1 Introduction and Preliminaries

Some basic definitions, including *dependency* and *independency* of systems of vectors and $(t, m, s)-$nets, are given in section 2. They then lead to the notions of *digital nets*, *superimposed codes* and *superimposed designs* together with some illustrative examples in section 3 and 4. The independency of systems of vectors over $GF(q)$, that is, $(d, m, m, s)-$*systems* plays an important role for digital nets as an generalization of the parity-check matrix for linear codes in the section 3. Moreover, we use $(d, k, m, s)-$systems will be used for the construction of superimposed codes in subsection 4-4.

The digital method and *digital nets* are two main subjects of this thesis. A $(t, m, s)-$net is a multiset of points in the $s-$dimensional unit cube $I^s, s \geq 1$, with a high degree of *regular uniform distribution*. A digital net with q^m points is constructed over the vector space $GF(q)^m$ by the digital method in terms of some combinatorial and number theoretic arguments. A key for constructing digital nets having stronger uniform distribution, i.e., with the parameter t as small as possible is related to the choice of $m \times m$ matrices $C_1, \cdots, C_s$ with some specific properties. The construction of good digital nets can therefore be transformed into a problem of combinatorial linear algebra over finite fields. And *the duality theory* for digital nets is a suitable way to transform the problem into construction of good linear codes in the metric spaces $(GF(q)^{ms}, d_m)$, including the Hamming spaces with $q = 2$.

On the other hand, we can choose $m \times m$ matrices $C_1, \cdots, C_s$ first to make the system C with a good property for constructing good digital nets. By the Theorem 3.1 [8, Theorem 2.1; 5, Theorem 6.1] in section 3, the notion of $(d, m, m, s)-$systems is introduced over the system C with fixed m, s and larger $d = m - t$ for constructing

digital nets with a parameter t and a stronger uniform distribution. The system C derived from *impulse response sequences* and *monic irreducible polynomials* is a suitable way for constructing good digital nets of great worth.

We will introduce how the technique of (*cyclic*) *digital method* and *duality theory* for digital nets can be applied to the construction of digital nets in subsection 3-1, and constructions for digital nets and examples in subsection 3-2. The quality parameter t of digital nets depends only on the choice of $m \times m$ matrices $C_1, \cdots, C_s$ if the value m, s are fixed in the digital method. Moreover, we consider the subspace M spanned $\{c_{1,j}, c_{2,j}, \cdots, c_{s,j}\}_{j=1}^{m}$ by and then the relationship between perpendicular $M^{\perp}$ and $(d, m, m, s)-$systems in terms of $\delta_m(M^{\perp})$ in the duality theory, in addition to the subspace $M^{\perp}$ with $\dim(M^{\perp}) = ms - m$ provided by cyclic digital method. Hence the technique of constructions for digital nets is constructing $(d, m, m, s)-$systems $C_1, \cdots, C_s$. So we introduce two ideas for constructing digital nets: the first method is producing $(d, m, m, s)-$systems by the impulse response sequence, and the second method is constructing the subspace $M^{\perp}$ by the duality theory in subsection 3-2.

The notion of *superimposed* $(s, 1)-$*code* was first introduced in 1964 by Kautz and Singleton [3]. The *superimposed* $(s, l)-$*code* is defined in 2002 by A. D'yachkov and P. Vilenkin, A. Macula, D. Torney [2]. Moreover, the definition of $(s, l; e)-$ disjunct matrix is defined by the incidence matrix of a set system [9]. A *set system* $(X, \mathcal{F})$ is a set of points $X = \{x_1, \cdots, x_t\}$ and a family of subsets $\mathcal{F} = \{f_1, \cdots, f_N\}$ of X (called *blocks*) corresponds to a incidence matrix $M = [M(i, j)]_{t \times N}$ such that $M(i, j) = 1$ if and only if $x_i \in f_j$, and 0 otherwise. In the rest of this thesis, all set systems are treated in terms of their incidence matrix. Moreover, we will introduce generalizations of definitions called $(s, l; e)-$*disjunct matrices* and $(s, l; e)-$*separable matrices*, their relations and how to construct them. The concatenated construction was suggested in

