boldsymbol{C}_{(l_1,\ldots,l_\lambda)}$ and $\boldsymbol{C}_{(l'_1,\ldots,l'_\lambda)}$ are distinct for $i = 1, \ldots, s_1$. Since $\phi(\boldsymbol{C}_{(l_1,\ldots,l_\lambda)}) = \phi(\boldsymbol{C}_{(l'_1,\ldots,l'_\lambda)}) = \phi(\boldsymbol{A})$ and $\phi(\boldsymbol{A})$ has no repeated rows, it can be shown that $\boldsymbol{C}_{(l_1,\ldots,l_\lambda)}$ and $\boldsymbol{C}_{(l'_1,\ldots,l'_\lambda)}$ have no same rows. Thus, $\boldsymbol{C}$ has no repeated rows and consists of all the s_1^λ possible λ-tuples from F, i.e., $\boldsymbol{C}$ is an $OA(s_1^\lambda, s_1^\lambda, \lambda)$. The proof of Lemma 2 is complete.

Proof of Theorem 1

Since any element of F can be uniquely represented in the expression (2.1), all the elements of $\boldsymbol{u'Z}$ are distinct and nonzero. By noting that $\boldsymbol{AZ}$ is the matrix obtained by taking the columns of $\boldsymbol{A}_0$ labeled with the elements of $\boldsymbol{u'Z}$, we know that $\boldsymbol{AZ}$ is a balanced $D(s_1, m, s_1)$. Since $\boldsymbol{C}_{(l_1,\ldots,l_\lambda)}\boldsymbol{Z} = \boldsymbol{AZ} + \boldsymbol{1}_{s_1}\boldsymbol{v}'_{(l_1,\ldots,l_\lambda)}\boldsymbol{Z}$, it can be shown that $\boldsymbol{C}_{(l_1,\ldots,l_\lambda)}\boldsymbol{Z}$ is also a balanced $D(s_1, m, s_1)$. So the part (ii) of Theorem 1 follows. Furthermore, because $\boldsymbol{H} = (\alpha_0, \ldots, \alpha_{s_1-1})' \oplus (\boldsymbol{C}_{(l_1,\ldots,l_\lambda)}\boldsymbol{Z})$, the part (i) of Theorem 1 follows easily from Lemma 1.

Suppose now any t columns of $\boldsymbol{Z}$ are linearly independent over G. Let $\boldsymbol{Z}_0$ be a $\lambda \times t$ submatrix of $\boldsymbol{Z}$. From Lemma 2 (ii), $\phi(\boldsymbol{C}_{(l_1,\ldots,l_\lambda)})$ is an $OA(s_2^\lambda, s_2^\lambda, \lambda)$. Thus, for any fixed t-tuple $\boldsymbol{\eta}$ from G, the number of times that $\boldsymbol{\eta}$ appears as a row in $\phi(\boldsymbol{C}_{(l_1,\ldots,l_\lambda)})\boldsymbol{Z}_0$ is equal to the number of λ-tuples $\boldsymbol{b}$'s from G such that $\boldsymbol{bZ}_0 = \boldsymbol{\eta}$. Since $\boldsymbol{Z}_0$ has full column rank over G, it is known that this number is equal to $s_2^{\lambda-t}$. Therefore, $\phi(\boldsymbol{C}_{(l_1,\ldots,l_\lambda)})\boldsymbol{Z}$ is an $OA(s_1, s_2^m, t)$ and the part (iii) of Theorem 1 follows.

Proof of Theorem 2

Since the part (i) of Theorem 2 can be easily obtained by following the similar proof of Theorem 1 (ii), here we need only to prove the part (ii) of Theorem 2.

