AIMS Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 7(3): 4376–4385.
DOI: 10.3934/math.2022243
Received: 19 July 2021
Revised: 01 December 2021
Accepted: 12 December 2021
Published: 21 December 2021

Research article

Construction of random pooling designs based on singular linear space over finite fields

Xuemei Liu* **and Yazhuo Yu**

College of Science, Civil Aviation University of China, Tianjin, 300300, China

* **Correspondence:** Email: xm-liu771216@163.com; Tel: +8613820548321.

Abstract: Faced with a large number of samples to be tested, if there are requiring to be tested one by one and complete in a short time, it is difficult to save time and save costs at the same time. The random pooling designs can deal with it to some degree. In this paper, a family of random pooling designs based on the singular linear spaces and related counting theorems are constructed. Furtherly, based on it we construct an α-*almost* d^e-disjunct matrix and an α-*almost* $(d, r, z]$-disjunct matrix, and all the parameters and properties of these random pooling designs are given. At last, by comparing to Li's construction, we find that our design is better under certain condition.

Keywords: singular linear space; random pooling designs; α-*almost* d-disjunct matrix; error-tolerant
Mathematics Subject Classification: 05B30

1. Introduction

Pooling designs have a wide range of applications in biomolecular fields such as DNA library screening. Given some items with defects, divide the items into several subsets, and each subset is called a pool. The ultimate goal of pooling designs is to identify all defectives with the least number of tests. There are two possibilities for the test-outcome: One is negative if there are no defects contained in the pool, otherwise positive. As for group testing, if all pool tests are carried out simultaneously and the test-outcome of each pool will not affect each other, such group testing is called nonadaptive. This kind of test algorithm is suitable for the case of more experimental objects, which can greatly reduce the time required for testing (see Macula [1]).

Generally, d^z-disjunct matrix is the mathematical model of nonadaptive group testing, also called pooling designs. We typically use a $\{0, 1\}$ matrix $M = (a_{ij})$ to present pooling design, whose columns are in association to items and rows are in association to pools. Cell $a_{ij} = 1$ exhibits that the i th pool contains the j th item, otherwise $a_{ij} = 0$. A $(0, 1)$ matrix M is regarded as d^z-disjunct matrix if for any column C_0 and any d other columns $C_1, \cdots, C_d$, there exist at least z rows with a 1 in C_0 and 0 in all the other d columns.

The random group testing theory is a new branch of combinatorial group testing theory. Similar to pooling designs, the random pooling designs are used to screen the defect items in a large number of samples to be tested with the minimum number of tests. A range of possible performance measures is considered in the random pooling designs, including the expected numbers of unresolved positive and negative items, and the probability of a one-pass solution (i.e., the probability that the samples to be tested does not contain defective items). Thus, the random pooling designs optimizes the experiment to a certain extent.

Macula et al. firstly proposed the random group testing model in 2004. The random pooling designs for k-complexes and k_1-complexes are further constructed by using the α-*almost* k-disjunct matrices (see [2, 3]). In 2009, Lang et al. propose the definition of α-*almost* k^e-disjunct matrix, which is an error-tolerant design (see [4]). In 2018, Shi and et al. construct random pooling designs based on the finite related structures, and propose the definition of α-*almost* $(d, r, z]$-disjunct matrix in [5]. In 2019, Li et al. randomized the binary superposition code $M_q(n, k, d)$ and obtain new random pooling designs in [6]. Inspired by [5] and [6], we construct random pooling designs based on singular linear spaces.

We introduce some concepts and notations of random pooling designs for our following constructions in Section 2. In Section 3, based on the pooling design constructed by Theorem 3.1, we obtain three random pooling designs by means of the non-containment relationship of subspaces in singular linear space over finite fields. All the parameters and properties are given in Theorems 3.5–3.8. In Section 4, by comparing our α to Li's [6] parameters, we draw the conclusion that our design is superior to Li's under certain condition.

2. Preliminaries

In this section, we will introduce some propositions about random pooling designs and singular linear space.

