

# New construction of error-tolerant pooling designs

R. Ahlswede and H. Aydinian  
Department of Mathematics  
University of Bielefeld  
POB 100131, D-33501 Bielefeld, Germany  
Email: ahlswede@math.uni-bielefeld.de  
ayd@math.uni-bielefeld.de

**Abstract** We present a new class of error-tolerant pooling designs by constructing  $d^z$ -disjunct matrices associated with subspaces of a finite vector space.

**Keywords** Group testing, Nonadaptive algorithm, Pooling designs,  $d^z$ -disjunct matrix

## 1 Introduction

Combinatorial group testing has various practical applications [8], [9]. In the classical group testing model we have a set  $[n] = \{1, \dots, n\}$  of  $n$  items containing at most  $d$  defective items. The basic problem of group testing is to identify the set of all defective items with a small number of group tests. Each *group test*, also called a *pool*, is a subset of items. It is assumed that there is a testing mechanism that for each subset  $A \subset [n]$  gives one of two possible outcomes : *negative* or *positive*. The outcome is positive if  $A$  contains at least one defective and is negative otherwise.

A group testing algorithm is called *nonadaptive* if all tests are specified without knowledge of the outcomes of other tests. Traditionally, a nonadaptive group testing algorithm is called a *pooling design*. Pooling designs have many applications in molecular biology, such as DNA screening, nonunique probe selection, gene detection, etc. (see [9], [10]).

A pooling design is associated with a  $(0, 1)$ -inclusion matrix  $M = \{m_{ij}\}$ , where the rows are indexed by tests  $A_1, \dots, A_t \subset [n]$ , the columns are indexed by items  $1, \dots, n$ , and  $m_{ij} = 1$  if and only if  $j \in A_i$ . The major tool used for construction of pooling designs are  $d$ -disjunct matrices. Let  $M$  be a binary  $t \times n$  matrix where the columns  $C_1, \dots, C_n$  are viewed as subsets of  $[t] = \{1, \dots, t\}$  represented by their characteristic vectors. Then  $M$  is called  $d$ -disjunct if no column is contained in the union of  $d$  others. The notion of  $d$ -disjunctness was introduced by Kautz and Singleton [14]. They proved that a  $d$ -disjunct matrix  $M$  can

identify up to  $d$  defective items.  $d$ -disjunct matrices are also known as  $d$ -cover free families studied in extremal set theory [7].

The maximal  $d$  for which  $M$  is  $d$ -disjunct is called the degree of disjunctness and is denoted by  $d_{max}$ . Note that  $d$ -disjunctness of a pooling design is a sufficient, but not a necessary condition for identification of  $d$  defectives. However a  $d$ -disjunct pooling design has an advantage of a very simple decoding. Removing from the set of items all items in negative pools we get all defectives (see [9] for details).

A pooling design is called *error-tolerant* if it can detect/correct some errors in test outcomes. Biological experiments are known to be unreliable (see [9]), which, in fact, is a practical motivation for constructing efficient error-tolerant pooling designs.

For error correction in tests the notion of a  $d^z$ -disjunct matrix was introduced in [17]. A  $d$ -disjunct matrix is called  $d^z$ -disjunct if for any  $d + 1$  of its columns  $C_{i_1}, \dots, C_{i_{d+1}}$  we have  $|C_{i_1} \setminus (C_{i_2} \cup \dots \cup C_{i_{d+1}})| \geq z$ . In fact, the  $d^1$ -disjunctness is simply the  $d$ -disjunctness. A  $d^z$ -disjunct matrix can detect  $z - 1$  errors and correct  $\lfloor \frac{z-1}{2} \rfloor$  errors (see e.g. [10] or [9]). Constructions of  $d^z$ -disjunct matrices are given by many authors (see [2], [17], [18], [10]).