Assume now that there is a $\lambda \times t$ submatrix of $\boldsymbol{Z}$, denoted by $\boldsymbol{Z}_0$, which has full column rank over G. It can be shown that $\boldsymbol{Z}_0$ also has full column rank over F. Otherwise, there exists a nonzero vector $(a_1, \ldots, a_t)'$ over F such that $\boldsymbol{Z}_0(a_1, \ldots, a_t)' = \boldsymbol{0}$. Note that each a_i can be uniquely represented in (2.1) as the form of $\boldsymbol{b}'_i\boldsymbol{u}$, where $\boldsymbol{b}_i$ is a λ-vector over G for $i = 1, \ldots, t$. Thus, we have $\phi(\boldsymbol{Z}_0(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_t)'\boldsymbol{uu}') = \boldsymbol{Z}_0(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_t)'\phi(\boldsymbol{uu}') = \boldsymbol{0}$. It is known from the proof of Lemma 2 that $\phi(\boldsymbol{uu}')$ has full rank over G. Therefore, $\boldsymbol{Z}_0(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_t)' = \boldsymbol{0}$, a contradiction.

From Lemma 2, we know that $\boldsymbol{C}$ is an $OA(s_1^\lambda, s_1^\lambda, \lambda)$ over F and $\phi(\boldsymbol{C}_{(l_1,\dots,l_\lambda)})$ is an $OA(s_2^\lambda, s_2^\lambda, \lambda)$ over G. Then the conclusion in the part (ii) of Theorem 2 can be proved similar to Theorem 1 (iii) and so the remainder of the proof is omitted here.

Proof of Theorem 3

From Theorem 1 (i), it is easy to see that the matrix $\boldsymbol{H}$ constructed in Method 1 has no repeated rows. Similar to the proof of Theorem 2, it can be shown that the rows of $\boldsymbol{Z}$ are also linearly independent over F. It is known from Lemma 2 that $\boldsymbol{C}$ has no repeated rows. So, the matrix $\boldsymbol{H} = \boldsymbol{C}\boldsymbol{Z}$ constructed in Method 2 also has no repeated rows. The similar conclusion for each projected slice can be obtained by following the above arguments again.

Proof of Lemma 3

When $\boldsymbol{Z}_2 = (\boldsymbol{I}_\lambda, \boldsymbol{1}_\lambda)$ with $\lambda \geq s_2$, the conclusion obviously holds.

Now suppose that there exist a $\lambda \times \lambda$ submatrix of $\boldsymbol{Z}_2$, denoted by $\boldsymbol{Z}_0$, and a nonzero vector $\boldsymbol{b} = (b_0, \dots, b_{\lambda-1})'$ over G such that $\boldsymbol{b}'\boldsymbol{Z}_0 = \boldsymbol{0}$. Let $\Psi(Y) = b_0 + b_1 Y + \cdots + b_{\lambda-1}Y^{\lambda-1}$.

Now consider the case of $\boldsymbol{Z}_2 = (\boldsymbol{e}_1, \boldsymbol{e}_\lambda, \boldsymbol{W}_\lambda)$. Note that $\boldsymbol{b}'\boldsymbol{Z}_2 = (\Psi(0), b_{\lambda-1}, \Psi(\beta), \dots, \Psi(\beta^{s_2-1}))$. If $\boldsymbol{e}_\lambda$ is a column of $\boldsymbol{Z}_0$, then $b_{\lambda-1} = 0$ and $\Psi(Y)$ has $\lambda - 1$ distinct roots over G, a contradiction. Otherwise, $\Psi(Y) = 0$ has λ distinct roots over G, a contradiction again. Thus, the above $\boldsymbol{Z}_0$ doesn't exist.

Next, we focus on the case of $\boldsymbol{Z}_2 = (\boldsymbol{I}_3, \boldsymbol{W}_3)$ with the conditions that $\lambda = 3$ and s_2 is even. Note that $\boldsymbol{b}'\boldsymbol{Z}_2 = (\Psi(0), b_1, b_2, \Psi(\beta), \dots, \Psi(\beta^{s_2-1}))$. From the previous paragraph, we need only to consider the situation when $\boldsymbol{e}_2$ is a column of $\boldsymbol{Z}_0$. Then $b_1 = 0$. If $\boldsymbol{e}_3$ is also a column of $\boldsymbol{Z}_0$, then $b_2 = 0$ and $b_0 = 0$, a contradiction. Otherwise, there exist two elements of G, say η_1 and η_2, satisfying $b_0 + b_2\eta_1^2 = b_0 + b_2\eta_2^2 = 0$. By using the fact $\eta_1^2 = \eta_2^2$ if and only if $\eta_1 = \eta_2$ when s_2 is even, we conclude that $b_0 = b_2 = 0$, a contradiction again. Thus, the above $\boldsymbol{Z}_0$ doesn't exist yet.