Definition 2.1. [2] *Let M be $n \times t$ $\{0, 1\}$ matrix and let $\{a_v(i)\}$, where $1 \leq i \leq n$ and $1 \leq v \leq t$, be the column vectors of M. Let E be the event that a d-set of columns $\{a_{v_s}(i)\}_{s=1}^{d}$ has $a_v(i) \leq \bigvee_{s=1}^{d} \{a_{v_s}(i)\}$ with $a_v(i) \notin \{a_{v_s}(i)\}_{s=1}^{d}$. Let $0 < \alpha \leq 1$ be a real number. Given the uniform distribution on the d-set of columns of M, we say that M is α-almost d-disjunct if $Prob(E) \leq$ 1-α.*

Definition 2.2. [4] *Let M be $n \times t$ $\{0, 1\}$ matrix and let $\{C_v(i)\}$, where $1 \leq i \leq n$ and $1 \leq v \leq t$, be the column vectors of M. Let E be the event that a d-set of columns $\{C_{v_j}(i)\}_{j=1}^{d}(i \in \{1, 2, \cdots, n\})$ has at least $e + 1$ rows that are 1 in $C_v(i)$ and 0 in $\bigvee_{j=1}^{d} C_j(i)$, with $C_v(i) \notin \{C_{v_j}(i)\}_{j=1}^{d}$. Let $0 < \alpha \leq 1$ be a real number. Given the uniform distribution on the d-set of columns of M, we say that M is α-almost d^e-disjunct if $Prob(E) \geq \alpha$.*

Definition 2.3. [5] *Let M be $n \times t$ $\{0, 1\}$ matrix and let $\{C_v(i)\}$, where $1 \leq i \leq n$ and $1 \leq v \leq t$, be the column vectors of M. Let E be the event that an $(d + r)$-set of columns $\{C_{v_j}(i)\}_{j=1}^{d+r}$ $(i \in \{1, 2, \cdots, n\})$ has at least z rows that are 1 in $\bigwedge_{j=1}^{r} C_{v_j}(i)$ and 0 in $\bigvee_{j=r+1}^{r+d} C_j(i)$. Let $0 < \alpha \leq 1$ be a real number. Given the uniform distribution on the $(d + r)$-set of columns of M, we say that M is α-almost $(d, r, z]$-disjunct if $Prob(E) \geq \alpha$.*

Next, we will introduce some concepts and notations of the singular linear space for our following construction (see [7, 8]).

$\mathbb{F}_q$ is a finite field with q elements, where q is a prime power.

Let $\mathbb{F}_q^{(n+l)}$ denote the $(n+l)$-dimensional row vector space over $\mathbb{F}_q$, where n, l are two non-negative integers. The set of all $(n+l) \times (n+l)$ nonsingular matrices over $\mathbb{F}_q$ have the form

$$\begin{pmatrix} T_{11} & T_{12} \\ 0 & T_{22} \end{pmatrix},$$

forms a group under matrix multiplication, where T_{11} and T_{22} are nonsingular $n \times n$ and $l \times l$ matrices respectively. This kind of group is called the singular general linear group of degree $n+l$ over $\mathbb{F}_q$ and denoted as $GL_{n+l,n}(\mathbb{F}_q)$.

Suppose P is an m-dimensional subspace of $\mathbb{F}_q^{(n+l)}$, and use the same letter P to represent the matrix representation of the subspace P. The following is the definition of the action of $GL_{n+l,n}(\mathbb{F}_q)$ on $\mathbb{F}_q^{(n+l)}$:

$$\mathbb{F}_q^{(n+l)} \times GL_{n+l,n}(\mathbb{F}_q) \to \mathbb{F}_q^{(n+l)}$$

$$((x_1, \cdots, x_n, x_{n+1}, \cdots, x_{n+l}), T) \mapsto (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{n+l})T.$$

The above action is transitive on the set of all the subspaces with the same dimension. The vector space $\mathbb{F}_q^{(n+l)}$ together with the above group action, is called the $(n+l)$-dimensional singular linear space over $\mathbb{F}_q$ (see Wang et al. [7]).

Definition 2.4. [7] *Let E be the l-dimensional subspace of $\mathbb{F}_q^{(n+l)}$ generated by $e_{n+1}, e_{n+2}, \cdots, e_{n+l}$ and P be an m-dimensional subspace of $\mathbb{F}_q^{(n+l)}$. Then P is type (m, k) if $dim(P \cap E) = k$.*

Next we introduce some counting theorems of singular linear spaces $\mathbb{F}_q^{(n+l)}$.

Let $\mathcal{M}(m, k; n+l, n)$ denote the set of all subspaces of type (m, k) in $\mathbb{F}_q^{(n+l)}$, and let $N(m, k; n+l, n)$ denote the size of $\mathcal{M}(m, k; n+l, n)$.