Most known constructions of  $d^z$ -disjunct matrices are matrices with a constant column weight. Let  $M$  be a binary  $t \times n$  matrix with a constant column weight  $k$  and let  $s$  be the maximum size of intersection (number of common ones) between two different columns. Kautz and Singleton [14] observed that then  $M$  is  $d$ -disjunct with  $d = \lfloor \frac{k-1}{s} \rfloor$ . Moreover, for integers  $0 \leq s < k < t$  the maximum number  $n(d, t, w)$  for which there exists such a disjunct matrix is upper bounded by

$$n(d, t, k) \leq \binom{t}{s+1} / \binom{k}{s+1}. \quad (1.1)$$

Note that the columns of  $M$  considered as the family  $\mathcal{F}$  of  $k$ -subsets of  $[t]$  (called blocks) form an  $(s+1, k, t)$ -packing, that is each  $(s+1)$ -subset of  $[t]$  is contained in at most one block of  $\mathcal{F}$ . Note also that equality in (1.1) is attained if and only if  $\mathcal{F}$  is an  $(s+1, k, t)$ -Steiner system (each  $(s+1)$ -subset is contained in precisely one block).

Thus, packing designs can be used for construction of  $d$ -disjunct matrices. However, construction of good  $(s+1, k, t)$ -packings, in general, is known to be a difficult combinatorial problem. Several other constructions (see [9, Ch.3]) of disjunct matrices are also based on combinatorial structures or error correcting codes. We note that  $(s+1, k, t)$ -packings can also be described in terms of codes in the Johnson graph  $J(n, k)$  (or Johnson scheme) with minimum distance  $d_J = k - s$ . It seems natural to try other distance regular graphs (see [4] for definitions), for construction of  $d$ -disjunct matrices, using the idea of packings.

In this paper we construct new error-tolerant pooling designs associated with finite vector spaces. In Section 2 we briefly review some known constructions of disjunct matrices based on partial orders and determine the degree of disjunctness for the construction proposed by Ngo and Du [18]. Our main results are stated and proved in Section 3. We present a construction of  $d^z$ -disjunct matrices based on packings in finite projective spaces. For certain parameters the construction gives better performance than previously known ones.

## 2 $d^z$ -disjunct matrices from partial orders

Macula [16] proposed a simple direct construction of  $d$ -disjunct matrices. Given integers  $1 \leq d < k < m$ , let  $M = (m_{ij})$  be an  $\binom{m}{d} \times \binom{m}{k}$  matrix where the rows are indexed by elements of  $\binom{[m]}{d}$ , the columns are indexed by the elements of  $\binom{[m]}{k}$ , and  $m_{ij} = 1$  if we have containment relation between the subsets corresponding to the  $i$ th row and the  $j$ th column, otherwise  $m_{ij} = 0$ . Note that each column has weight  $\binom{k}{d}$  and each row has weight  $\binom{m-d}{k-d}$ . Macula showed that  $M$  is a  $d$ -disjunct matrix and  $d_{max} = d$ .

Similar constructions, using different posets, were given by several authors. Ngo and Du [18] extended Macula's construction to some geometric structures. In particular they considered the following construction of a  $d$ -disjunct matrix  $M_q(m, d, k)$  associated with finite vector spaces. Let  $GF(q)^m$  be the  $m$ -dimensional vector space over  $GF(q)$ . The set of all subspaces of  $GF(q)^m$ , called projective space, is denoted by  $\mathcal{P}_q(m)$ . Recall that  $\mathcal{P}_q(m)$  ordered by containment is known as the poset of linear spaces (or linear lattice). Given an integer  $0 \leq k \leq m$ , the set of all  $k$ -dimensional subspaces ( $k$ -spaces for short) of  $GF(q)^m$  is called a *Grassmannian* and denoted by  $\mathcal{G}_q(m, k)$ . Thus, we have  $\bigcup_{0 \leq k \leq m} \mathcal{G}_q(m, k) = \mathcal{P}_q(m)$ . A graph associated with  $\mathcal{G}_q(m, k)$  is called the *Grassmann graph*, when two vertices (elements of  $\mathcal{G}_q(m, k)$ )  $V$  and  $U$  are adjacent iff  $\dim(V \cap U) = k - 1$  (see [4] for more insight). It is known that the size of the Grassmannian  $|\mathcal{G}_q(m, k)|$  is determined by the  $q$ -ary Gaussian coefficient  $\begin{bmatrix} m \\ k \end{bmatrix}_q$ ;  $k = 0, 1, \dots, m$  ( $\begin{bmatrix} m \\ 0 \end{bmatrix}_q \triangleq 1$ ),