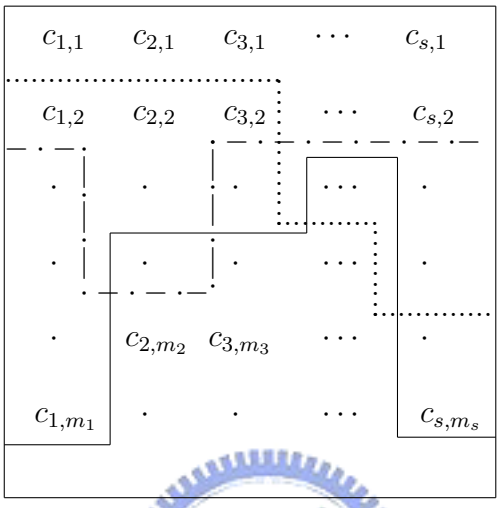
[3], and used to construct superimposed $(s, l)-$codes [2] and $(s, l; e)-$disjunct matrices [9].

We will review some papers about *disjunct matrices* and *separable matrices* in subsection 4-1 and count the minimum Hamming distance over boollean sum of m columns (and at most m columns) e_m (and $e_{\leq m}$) over the $(0, 1)-$matrix M, row-indexed and column-indexed by $d-$subsets and $k-$subsets respectively of $[n]$ such that $M(A, B) = 1$ if $A \subseteq B$ and 0 otherwise to get some examples of disjunct matrices and separable matrices in subsection 4-2. The above results will be generalized to its $q-$analog over vector spaces over finite fields. As generalizations of $(s, l)-$disjunct matrices and $(s, l)-$separable matrices, the definitions of $(s, l; e)-$disjunct matrices and $(s, l; e)-$separable matrices will be introduced together with their relations and their constructions in subsection 4-3. For their construction, we apply the concatenated construction for $(s, l; e)-$disjunct matrices to construct $(s, l; e)-$separable. Moreover, some relationship between $(d, k, m, s)-$systems and superimposed codes are given in subsection 4-4. When $m = 1$, $(d, k, 1, s)-$systems and binary codes as well will be used to the construction of superimposed $(a, b)-$codes, and when $m \geq 2$, it can be also used to construct superimposed $(a, b)-$codes.

In this thesis, we introduce some definitions and theorems of some papers about digital nets, disjunct matrices and separable matrices. Moreover, we give a construction for digital nets in terms of impulse response sequences in subsection 3-2-1, consider the parameters e_m and $e_{\leq m}$ over the Johnson schemes and the Grassmann schemes and concatenated construction for $(s, l; e)-$separable matrices in subsection 4-2, and construct superimposed $(s, l)-$codes by $(d, k, m, s)-$systems in subsection 4-4.

2 $(d, k, m, s)-$Systems

The notions of *dependency* and *independency* of systems of vectors and $(t, m, s)-$nets will lead to the notions of *digital nets*, *superimposed codes* and *superimposed designs*.



Definition 2.1 [6, P.221] Let $m \geq 1$ and $m_1, \cdots, m_s$ be positive integers, we define

$$R(m; m_1, \cdots, m_s) = R(m; m_1, \cdots, m_s) = \max_C(\min \sum_{i=1}^{s} d_i) = \max_C(\rho(C))$$

where the maximum is over all systems $C = \{c_{i,j_i} \in GF(q)^m \mid 1 \leq i \leq s, 1 \leq j_i \leq m_i\}$ of row vectors $c_{i,j_i} \in GF(q)^m$, and the minimum is over all *linearly dependent* subsystems $\{c_{i,j_i} \mid 1 \leq i \leq s, 1 \leq j_i \leq d_i\}$ of C with integers $0 \leq d_i \leq m_i$ for $1 \leq i \leq s$ and with $\sum_{i=1}^{s} d_i \geq 1$.

Remarks 2.1

1. Let H be the matrix of order $m \times s$ with columns $c_{1,1}^T, c_{1,2}^T, \cdots, c_{1,s}^T$. If $s > m$ and $\text{rank}(H) = m$, then H is *the parity-check matrix* of a linear code C over $GF(q)$ of length s, with dimension $s - m$ and with minimum distance $\rho(C)$.

2.The value $R(m; m_1, \cdots, m_s)$ is between 2 and $m+1$, and the equality and the equality $R(m; m_1, \cdots, m_s) = m + 1$ holds if and only if there exists *a maximal distance*

separable (*MDS*) code over $GF(q)^m$ of length s, and with dimension $s-m$.