Proposition 2.5. (Wan [8], Corollary 1.9) *Let $0 \le k \le m \le n$, then the number of m-dimensional vector subspaces containing a given k-dimensional vector subspace $\mathbb{F}_q^n$ is equal to $\begin{bmatrix} n-k \\ m-k \end{bmatrix}_q$.*

Proposition 2.6. (Wan [8], Lemma 2.1) *$\mathcal{M}(m, k; n+l, n)$ is non-empty if and only if $0 \le k \le l$ and $0 \le m-k \le n$. Moreover, if $\mathcal{M}(m, k; n+l, n)$ is non-empty, then if forms an orbit of subspaces under $GL_{n+l,n}(\mathbb{F}_q)$ and*

$$N(m, k; n+l, n) = q^{(m-k)(l-k)} \begin{bmatrix} n \\ m-k \end{bmatrix}_q \begin{bmatrix} l \\ k \end{bmatrix}_q.$$

For a fixed subspace P of type (m, k) in $\mathbb{F}_q^n$, let $\mathcal{M}(m_1, k_1; m, k; n+l, n)$ denote the set of all the subspaces of type (m_1, k_1) contained in P, and let $N(m_1, k_1; m, k; n+l, n) = |\mathcal{M}(m_1, k_1; m, k; n+l, n)|$. By the transitivity of $GL_{n+l,n}(\mathbb{F}_q)$ on the set of subspaces of the same type, $N(m_1, k_1; m, k; n+l, n)$ is independent of the particular choice of the subspace P of type (m, k).

Proposition 2.7. (Wan [8], Lemma 2.2) *$\mathcal{M}(m_1, k_1; m, k; n+l, n)$ is non-empty if and only if $0 \le k_1 \le k \le l$ and $0 \le m_1 - k_1 \le m-k \le n$. Moreover, if $\mathcal{M}(m_1, k_1; m, k; n+l, n)$ is non-empty, then*

$$N(m_1, k_1; m, k; n+l, n) = q^{(m_1-k_1)(k-k_1)} \begin{bmatrix} m-k \\ m_1-k_1 \end{bmatrix}_q \begin{bmatrix} k \\ k_1 \end{bmatrix}_q.$$

3. The construction of random pooling designs

In this section, we will propose some random pooling designs. Firstly, the construction of the binary matrix is given as follows.

Theorem 3.1. [9] *For* $max\{0, r+m-n\} \leq j \leq r$ *and* $m \leq n$, *let* P_0 *be a given* m*-dimensional subspace of* $\mathbb{F}_q^n$ *and let* Q_0 *be a given* j*-dimensional subspace of* $\mathbb{F}_q^n$ *with* $Q_0 \subseteq P_0$. *Then the number of* r*-dimensional subspaces of* $\mathbb{F}_q^n$ *intersecting* P_0 *at* Q_0 *is* $f(j, r, n; m) = q^{(r-j)(m-j)} \begin{bmatrix} n-m \\ r-j \end{bmatrix}_q$. *Moreover, for the integer* $0 \leq \alpha \leq n+j-m-r$, *the function* $f(j, r, n; m)$ *about* α *is decreasing.*

Definition 3.2. *Given integers* i, r, m, k, n, l *with* $0 \leq k \leq l$, $0 \leq m-k \leq n$ *and* $0 \leq i \leq r \leq m-k-2$. *Let* $M_q(i; r, 0; m, k; n+l, n)$ *be the binary matrix whose rows are indexed by* $\mathcal{M}(r, 0; n+l, n)$ *and columns are indexed by* $\mathcal{M}(m, k; n+l, n)$. $M_q(i; r, 0; m, k; n+l, n)$ *has a* 1 *in row* h *and column* j *if and only if* $dim(A \cap B) = i$, *where* A *is the* h*-th subspace and* B *is the* j*-th subspace, otherwise* 0.

Theorem 3.3. *Let* $R = \mathcal{M}(r, 0; n+l, n)$, $S = \mathcal{M}(m, k; n+l, n)$ *are the sample spaces composed of all rows and all columns of the binary matrix* $M_q(i; r, 0; m, k; n+l, n)$ *respectively. Now we randomly select any* N *rows from* R *and any* t *columns from* S *to form a sub-matrix* $M_q^s(i; r, 0; m, k; n+l, n)$. *Let* E_1 *be a random event that the sub-matrix* $M_q^s(i; r, 0; m, k; n+l, n)$ *has a* 1 *in row* h *and column* j. *And let* E_0 *be an random event that the sub-matrix* $M_q^s(i; r, 0; m, k; n+l, n)$ *has a* 0 *in row* h *and column* j.