$$|\mathcal{G}_q(m, k)| = \begin{bmatrix} m \\ k \end{bmatrix}_q = \frac{(q^m - 1)(q^{m-1} - 1) \cdots (q^{m-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}. \quad (2.1)$$

For integers  $1 \leq r < k < m$ , the  $\begin{bmatrix} m \\ r \end{bmatrix}_q \times \begin{bmatrix} m \\ k \end{bmatrix}_q$  incidence matrix  $M_q(m, r, k) = (m_{ij})$  is defined as follows. The rows and the columns are indexed by the elements of  $\mathcal{G}_q(m, r)$  and  $\mathcal{G}_q(m, k)$  (given in a fixed ordering), respectively, and  $m_{ij} = 1$  if we have containment relation, otherwise  $m_{ij} = 0$ . Note that each column of  $M_q(m, r, k)$  has weight  $\begin{bmatrix} k \\ r \end{bmatrix}_q$  and each row has weight  $\begin{bmatrix} m-r \\ k-r \end{bmatrix}_q$ . Ngo and Du showed that  $M_q(m, r, k)$  is an  $r$ -disjunct matrix. However D'yachkov et al. [10] observed that the degree of disjunctness of  $M_q(m, r, k)$  can be much bigger than  $r$ . Moreover, the construction can in general tolerate many errors.

**Theorem DHMVW** [10]

For  $k - r \geq 2$  and  $d < \frac{q(q^{k-1}-1)}{q^{k-r}-1}$ , the matrix  $M_q(m, r, k)$  is  $d^z$ -disjunct with

$$z \geq \begin{bmatrix} k \\ r \end{bmatrix}_q - d \begin{bmatrix} k-1 \\ r \end{bmatrix}_q + (d-1) \begin{bmatrix} k-2 \\ r \end{bmatrix}_q. \quad (2.2)$$

The bound is tight for  $d \leq q + 1$ .

Note that the maximum number  $d$  in (2.2) for which  $z > 0$  is  $d = \frac{q(q^{k-1}-1)}{q^{k-r}-1}$ . Thus, the theorem tells us that  $d_{max} \geq \frac{q(q^{k-1}-1)}{q^{k-r}-1}$ . In fact, we determine  $d_{max}$  for every  $M_q(m, r, k)$ .

**Theorem 1** For integers  $1 \leq r < k < m$ , the degree of disjunctness of  $M_q(m, r, k)$  equals

$$d_{max} = \frac{q(q^r - 1)}{q - 1}. \quad (2.3)$$

**Proof.** Let  $V \in \mathcal{G}_q(m, k)$ . We wish to determine the minimum size of a set of  $k$ -spaces which cover (contain) all  $r$ -spaces of  $V$ . Suppose  $U_1, \dots, U_p \in \mathcal{G}_q(m, k)$  is a minimal covering of the  $r$ -spaces of  $V$ . Without loss of generality, we may assume that  $\dim(U_i \cap V) = k - 1$  for  $i = 1, \dots, p$ . Therefore,  $W_1 = U_1 \cap V, \dots, W_p = U_p \cap V$  can be viewed as a set of hyperplanes of  $\mathcal{P}_q(k)$  that cover all  $r$ -spaces of  $\mathcal{P}_q(k)$ . Let now  $A_i \in \mathcal{P}_q(k)$  be the orthogonal space of  $W_i$ ;  $i = 1, \dots, p$ . Thus,  $\mathcal{A} = \{A_1, \dots, A_p\}$  is a set of one dimensional subspaces, that is points, in  $\mathcal{P}_q(k)$ . By the principle of duality, every  $(k - r)$ -space of  $\mathcal{P}_q(k)$  contains an element of  $\mathcal{A}$ . To complete the proof we use the following result.