3. $R(m;m_1,\cdots,m_s) \geq R(m;m,\cdots,m)$ for $m \leq \min_{1\leq i\leq s} m_i$ and $R(m;m_1,\cdots,m_s) \leq R(m;m,\cdots,m)$ for $m \geq \max_{1\leq i\leq s} m_i$.

4. For a system $C = \{c_{i,j_i} \in GF(q)^m \mid 1 \leq i \leq s, 1 \leq j_i \leq m_i\}$ over $GF(q)$, and two subsystems $C_1 = \{c_{i,j_i} \in GF(q)^m \mid 1 \leq i \leq s, 1 \leq j_i \leq d_i\}$ and $C_2 = \{c_{i,j_i} \in GF(q)^m \mid 1 \leq i \leq s, 1 \leq j_i \leq d_i'\}$ with $\sum_{i=1}^s d_i' > \sum_{i=1}^s d_i$, if C_1 linearly dependent, then C_2 is also linearly dependent. Hence, the smaller the value of $\sum_{i=1}^s d_i$ is, the harder the subsystem $\{c_{i,j_i} \mid 1 \leq i \leq s, 1 \leq j_i \leq d_i\}$ is linearly dependent, i.e., the number $\min \sum_{i=1}^s d_i = \rho(C)$ is considered.

For constructing digital nets with interests, we have to construct a system $C = \{c_{i,j} \in GF(q)^m \mid 1 \leq i \leq s, 1 \leq j \leq m\}$ whose any subsystem $\{c_{i,j} \mid 1 \leq i \leq s, 1 \leq j \leq d_i\}$ is linearly independent with as large as possible $\sum_{i=1}^s d_i = d$ (by the Theorem 3.1 [8, Theorem 2.1; 5, Theorem 6.1]).

Definition 2.2 [8, Def 3.1] A system $\{c_{i,j} \in GF(q)^k \mid 1 \leq i \leq s, 1 \leq j \leq m\}$ is called *a* $(d,k,m,s)-$*system* over $GF(q)$ if any subsystem $\{c_{i,j} \in GF(q)^k \mid 1 \leq i \leq s, 1 \leq j \leq d_i\}$ is linearly independent with $\sum_{i=1}^s d_i = d$ and $d \leq \min\{k, ms\}$.

Remarks 2.2

1. A linear code of length s, with dimension at least $s-k$, and with minimum distance at least $d+1$ can be obtained by a $(d,k,1,s)-$system $\{c_i \in GF(q)^k \mid 1 \leq i \leq s\}$ over $GF(q)$, by using the columns $c_1^T, \cdots, c_s^T$ as its parity-check matrix.

2. For a system $C = \{c_{i,j} \in GF(q)^k \mid 1 \leq i \leq s, 1 \leq j \leq m\}$ over $GF(q)$, the larger the value of $\sum_{i=1}^s d_i = d$ is, the harder the subsystem $\{c_{i,j} \in GF(q)^k \mid 1 \leq i \leq s, 1 \leq$

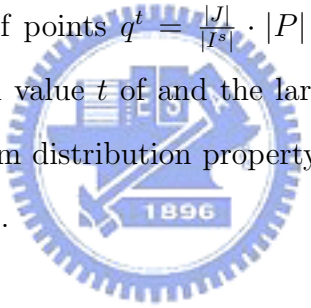
$j \leq d_i\}$ is linearly independent. So if the system C is a $(d, m, k, s)-$system, then it is also a $(i, m, k, s)-$system for $0 \leq i \leq d$.

Definition 2.3 [8, Def 1.1] A $(t, m, s)-net$ in base q is a point set P of q^m points in I^s such that every subinterval

$$J = \prod_{i=1}^{s} [\frac{a_i}{q^{d_i}}, \frac{(a_i + 1)}{q^{d_i}}) \subseteq I^s$$

with $0 \leq a_i < q^{d_i}$ for $1 \leq i \leq s$ and with $\prod_{i=1}^{s} \frac{1}{q^{d_i}} = q^{t-m}$ contains exactly q^t points of P.