According to the above definitions, we have

$$\begin{aligned} P(E_1) &= \frac{q^{(m-i)(r-i)} \begin{bmatrix} n+l-r \\ m-i \end{bmatrix}_q \times q^{(m-i)(r-i)} \begin{bmatrix} n+l-m \\ r-i \end{bmatrix}_q}{N(r, 0; n+l, n) \times N(m, k; n+l, n)}, \\ P(E_0) &= 1 - P(E_1). \end{aligned}$$

Proof. *By the above Theorem 3.1 and Definition 3.2, we can know that the binary matrix* $M_q(i; r, 0; m, k; n+l, n)$ *is an* $N(r, 0; n+l, n) \times N(m, k; n+l, n)$ *matrix with row weight* $q^{(m-i)(r-i)} \begin{bmatrix} n+l-r \\ m-i \end{bmatrix}_q$, *and with column weight* $q^{(m-i)(r-i)} \begin{bmatrix} n+l-m \\ r-i \end{bmatrix}_q$. *Hence there are a total of* $N(r, 0; n+l, n) \times N(m, k; n+l, n)$ *elements in the matrix* $M_q(i; r, 0; m, k; n+l, n)$, *of which the number of* 1 *is* $q^{(m-i)(r-i)} \begin{bmatrix} n+l-r \\ m-i \end{bmatrix}_q \times q^{(m-i)(r-i)} \begin{bmatrix} n+l-m \\ r-i \end{bmatrix}_q$.

Then we have

$$P(E_1) = \frac{q^{(m-i)(r-i)} \begin{bmatrix} n+l-r \\ m-i \end{bmatrix}_q \times q^{(m-i)(r-i)} \begin{bmatrix} n+l-m \\ r-i \end{bmatrix}_q}{N(r, 0; n+l, n) \times N(m, k; n+l, n)},$$

Obviously, E_0 *is the opposite event of* E_1. *Hence,* $P(E_0) = 1 - P(E_1)$.

Next we will simplify $P(E_1)$.

$$P(E_1)$$

$$= \frac{q^{(m-i)(r-i)}\begin{bmatrix} n+l-r \\ m-i \end{bmatrix}_q \times q^{(m-i)(r-i)}\begin{bmatrix} n+l-m \\ r-i \end{bmatrix}_q}{N(r,0;n+l,n)\times N(m,k;n+l,n)}$$

$$= \frac{q^{(m-i)(r-i)}\begin{bmatrix} n+l-r \\ m-i \end{bmatrix}_q \times q^{(m-i)(r-i)}\begin{bmatrix} n+l-m \\ r-i \end{bmatrix}_q}{q^{rl}\begin{bmatrix} n \\ r \end{bmatrix}_q \times q^{(m-k)(l-k)}\begin{bmatrix} n \\ m-k \end{bmatrix}_q \begin{bmatrix} l \\ k \end{bmatrix}_q}$$

$$= \frac{q^{(m-i)(r-i)}\frac{\prod_{j=(n+l-r)-(m-i)+1}^{n+l-r}(q^j-1)}{\prod_{j=1}^{m-i}(q^j-1)} \times q^{(m-i)(r-i)}\frac{\prod_{j=(n+l-m)-(r-i)+1}^{n+l-m}(q^j-1)}{\prod_{j=1}^{r-i}(q^j-1)}}{q^{rl}\frac{\prod_{j=n-r+1}^{n}(q^j-1)}{\prod_{j=1}^{r}(q^j-1)} \times q^{(m-k)(l-k)}\frac{\prod_{j=n-(m-k)+1}^{n}(q^j-1)}{\prod_{j=1}^{m-k}(q^j-1)} \times \frac{\prod_{j=l-k+1}^{l}(q^j-1)}{\prod_{j=1}^{k}(q^j-1)}}$$

$$= \frac{\frac{\prod_{j=(n+l-r)-(m-i)+1}^{n+l-r}(q^{r+j-i}-q^{r-i})}{\prod_{j=1}^{m-i}(q^j-1)} \times \frac{\prod_{j=(n+l-m)-(r-i)+1}^{n+l-m}(q^{m+j-i}-q^{m-i})}{\prod_{j=1}^{r-i}(q^j-1)}}{\frac{\prod_{j=n-r+1}^{n}(q^{l+j}-q^l)}{\prod_{j=1}^{r}(q^j-1)} \times \frac{\prod_{j=n-(m-k)+1}^{n}(q^{l+j-k}-q^{l-k})}{\prod_{j=1}^{m-k}(q^j-1)} \times \frac{\prod_{j=l-k+1}^{l}(q^j-1)}{\prod_{j=1}^{k}(q^j-1)}}$$