Finally, we consider the case of $\boldsymbol{Z}_2 = (\boldsymbol{W}_3', \boldsymbol{I}_{s_2-1})$ with the conditions that $\lambda = s_2 - 1$ and s_2 is even. Note that $\boldsymbol{b}'\boldsymbol{Z}_2 = (\boldsymbol{b}'\boldsymbol{W}_3', \boldsymbol{b}')$. If $\boldsymbol{Z}_0 = \boldsymbol{I}_{s_2-1}$, then $\boldsymbol{b} = \boldsymbol{0}$, a contradiction. Otherwise, without loss of generality, suppose the last

$s_2 - 2 - k$ columns of $\boldsymbol{I}_{s_2-1}$ are involved in $\boldsymbol{Z}_0$, where $0 \le k \le 2$. Then $b_i = 0$ for $k < i \le s_2 - 2$. Obtain a matrix $\boldsymbol{W}$ by collecting the $k+1$ columns of $\boldsymbol{W}_3'$ involved in $\boldsymbol{Z}_0$. Then $\boldsymbol{b}'\boldsymbol{W} = 0$ and $(b_0, \ldots, b_k)\boldsymbol{W}^{(k+1)} = 0$, where $\boldsymbol{W}^{(k+1)}$ is the submatrix obtained by taking the first $k+1$ rows of $\boldsymbol{W}$. It can be easily verified that any $(k+1) \times (k+1)$ submatrix of $\boldsymbol{W}_3$ has full rank over G for $0 \le k \le 2$ when s_2 is even. Thus, $b_i = 0$ for $0 \le i \le k$, a contradiction again. So, the above $\boldsymbol{Z}_0$ doesn't exist yet.

In all, the conclusion in Lemma 3 holds for different generator matrices $\boldsymbol{Z}_2$ in (4.2). The proof is complete.

Proof of Lemma 4

By noting that $\boldsymbol{B}_j$ is a subarray of the multiplication table of F, the part (i) of Lemma 4 follows. Recall that $\boldsymbol{\Gamma}(:,1)$ is a permutation of all elements in $F_0 = \{a_0 + a_1 x + \cdots + a_{u_2-1}x^{u_2-1} | a_j \in GF(p)\}$. From Lemma 2 in Qian and Wu (2009), we know $\varphi(\boldsymbol{B}_{11}) = \varphi(\boldsymbol{\Gamma}(:,1))\varphi(\boldsymbol{\Gamma}(:,1))'$ for $u_1 \ge 2u_2 - 1$ and thus $\varphi(\boldsymbol{B}_{11})$ is a $D(s_2, s_2, s_2)$. For $1 \le k_1 < k_2 \le q$, from the formula (2.5) we have $\varphi(\boldsymbol{B}_{ij}(:,k_1)) - \varphi(\boldsymbol{B}_{ij}(:,k_2)) = \varphi(\boldsymbol{B}_{11}(:,k_1)) - \varphi(\boldsymbol{B}_{11}(:,k_2)) + \varphi(\boldsymbol{\Gamma}(k_1,1)c_i(x) - \boldsymbol{\Gamma}(k_2,1)c_i(x))$. Hence, $\varphi(\boldsymbol{B}_{ij})$ is also a $D(s_2, s_2, s_2)$ for $i, j = 1, \ldots, q$.

Proof of Theorem 9

Since $\boldsymbol{H} = (\boldsymbol{\Gamma}(:,1)', \ldots \boldsymbol{\Gamma}(:,q)')' \oplus \boldsymbol{B}_2$, the part (i) of Theorem 9 follows from Lemma 1 and Lemma 4. Note that $\varphi(\boldsymbol{B}_{j2})$ is a $D(s_2, s_2, s_2)$ and $\varphi(\boldsymbol{\Gamma}(:,i))$ is an $OA(s_2, s_2^1, 1)$. By following Lemma 1, we know $\varphi(\boldsymbol{H}_{ij})$ is an $OA(s_2^2, s_2^{s_2}, 2)$ for $i, j = 1, \ldots, q$.