Equivalently, a $(t, m, s)-$net is a point set P in *uniform distribution* on any subinterval $J = \prod_{i=1}^{s} [\frac{a_i}{q^{d_i}}, \frac{(a_i+1)}{q^{d_i}}) \subseteq I^s$, i.e., on any subinterval with the same volume, they contain the same number of points $q^t = \frac{|J|}{|I^s|} \cdot |P| = \prod_{i=1}^{s} \frac{1}{q^{d_i}} \cdot q^m = q^{t-m} \cdot q^m$. By definition, $t \leq m$, the small value t of and the large the family of intervals J imply that the stronger the uniform distribution property. The number t is often called *the quality parameter* of the net.



Remarks 2.3

1. The point set P in the definition of $(t, m, s)-$net is allowed to be a multi-set, i.e., multiplicities of elements in the point set are allowed and taken into account.

2. The trivial case is a $(m, m, s)-$net. That is points q^m in I^s form a $(m, m, s)-$net.

Then we will state the relation of the system C with dependency and independency and digital $(t, m, s)-$nets. For any subsystems $\{c_{i,j_i} \mid 1 \leq i \leq s, 1 \leq j_i \leq d_i\}$ with integers $0 \leq d_i \leq m_i$ for $1 \leq i \leq s$:

(i) If it is linear dependent and given $m, m_i, \cdots, m_s$ and $C_{i,j} \in GF(q)^m$, then $\rho(C) = \min \sum_{i=1}^{s} d_i$.

(ii) If it is linear independent and given $m = m_i = \cdots = m_s$ and $C_{i,j} \in GF(q)^k$, then the system is a $(d, k, m, s)-$system with $d = \sum_{i=1}^{s} d_i$.

a. We can construct a linear code by using a $(d, k, 1, s)-$system as *the parity-check matrix*.

b. We can construct a $(m-t, m, s)-$net by using a $(d, m, m, s)-$system as *generating matrices*.

Moreover, we will introduce the digital method and their constructions by $(d, k, m, s)-$systems in section 3.

3 Digital Method and Parity Check Matrices

We will introduce the technique of the (cyclic) digital method and duality theory for the construction of digital nets in subsection 3-1. The point set $P(GF(q)^m) = (T(C_1 \cdot GF(q)^m), T(C_2 \cdot GF(q)^m), \cdots, T(C_s \cdot GF(q)^m))$ where $T(C_i \cdot GF(q)^m) = \sum_{j=1}^{m} \frac{\psi(c_{i,j} \cdot GF(q)^m)}{q^j} \in [0,1)$ in the digital method such that *the quality parameter* t depends on only the choice of the matrices $C_1, C_2, \cdots, C_s$ if the value m, s are fixed. So it is directly to construct digital $(d, m, m, s)-$nets by systems $C = \{C_1, C_2, \cdots, C_s\}$. Moreover, we will consider the subspace M spanned by $\{c_{1,j}c_{2,j}\cdots c_{s,j}\}_{j=1}^{m}$ and then the relationship between perpendicular $M^{\perp}$ and $(d, m, m, s)-$systems in terms of $\delta_m(M^{\perp})$. And we introduce the cyclic digital method constructing the subspace $M^{\perp}$ with $\dim(M^{\perp}) = ms - m$ for the duality theory. Hence we introduce two ideas to construct digital nets: the first method is producing $(d, m, m, s)-$systems by impulse response sequences, and the second method is producing the subspace $M^{\perp}$ by duality theory in subsection 3-2. Some examples of digital nets constructed by methods just mentioned will be included in subsection 3-2.

3-1 The digital method

We will introduce the technique of (cyclic) digital method and duality theory for digital nets for the construction of digital nets. The digital method uses a system of *generating matrices* $\{C_1, C_2, \cdots, C_s\} \in M_{m\times m}(q)$ in terms of some combinatorial and number theoretic argument constructing digital nets. And duality theory uses $M^{\perp} \subseteq GF(q)^{ms}$ and the value of $\delta_m(M^{\perp})$ to determine the parameter t to construct good digital nets. Moreover, cyclic digital method is the technique to construct $M^{\perp} \subseteq GF(q)^{ms}$ with $\dim(M^{\perp}) = ms - m$ for the construction of digital nets.