$$< (\frac{q^{n+l-m+1}-q^{r-i}}{q-1})^{m-i}\cdot(\frac{q^{n+l-r+1}-q^{m-i}}{q-1})^{r-i}\cdot(\frac{q^r}{q^{n+l}-q^l})^r\cdot(\frac{q^{m-k}}{q^{n+l-k}-q^{l-k}})^{m-k}\cdot(\frac{q^k}{q^l-1})^k$$

$$< q^{(m+r-2n-2l)i+(n-m+k)k+1}.$$

For the sake of convenience, we let $P(E_1) < q^\delta$, with $\delta = (m + r - 2n - 2l)i + (n - m + k)k + 1$ and $\delta < 0$. Based on Theorem 3.3, a family of random pooling design is given as follows.

Theorem 3.4. *Given $\delta = (m + r - 2n - 2l)i + (n - m + k)k + 1$ and $\delta < 0$. The probability that an $N \times t$ random sub-matrix $M_q^s(i; r, 0; m, k; n + l, n)$ is a d-disjunct matrix is at least*

$$(d+1)\begin{pmatrix} t \\ d+1 \end{pmatrix}[1 - q^\delta(1-q^\delta)^d]^N.$$

Proof. *Select $d + 1$ columns $\{a_{v_s}(i)\}_{s=1}^d$ from t columns of matrix $M_q^s(i; r, 0; m, k; n + l, n)$ randomly. Let E be a random event that the matrix $M_q^s(i; r, 0; m, k; n + l, n)$ has a row $r_i (i = 1, 2, \cdots, N)$ that are 1 in $a_{v_0}(i)$ and 0 in $\bigvee_{j=1}^{d} a_{v_j}(i)$. Then the probability of event E is*

$$P(E) = P(E_1)P^d(E_0).$$

There are a total of $(d+1)\begin{pmatrix} t \\ d+1 \end{pmatrix}$ ways to select $d+1$ columns randomly from $M_q^s(i; r, 0; m, k; n + l, n)$. Hence, the probability of random event E' that the above row does not exist in $M_q^s(i; r, 0; m, k; n + l, n)$ is

$$P(E') = (d+1)\begin{pmatrix} t \\ d+1 \end{pmatrix}[1 - P(E_1)P^d(E_0)]^N.$$

Since

$$P(E_1) = \frac{q^{(m-i)(r-i)}\begin{bmatrix} n+l-r \\ m-i \end{bmatrix}_q \times q^{(m-i)(r-i)}\begin{bmatrix} n+l-m \\ r-i \end{bmatrix}_q}{N(r,0;n+l,n)\times N(m,k;n+l,n)},$$

There we have

$$P(E') = (d+1)\binom{t}{d+1}[1-P(E_1)P^d(E_0)]^N$$
$$< (d+1)\binom{t}{d+1}[1-q^{\delta}(1-q^{\delta})^d]^N$$

Let $K = [1-q^{\delta}(1-q^{\delta})^d]$. *Obviously,* $0 < K < 1$. *According to* [8] *we have*

$$N \geq -log_K[(d+1)\binom{t}{d+1}] \geq dlog_K(d+1) - (d+1)log_K t.$$

In other words, there is a d-disjunct matrix in the sub-matrix $M_q^s(i;r,0;m,k;n+l,n)$ *when satisfying* $N \geq -log_K[(d+1)\binom{t}{d+1}] \geq dlog_K(d+1)-(d+1)log_K t$. *Hence, the probability that the matrix* $M_q^s(i;r,0;m,k;n+l,n)$ *is a d-disjunct matrix is at least*

$$(d+1)\binom{t}{d+1}[1-q^{\delta}(1-q^{\delta})^d]^N.$$

For convenience, the following δ all satisfying $\delta = (m+r-2n-2l)i + (n-m+k)k + 1$ and $\delta < 0$.