**Theorem BB** [3] *Let  $\mathcal{A} \subset GF(q)^m \setminus \{0\}$  have a non-empty intersection with every  $(k - r)$ -space of  $\mathcal{P}_q(k)$ . Then  $|\mathcal{A}| \geq (q^{r+1} - 1)/(q - 1)$ , with equality if and only if  $\mathcal{A}$  consists of  $(q^{r+1} - 1)/(q - 1)$  points of an  $(r + 1)$ -space of  $\mathcal{P}_q(k)$ .*

It is clear now that  $d_{max} = (q^{r+1} - 1)/(q - 1) - 1$ . □

### 3 New construction

Our construction of a disjunct matrix  $M$  is based on packings in  $\mathcal{P}_q(m)$ . For integers  $0 \leq s < k < m$ , a subset  $\mathcal{C} \subset \mathcal{G}(m, k)$  (with the elements called blocks) is called an  $[s + 1, k, m]_q$ -packing if each  $(s + 1)$ -space of  $\mathcal{P}_q(m)$  is contained in at most one block of  $\mathcal{C}$ . This clearly means that  $\dim(V \cap U) \leq s$  for every distinct pair  $V, U \in \mathcal{C}$ .  $\mathcal{C}$  is called an  $[s + 1, k, m]_q$ -Steiner structure if each  $(s + 1)$ -space of  $\mathcal{P}_q(m)$  is contained in precisely one block of  $\mathcal{C}$ . Let  $N(m, k, s)$  denote the maximum size of an  $[s + 1, k, m]_q$ -packing.

An equivalent definition of an  $[s + 1, k, m]_q$ -packing can be given in terms of the subspace distance  $d_S(V, U)$  defined (in general for any  $V, U \in \mathcal{P}_q(m)$ ) by  $d_S(V, U) = \dim V + \dim U - 2 \dim(V \cap U)$  ([1], [15]). Then clearly  $d_S(V, U) \geq 2(k - s)$  for every pair of elements  $V, U \in \mathcal{C}$ . The following simple observation is an analogue of (1.1) for projective spaces. Let  $M$  be the incidence matrix of an  $[s + 1, k, m]_q$ -packing  $\mathcal{C}$  with  $s \geq 1$ , that is the  $t \times n$  matrix where the rows (resp. columns) are indexed by the nonzero elements of  $GF(q)^n$  (resp. by the blocks of  $\mathcal{C}$ ) given in a fixed ordering.

**Lemma 1** (i) *For  $d \leq q^{k-s}$ , the matrix  $M$  is  $d^z$ -disjunct with  $z = q^k - 1 - d(q^s - 1)$ .  
(ii) *The number of columns**

$$n \leq N(m, k, s) \leq \left[ \begin{matrix} m \\ s + 1 \end{matrix} \right]_q / \left[ \begin{matrix} k \\ s + 1 \end{matrix} \right]_q \quad (3.1)$$

*with both equalities if and only if  $\mathcal{C}$  is an  $[s + 1, k, m]_q$ -Steiner structure.*

**Proof.** (i) By the definition of an  $[s + 1, k, m]_q$ -packing, each  $(s + 1)$ -space is contained in at most one  $k$ -space of  $\mathcal{C}$ . Therefore, any two columns in  $M$  have at most  $q^s - 1$  common ones. Hence, a column in  $M$  can be covered by at most  $\lceil \frac{q^k - 1}{q^s - 1} \rceil > q^{k-s}$  other columns. Note that in case  $s \mid k$ , the space  $GF(q)^k$  can be partitioned by  $s$ -spaces (see [5]) and  $d_{max} = \frac{q^k - 1}{q^s - 1} - 1$ .  
(ii) Since the number of  $(s + 1)$ -spaces contained in a  $k$ -space is  $\left[ \begin{matrix} k \\ s + 1 \end{matrix} \right]_q$ , we have the following

packing bound  $N(m, k, s) \leq \binom{m}{s+1}_q / \binom{k}{s+1}_q$  (see [1], [20], [15]). The equality in (3.1) is attained iff we have a partition of all  $(s+1)$ -spaces by the blocks of  $\mathcal{C}$ .  $\square$