3-1-1 The digital method [8, P.2]

For a system of generating matrices $\{C_1, C_2, \cdots, C_s\} \in M_{m\times m}(q)$, and a bijection

$$\psi : GF(q) \to \{0, 1, \cdots, q-1\}$$

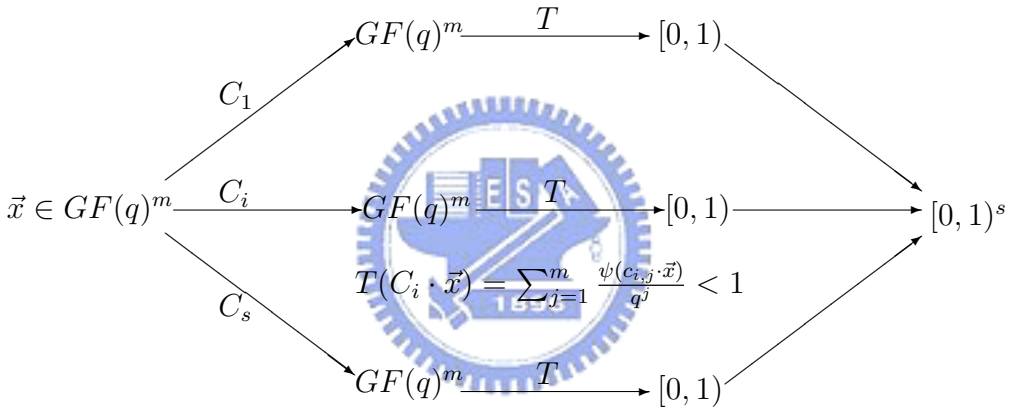
defined the map

$$T : GF(q)^m \to [0, 1)$$

by

$$T(h) = \sum_{j=1}^{m} \psi(h_j) q^{-j},$$

where $h = (h_1, \cdots, h_m) \in GF(q)^m$.



Definition 3.1 The set $P(GF(q)^m) = (T(C_1 \cdot GF(q)^m), T(C_2 \cdot GF(q)^m), \cdots, T(C_s \cdot GF(q)^m))$ is called *a digital* $(t, m, s)-$*net* over if it is *a* $(t, m, s)-$*net in base* q.

Remarks 3.1

1. The identity function ψ works for works for the function in case q is a prime. The function $\psi(0) = 0$ and $\psi(a^k) = k$ works for the finite field $GF(q) = \{0, 1, a, a^2, \cdots, a^{q-2}\}$ for some generator $a \in GF(q)$.

2. For the map T,

$$T(h) = \sum_{j=1}^{m} \psi(h_j) q^{-j} = \frac{\psi(h_1)}{q} + \frac{\psi(h_2)}{q^2} + \cdots + \frac{\psi(h_m)}{q^m} (\text{ in base } q)$$

$$\leq \frac{q-1}{q} + \frac{q-1}{q^2} + \cdots + \frac{q-1}{q^m}$$
$$= \frac{q-1}{q} \cdot (1 + \frac{1}{q} + \cdots + \frac{1}{q^{m-1}})$$
$$< 1.$$

The $q-$ary representation of a number $0.d_1d_2d_3\cdots$ in base q where the digital $d_i \in \{0, \cdots, q-1\}$ is that $0.d_1d_2d_3\cdots = \frac{d_1}{q} + \frac{d_2}{q^2} + \frac{d_3}{q^3} + \cdots$. So the motivation for the term of digital method is because of the component of each point of the digital net is given in terms of the expansions of numbers in the base of q.

3. Since ψ, T are bijections, the quality parameter t depends on only the choice of the matrices $C_1, C_2, \cdots, C_s$ if the values m, s are fixed for a digital $(t, m, s)-$nets. For a $(d, m, m, s)-$system $C = \{C_1, C_2, \cdots, C_s\}$, the number of points on the subinterval $J = \prod_{i=1}^{s}[\frac{a_i}{q^{d_i}}, \frac{(a_i+1)}{q^{d_i}})$ is equal to the number of solutions for the system, $C_i\vec{x} \in [\frac{a_i}{q^{d_i}}, \frac{(a_i+1)}{q^{d_i}})$, $1 \leq i \leq s$ of $m \times s$ equations with m variables over $GF(q)$. So for $J = \prod_{i=1}^{s}[\frac{a_i}{q^{d_i}}, \frac{(a_i+1)}{q^{d_i}})$, we just consider the $\sum_{i=1}^{s} d_i = d$ equations which are constructed by *the linear independent system* $\{c_{i,j} \in GF(q)^m \mid 1 \leq i \leq s, 1 \leq j \leq d_i\}$, so there are q^{m-d} solutions. That is, there are q^{m-d} points in any subinterval $J = \prod_{i=1}^{s}[\frac{a_i}{q^{d_i}}, \frac{(a_i+1)}{q^{d_i}})$.