Theorem 3.5. *The random matrix* $M_q^s(i;r,0;m,k;n+l,n)$ *is an* α*-almost d-disjunct matrix when* $N \geq dlog_K(d+1) - (d+1)log_K t$*, where*

$$\alpha = (d+1)\binom{t}{d+1}[1-q^{\delta}(1-q^{\delta})^d]^N.$$

Proof. *It can be directly obtained by Theorem 3.3 and Definition 2.2.*

Next, based on Theorem 3.3, we will give two family of random pooling designs with error-tolerance.

Theorem 3.6. *The random matrix* $M_q^s(i;r,0;m,k;n+l,n)$ *is an* α*-almost* d^e*-disjunct matrix, where*

$$\alpha = (d+1)\binom{t}{d+1}[q^{\delta}(1-q^{\delta})^d]^{e+1}.$$

Proof. *Select d columns* $\{a_{v_j}(i)\}_{j=1}^d$ *from t columns of the matrix* $M_q^s(i;r,0;m,k;n+l,n)$ *randomly. Let E be the event that the matrix* $M_q^s(i;r,0;m,k;n+l,n)$ *has at least* $e+1$ *rows that are* 1 *in* $a_{v_0}(i)$ *and* 0 *in* $\bigvee_{j=1}^{d} a_{v_j}(i)$*, with* $a_{v_0}(i) \notin \{a_{v_j}(i)\}_{j=1}^d$*. According to Theorem 3.5, we have*

$$P(\overline{E'}) = P\{a_{v_0}(i) = 1 \text{ and } C_1(i) = \cdots = C_d(i) = 0,\ \exists\, i \in [N]\} = P(E_1)P^d(E_0).$$

Hence, the probability that there are at least $e+1$ *rows so that* $a_{v_0}(i) > \bigvee_{j=1}^{d} a_{v_j}(i)$ *in* d *columns is* $[P(E_1)P^d(E_0)]^{e+1}$.

There we have

$$P(E) \geq (d+1)\binom{t}{d+1}[q^{\delta}(1-q^{\delta})^d]^{e+1},$$

i.e.,

$$\alpha = (d+1)\binom{t}{d+1}[q^{\delta}(1-q^{\delta})^d]^{e+1}.$$

Theorem 3.7. *The random matrix* $M_q^s(i;r,0;m,k;n+l,n)$ *is an* α*-almost* $(d,r,z]$*-disjunct matrix, where*

$$\alpha = \binom{d+r}{r}\binom{t}{d+r}[q^{r\delta}(1-q^{\delta})^d]^z.$$

Proof. *Select* $d+r$ *columns* $\{C_{v_j}(i)\}_{j=1}^{d+r}$ *from* t *columns of matrix* $M_q^s(i;r,0;m,k;n+l,n)$ *randomly. Let* E *be the event that* $M_q^s(i;r,0;m,k;n+l,n)$ *has at least* z *rows that are* 1 *in* $\bigwedge_{j=1}^{r} C_{v_j}(i)$ *and* 0 *in* $\bigvee_{j=r+1}^{r+d} C_{v_j}(i)$.

Let E' *be a random event that there are one row* i *such that* $\bigwedge_{j=1}^{r} C_{v_j}(i) > \bigvee_{j=r+1}^{r+d} C_{v_j}(i)$ *for the* $d+r$ *columns* $\{C_{v_j}(i)\}_{j=1}^{d+r}(i=1,2,\cdots,N)$*. Therefore, we have*

$$\begin{aligned}
P(\overline{E'}) &= P\{C_1(i) = \cdots = C_d(i) = 0 \text{ and } C_{r+1}(i) = \cdots = C_{r+d}(i) = 1, i \in [N]\}\\
&= P(E_1)^r P^d(E_0)\\
&= P(E_1)^r(1-P(E_1))^d.\\
P(E) &\geq \binom{d+r}{r}\binom{t}{d+r}[q^{r\delta}(1-q^{\delta})^d]^z.
\end{aligned}$$

Hence,

$$\alpha = \binom{d+r}{r}\binom{t}{d+r}[q^{r\delta}(1-q^{\delta})^d]^z.$$

According to the Theorems 3.6 and 3.7, the random matrix $M_q^s(i;r,0;m,k;n+l,n)$ has properties as follows.