A challenging problem is to find Steiner structures in  $\mathcal{P}_q(n)$ . Note that no nontrivial Steiner structures, except for the case  $s = 0$  when we have a partition of  $GF(q)^m$  by  $k$ -spaces, are known. Properties of Steiner structures in  $\mathcal{P}_q(n)$ , introduced in [1] are studied in [19].

**Theorem WXS** [20] (**KK** [15]) *Given integers  $1 < k < m$ , there exists an explicit construction of an  $[s+1, k, m]_q$ -packing  $\mathcal{C}$  with*

$$|\mathcal{C}| = \begin{cases} q^{(s+1)(m-k)} & \text{if } m \geq 2k, 0 \leq s < k \\ q^{k(s+1)} & \text{if } m < 2k, 0 \leq s < m - k. \end{cases} \quad (3.2)$$

The construction of such packings is based on Gabidulin codes [13]. The explicit description (in terms of subspace codes) is given in [20] and in [15]. For completeness we describe this construction here (in terms of  $[s+1, k, m]_q$ -packings). Let  $\mathbb{F}_q^{k \times r}$  denote the set of all  $k \times r$  matrices over  $GF(q)$ . For  $X, Y \in \mathbb{F}_q^{k \times r}$  the rank distance between  $X$  and  $Y$  is defined as  $d_R(X, Y) = \text{rank}(X - Y)$ . It is known that the rank-distance is a metric [13]. Codes in metric space  $(\mathbb{F}_q^{k \times r}, d_R)$  are called rank-metric codes. It is known [13] that for a rank-metric code  $\mathcal{C} \subseteq \mathbb{F}_q^{k \times r}$  with minimum distance  $d_R(\mathcal{C})$  one has the Singleton bound  $\log_q |\mathcal{C}| \leq \min\{k(r - d_R(\mathcal{C}) + 1), r(k - d_R(\mathcal{C}) + 1)\}$ . Codes attaining this bound are called maximum-rank-distance codes (MRD). An important class of rank-metric codes are Gabidulin codes [13]. They are linear MRD codes, which exist for all parameters  $k, r$  and  $d_R \leq \min\{k, r\}$ . The construction of an  $[s+1, k, m]_q$ -packing from an MRD code is as follows. Consider the space  $\mathbb{F}_q^{k \times (m-k)}$  ( $m \geq k$ ). Let first  $m \geq 2k$ . Then for any integer  $0 \leq s \leq k$  there exists a Gabidulin code  $\mathcal{C}_G \subset \mathbb{F}_q^{k \times (m-k)}$  of minimum distance  $d_R = k - s$  and size  $q^{(s+1)(m-k)}$ . To each matrix  $A \in \mathcal{C}_G$  we put into correspondence the matrix  $[I_k | A] \in \mathbb{F}_q^{k \times m}$  ( $I_k$  is the  $k \times k$  identity matrix). We define now the set of  $k$ -spaces  $\mathcal{C}(m, k, s)_q = \{\text{rowspan}([I_k | A]) : A \in \mathcal{C}_G\}$ . It can easily be observed now that  $\dim(V \cap U) \leq s$  for all pairs  $V, U \in \mathcal{C}(m, k, s)_q$ . This means that  $\mathcal{C}(m, k, s)_q$  is an  $[s+1, k, m]_q$ -packing with  $|\mathcal{C}(m, k, s)_q| = |\mathcal{C}_G| = q^{(s+1)(m-k)}$ . Similarly is described the  $[s+1, k, m]_q$ -packing  $\mathcal{C}(m, k, s)_q$  for  $m < 2k$ . Note that for our purposes the case  $m \geq 2k$  is more important.