Let $deg\{f(x)\}$ denote the degree of a polynomial $f(x) \in F$, or more precisely the polynomial $f(x)$ modulo $p_1(x)$. If two elements of F are in the same column of $\boldsymbol{\Gamma}$, from the formula (2.5) we know the degree of their difference is less than u_2. Now partition the elements of $\boldsymbol{\Gamma}(:,1)$ into p groups, each of size $q = s_1/s_2 = p^{u_2-1}$, according to the rule that any two elements $f_1(x)$ and $f_2(x)$ of $\boldsymbol{\Gamma}(:,1)$ are in the same group if and only if $deg\{f_1(x) - f_2(x)\} \le u_2 - 2$. Suppose $\boldsymbol{\Gamma}(l_1,1), \boldsymbol{\Gamma}(l_2,1), \ldots, \boldsymbol{\Gamma}(l_q,1)$ are from the same group. For $1 \le k \le s_2$, we have $\boldsymbol{B}_{j2}(l_1,k) - \boldsymbol{B}_{j2}(l_2,k) = [\boldsymbol{\Gamma}(l_1,1) - \boldsymbol{\Gamma}(l_2,1)][\boldsymbol{\Gamma}(k,1) + c_2(x)]$, where $deg\{c_2(x)\} = u_2$. Then $deg\{\boldsymbol{B}_{j2}(l_1,k) - \boldsymbol{B}_{j2}(l_2,k)\} \ge u_2$ and $\boldsymbol{B}_{j2}(l_1,k)$ and $\boldsymbol{B}_{j2}(l_2,k)$ are in different columns of $\boldsymbol{\Gamma}$. As a result, $\boldsymbol{B}_{j2}(l_1,k), \ldots, \boldsymbol{B}_{j2}(l_q,k)$ are in distinct columns of $\mathbf{\Gamma}$ and thus each column of $\mathbf{\Gamma}$ contains exactly p elements of $\boldsymbol{B}_{j2}(:,k)$. From $\boldsymbol{H}_{ij}(:,k) = \mathbf{\Gamma}(:,i) \oplus \boldsymbol{B}_{j2}(:,k) = \mathbf{\Gamma}(:,1) \oplus \boldsymbol{B}_{j2}(:,k) + c_i(x)$, it can be easily verified that $\boldsymbol{H}_{ij}(:,k)$ is balanced for $i, j = 1, \ldots, q$. The proof is complete.

Proof of Theorem 10

Since the k-th elements of $\boldsymbol{u}_{i1}, \ldots, \boldsymbol{u}_{iq}$ form a permutation of $\{1, \ldots, q\}$ for $k = 1, \ldots, t$, it is easy to see that each $\boldsymbol{H}_i$ is balanced for $i = 1, \ldots, q^{t-1}$. For any $(l_1, \ldots, l_t) \in Q^t$, by noting that the first t columns of $\rho(\boldsymbol{H}_{(l_1,\ldots,l_t)})$ have each of the s_2^t possible t-tuples from G as a row and the last column is the sum of the first t columns, we know that $\rho(\boldsymbol{H}_{(l_1,\ldots,l_t)})$ is an $OA(s_2^t, s_2^{t+1}, t)$. The proof is complete.

Proof of Theorem 11

The part (ii) of Theorem 11 follows by noting that $\rho(\boldsymbol{A}) = \boldsymbol{A}_0$ and $\rho(\boldsymbol{v}_{(l_1,\ldots,l_t)}) = 0$ for any $(l_1, \ldots, l_t) \in Q^t$. Since any $s_2^t \times t$ submatrix of $\boldsymbol{H}_{(l_1,\ldots,l_t)}$ or $\rho(\boldsymbol{H}_{(l_1,\ldots,l_t)})$ has no repeated rows, it can be shown that any $s_1^t \times t$ submatrix of $\boldsymbol{H}$ has no repeated rows and thus consists of all the s_1^t possible t-tuples from F, i.e., $\boldsymbol{H}$ is an $OA(s_1^t, s_1^{t+1}, t)$.