Theorem 3.8. *Let* $\{a_{v_j}(i) | i=1,2,\cdots,N; j=1,2,\cdots,t\}$ *be the columns of* $M_q^s(i;r,0;m,k;n+l,n)$*.*
1) *Select a d-set* $\{a_{v_j}(i)\}_{j=1}^{d}$ *from* $M_q^s(i;r,0;m,k;n+l,n)$ *randomly, then*

$$P\{d_H(a_v(i), \bigvee_{j=1}^{d} a_v(i)) \geq 2e+1\} \geq (d+1)\binom{t}{d+1}[1-q^{\delta}(1-q^{\delta})^d]^{e+1};$$

2) *Select a d-set* $\{a_{v_k}(i)\}_{k=1}^{d+r}$ *from* $M_q^s(i;r,0;m,k;n+l,n)$ *randomly, then*

$$P\{d_H(\bigwedge_{k=1}^{r} a_{v_k}(i), \bigvee_{k=r+1}^{r+d} a_{v_{j_m}}(i)) \geq z\} \geq \binom{d+r}{r}\binom{t}{d+r}[q^{r\delta}(1-q^{\delta})^d]^z.$$

Proof. *It can be directly obtained by Definitions 2.2, 2.3 and Theorems 3.6, 3.7.*

4. Analyzing parameter

In the random pool design, the parameter α represents the probability that a binary matrix is a disjunctive matrix. And the larger the parameter α is, the better the design is. Next, we use α as a standard to measure the pros and cons of the random pooling design.

For the parameter of α-*almost* d^e-disjunct matrix, we can know from Theorem 3.6 that the α is

$$\alpha = (d+1)\binom{t}{d+1}[q^{\delta}(1-q^{\delta})^d]^{e+1}.$$

Li et al. constructed random pooling designs based on the binary superposition code $M_q(n,k,d)$ (see [6]). They constructed an α-*almost* d^e-disjunct matrix, where α_1 is

$$\alpha_1 = (d+1)\binom{t}{d+1}[q^{2(k-n)d}(1-q^{2(k-n)d})^d]^{e+1}.$$

Theorem 4.1. *Let $x < -log_q(d+1)$, then the function $f(x) = q^x(1-q^x)^d$ is monotonically increasing.*

Proof. *Taking the derivative of the function $f(x)$, we have that*

$$\begin{aligned} f'(x) &= q^x \cdot lnq \cdot (1-q^x)^d + q^x \cdot d \cdot (1-q^x)^{d-1} \cdot (-q^x) \cdot lnq \\ &= q^x \cdot lnq \cdot (1-q^x)^{d-1} \cdot [1-(d+1)q^x]. \end{aligned}$$

If $x < -log_q(d+1)$, the function $f(x) = q^x(1-q^x)^d$ is monotonically increasing.

Theorem 4.2. *Let $2(k-n)d < \delta < -log_q(d+1)$, then $\alpha > \alpha_1$.*

Proof.

$$\begin{aligned} \frac{\alpha}{\alpha_1} &= \frac{(d+1)\binom{t}{d+1}[q^{\delta}(1-q^{\delta})^d]^{e+1}}{(d+1)\binom{t}{d+1}[q^{2(k-n)d}(1-q^{2(k-n)d})^d]^{e+1}} \\ &= \frac{[q^{\delta}(1-q^{\delta})^d]^{e+1}}{[q^{2(k-n)d}(1-q^{2(k-n)d})^d]^{e+1}} \\ &= (\frac{q^{\delta}(1-q^{\delta})^d}{q^{2(k-n)d}(1-q^{2(k-n)d})^d})^{e+1}. \end{aligned}$$

From Theorem 4.1 we can know that if $2(k-n)d < \delta < -log_q(d+1)$, $q^{\delta}(1-q^{\delta})^d > q^{2(k-n)d}(1-q^{2(k-n)d})^d$. Furtherly, we have $\alpha > \alpha_1$.

We have similar results for α-*almost* $(d,r,z]$-disjunct matrix. For the parameter of the α-*almost* d^e-disjunct matrix, we can know from Theorem 3.6 that the α' is

$$\alpha' = \binom{d+r}{r}\binom{t}{d+r}[q^{r\delta}(1-q^{\delta})^d]^z.$$

In [6], the parameter of α-*almost* $(d,r,z]$-disjunct matrix is α_2

$$\alpha_2 = \binom{d+r}{r}\binom{t}{d+r}[q^{2(k-n)rd}(1-q^{2(k-n)d})^d]^z.$$

Then we have the results as follow.