The following is a useful estimate for the Gaussian coefficients. A proof can be found in [6] (and in [15] for the case  $q = 2$ ).

**Lemma 2** *For integers  $1 \leq k < m$  we have*

$$q^{(m-k)k} < \binom{m}{k}_q < \alpha(q) \cdot q^{(m-k)k}, \quad (3.3)$$

where  $\alpha(2) = 4$  and  $\alpha(q) = \frac{q}{q-2}$  for  $q \geq 3$ .

Note that Lemma 2 in conjunction with Theorem WXS applied to our upper bound (3.1) shows that  $\mathcal{C}(m, k, s)_q$  is nearly optimal:

$$|\mathcal{C}(m, k, s)_q| \leq |N(m, k, s)_q| < \alpha(q) \cdot q^{(s+1)(m-k)} = \alpha(q) \cdot |\mathcal{C}(m, k, s)_q|.$$

Here actually  $\lim \alpha(q) = 1$ , as  $q \rightarrow \infty$ , yields asymptotic optimality.

Let  $P(m, k, s)_q$  denote the incidence matrix of  $\mathcal{C}(m, k, s)_q$ . We summarize our findings in

**Theorem 2** *Given integers  $1 \leq s < k \leq \frac{1}{2}m$  and a prime power  $q$ , we have*  
(i)  $P(m, k, s)_q$  is a  $d$ -disjunct  $t \times n$  matrix where  $t = q^m - 1$ ,  $n = q^{(s+1)(m-k)}$ ,  $d = q^{k-s}$ .  
(ii) For any  $d \leq q^{k-s}$ , the matrix  $P(m, k, s)_q$  is  $d^z$ -disjunct with  $z = q^k - 1 - d(q^s - 1)$ .

Finally, we explain how good our construction is. Let  $t(d, n)$  denote the minimum number of rows for a  $d$ -disjunct matrix with  $n$  columns. In the literature known are the bounds asymptotic in  $n$

$$\Omega(1/d^2) \leq \frac{\log n}{t(d, n)} \leq O((\log d)/d^2) \quad (3.4)$$

(log is always of base 2). The lower bound is proved in [14], [11], [7] (see also [12], [9, ch.2]) using probabilistic methods. The upper bound is due to D'yachkov and Rykov [11].

Next we compare our construction with the construction in Ngo and Du [18], described in Section 2 (both constructions we take over  $GF(q)$ ). In their construction we have  $n \leq \alpha(q)q^{(m-k)k}$ ,  $t \geq q^{(m-r)r}$  (Lemma 2),  $d = \frac{q(q^r-1)}{q-1}$  (Theorem 2), and rate  $(\log n)/t$ .

For the parameters in our construction we use the notation  $n_0, k_0, t_0, d_0$ . Thus,  $n_0 = q^{(s+1)(m_0-k_0)}$ ,  $t_0 = q^{m_0} - 1$ ,  $d_0 \geq q^{k_0-s}$ . We put  $m_0 = m$ ,  $k_0 = k$ ,  $s = k - r - 1$ . Then we have  $n_0 = q^{(k-r)(m-k)}$ ,  $t_0 = q^m - 1$ ,  $d_0 \geq q^{r+1} > d$ , and rate  $(\log n_0)/t_0$ . A simple calculation shows that  $(\log n_0)/t_0$  exceeds  $(\log n)/t$  by a factor  $q^{m(r-1)-r^2} \cdot \frac{k-r}{k+1}$ .