Theorem 4.3. *Let $x < log_q \frac{r}{r+d}$, then the function $g(x) = q^{rx}(1-q^x)^d$ is monotonically increasing.*

Proof. *Taking the derivative of the function $g(x)$, we have that*

$$\begin{aligned} g'(x) &= r \cdot q^{rx} \cdot lnq \cdot (1-q^x)^d - d \cdot q^{rx} \cdot q^x \cdot lnq \cdot (1-q^x)^{d-1} \\ &= q^{rx} \cdot lnq \cdot (1-q^x)^{d-1} \cdot [r - (r+d)q^x]. \end{aligned}$$

If $x < log_q \frac{r}{r+d}$, the function $g(x) = q^{rx}(1-q^x)^d$ is monotonically increasing.

Theorem 4.4. *Let $2(k-n)d < \delta < log_q \frac{r}{r+d}$, then $\alpha' > \alpha_2$.*

Proof.

$$\begin{aligned} \frac{\alpha'}{\alpha_2} &= \frac{\begin{pmatrix} d+r \\ r \end{pmatrix}\begin{pmatrix} t \\ d+r \end{pmatrix}[q^{r\delta}(1-q^\delta)^d]^z}{\begin{pmatrix} d+r \\ r \end{pmatrix}\begin{pmatrix} t \\ d+r \end{pmatrix}[q^{2(k-n)rd}(1-q^{2(k-n)d})^d]^z} \\ &= \frac{[q^{r\delta}(1-q^\delta)^d]^z}{[q^{2(k-n)rd}(1-q^{2(k-n)d})^d]^z} \\ &= (\frac{q^{r\delta}(1-q^\delta)^d}{q^{2(k-n)rd}(1-q^{2(k-n)d})^d})^z \end{aligned}$$

From Theorem 4.3 we can know that if $2(k-n)d < \delta < log_q \frac{r}{r+d}$, $q^{r\delta}(1-q^\delta)^d > q^{2(k-n)rd}(1-q^{2(k-n)d})^d$. Furtherly, we have $\alpha' > \alpha_2$.

5. Conclusions

In this paper, we obtain a family of random pooling designs based on the singular linear spaces and related counting theorems firstly. Besides, based on Theorem 3.3 we construct an α-*almost* d^e-disjunct matrix and an α-*almost* $(d, r, z]$-disjunct matrix, which are random pooling designs with error-tolerant property. Furtherly, all the parameters and properties of these random pooling designs are given in Theorems 3.5–3.8, which indicate the characteristics of sample data to a certain extent. According to this, the testor can choose the appropriate number of items to detect. It helps us saving time and costs of the tests to some degree. At last, by comparing to Li's construction, we find that our design is better under certain condition.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grant No. 11701558.

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. A. J. Macula, A simple construction of d-disjunct matrices with certain constant weights, *Discrete Math.,* **162** (1996), 311–312. https://doi.org/10.1016/0012-365X(95)00296-9
2. A. J. Macula, V. V. Rykov, S. Yekhanin, Trivial two-stage group testing for complexes using almost disjunct matrices, *Discrete Appl. Math.,* **137** (2004), 97–107. https://doi.org/10.1016/S0166-218X(03)00191-4
3. A. J. Macula, L. J. Popyack, A group testing method for finding patterns in data, *Discrete Appl. Math.,* **144** (2004), 149–157. https://doi.org/10.1016/j.jmatprotec.2004.09.023
4. W. Lang, Y. Wang, J. Yu, S. Gao, W. Wu, Error-tolerant trivial two-stage group testing for complexes using almost separable and almost disjunct matrices, *Discrete Math. Algorit.,* **1** (2009), 235–251.
5. H. Shi, W. Rui, Construction and properties of a class of random d-disjunct matrices, *Math. Pract. Theory,* **48** (2018), 306–310. https://doi.org/10.1515/hzhz-2018-0007
6. Y. Li, S. Wang, J. Liu, Random pooling designs under the binary superposition code $M_q(n, k, d)$, *Math. Pract. Theory,* **49** (2019), 310–314. https://doi.org/10.1177/0049085719844117
7. K. Wang, J. Guo, F. Li, Singular linear space and its applications, *Finite Fields Th. App.,* **17** (2011), 395–406. https://doi.org/10.4000/geomorphologie.9607
8. Z. Wan, *Geometry of classical groups over finite fields, 2 Eds.*, New York: Science Press, 2002.
9. J. Guo, K. Wang, Pooling designs with surprisingly high degree of error correction in a finite vector space, *Discrete Appl. Math.,* **160** (2012), 2172–2176. https://doi.org/10.1016/j.dam.2012.05.018

AIMS Press