Let us take now in our construction  $q = 2$ ,  $m = 2k$ . Then we have  $d = 2^{k-s}$ ,  $t = 2^{2k} - 1$ ,  $n = 2^{(s+1)k}$  and hence

$$\frac{\log n}{t} > \frac{(s+1)k}{2^{2k}} > \frac{s+1}{2^{2s}} \cdot \frac{\log d}{d^2}.$$

**Corollary 1** *Given integer  $s \geq 1$ , our construction gives a class of  $d$ -disjunct  $t \times n$  matrices with parameters  $d = 2^{k-s}$ ,  $t = 2^{2k}$ ,  $n = 2^{(s+1)k}$  attaining the upper bound in (3.4), that is rate  $(\log n)/t = \Omega((\log d)/d^2)$ .*

## References

- [1] R. Ahlswede, H. Aydinian, and L.H. Khachatrian, On perfect codes and related concepts, Des. Codes Cryptogr. 22, no. 3, 221–237, 2001.
- [2] D.J. Balding and D.C. Torney, Optimal pooling designs with error detection, J. Combin. Theory Ser. A 74, no. 1, 131–140, 1996.
- [3] R.C. Bose and R.C. Burton, A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonal codes, J. Combin. Theory 1, 96–104, 1996.
- [4] A.E. Brouwer, A.M. Cohen, and A. Neumaier, Distance-Regular graphs, Springer-Verlag, Berlin Heidelberg, 1989.

- [5] T. Bu, Partitions of a vector space, *Discrete Math.* 31, no. 1, 179-83, 1980.
- [6] W.E. Clark and M.E.H. Ismail, Binomial and  $Q$ -binomial coefficient inequalities related to the hamiltonicity of the Kneser graphs and their  $Q$ -analogues, *J. Combin. Theory Ser. A* 76, no. 1, 83-98, 1996.
- [7] P. Erdős, P. Frankl, and Z. Füredi, Families of finite sets in which no set is covered by the union of  $r$  others, *Isr. J. Math.* 51, no. 1-2, 79-89, 1985.
- [8] D.-Z. Du and F.K. Hwang, *Combinatorial Group Testing and its Applications*, World Scientific, 2nd edit., Singapore, 2000.
- [9] D.-Z. Du and F.K. Hwang, *Pooling Designs and Nonadaptive Group Testing-Important Tools for DNA sequencing*, World Scientific, 2006.
- [10] A. D'yachkov, F.K. Hwang, A. Macula, P. Vilenkin, and C. Weng, A construction of pooling designs with some happy surprises, *J. Comput. Biology* 12, 1129-1136, 2005.
- [11] A. D'yachkov, V.V. Rykov, Bounds on the length of disjunctive codes, *Problems Inform. Transmission* 18, no. 3, 7-13, 1982.
- [12] A. D'yachkov, V.V. Rykov, and A.M. Rashad, Superimposed distance codes, *Problems Control Inform.* 18, no. 4, 237-250, 1989.
- [13] E.M. Gabidulin, Theory of codes with maximum rank distance, *Problems Inform. Transmission* 21, no. 1, 1-12, 1985.
- [14] W.H. Kautz and R.C. Singleton, Nonrandom binary superimposed codes, *IEEE Trans. Info. Theory* 10, 363-377, 1964.
- [15] R. Koetter and F.R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. Info. Theory* 54, no. 8, 3579 - 3591, 2008.
- [16] A.J. Macula, A simple construction of  $d$ -disjunct matrices with certain constant weights, *Discrete Math.* 162, 311-312, 1996.
- [17] A.J. Macula, Error-correcting nonadaptive group testing with  $d^z$ -disjunct matrices, *Discrete Appl. Math.* 80, 217-222, 1996.
- [18] H.Q. Ngo and D.-Z. Du, New constructions of non-adaptive and error-tolerance pooling designs, *Discrete Math.* 243, 161-170, 2002.
- [19] M. Schwartz and T. Etzion, Codes and anticode in the Grassman graph, *J. Combin. Theory Ser. A* 97, no. 1, 27-42, 2002.
- [20] H. Wang, C. Xing, and R. Safavi-Naini, Linear authentication codes: bounds and constructions, *IEEE Trans. Info. Theory* 49, no. 4, 866-872, 2003.