a $(d, m, m, s)-$system $\xrightarrow{\text{the digital method}}$ a digital $(m-d, m, s)-$net

3-1-2 Duality theory for digital nets [8, P.4 P.5, 7]

The problem of constructing good digital nets can now be viewed as the problem of constructing good linear codes in some metric spaces including Hamming spaces. The duality theory for digital nets was first applied in 2001 by H. Niederreiter, G. Pirsic [7].

Let $M \subseteq GF(q)^{ms}$ be the row space of the matrix M given below and $M^{\perp} \subseteq$

$GF(q)^{ms}$ be the perb space,

$$M = \begin{pmatrix} \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ c_{1,j} & c_{2,j} & \vdots & c_{s,j} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix}_{m \times ms}$$

Define a weight v on $GF(q)^m$ by $v(0) = 0$, and

$$v(a_i) = \max\{j : a_{ij} \neq 0\},$$

where $a_i = (a_{i1}, \cdots, a_{im})$. Moreover, a weight V_m on $GF(q)^{ms}$ is defined by

$$V_m(a_1, \cdots, a_s) = \sum_{i=1}^{s} v(a_i).$$

$$\begin{array}{ccc} GF(q)^{ms} \cong (GF(q)^m)^s & \xrightarrow{V_m} & \{0, 1, 2, \cdots, sm\} \\ \uparrow & & \\ GF(q)^m & \xrightarrow{v} & \{0, 1, 2, \cdots, m\} \end{array}$$

Note that $(GF(q)^{ms}, d_m)$ is a metric space with a metric $d_m(A, B) = V_m(A - B)$ for $A, B \in GF(q)^{ms}$. In the case $m = 1$, the weight $d_m(A, B) = V_m(A - B)$ is the classical Hamming space in coding theory.

Definition 3.2 [8, P.5] $\delta_m(N) = \min_{A \in N \setminus 0} V_m(A)$ for any nontrivial subspace N of $GF(q)^{ms}$.

A lower bound for t of digital $(t, m, s)-$nets obtained with $\delta_m(M^{\perp})$ is given by Theorem 3.3 [8, Theorem 4.3; 7, Theorem 1] in subsection 3-2-2. Moreover, Corollary

3.1 [8, Cor 4.4] combines Theorem 3.3 [8, Theorem 4.3; 7, Theorem 1] and duality with $t = m + 1 - \delta_m(M^{\perp})$ to obtain a good digital $(t, m, s)-$net in subsection 3-2-2.

3-1-3 Cyclic digital method [8, P.7]

An analog of cyclic codes for digital nets is introduced in this section. We adopt the viewpoint that cyclic codes can be defined by prescribing *roots of polynomials*.

$P = \{f \in GF(q^m)[x] \mid \deg(f) < s\} \cong GF(q)^{ms}$.
For $f(x) = \sum_{i=1}^{s} r_i(f)x^{i-1}$ with $r_i(f) = \sum_{j=1}^{m} c_{i,j}(f)B_{ij}$ where $B_i = (B_{i1}, B_{i2}, \cdots, B_{im})$ is an order basis of $GF(q^m)$ over $GF(q)$ and $c_i = (c_{i1}, c_{i2}, \cdots, c_{im}), 1 \leq i \leq s$. Then

$$\phi : f \in P \longrightarrow (c_1, c_2, \cdots, c_s) \in GF(q)^{ms}$$

is an isomorphism from P onto $GF(q)^{ms}$. Let further

$$P_\alpha = \{f \in P \mid f(\alpha) = 0, \alpha \in GF(q)\},$$

then $\dim(P_\alpha) = ms - m = \dim(\phi(P_\alpha)) = \dim N_\alpha$. By Corollary 3.1 [8, Cor 4.4], we can construct a digital net over $GF(q)$ with the subspace N_α, called *a cyclic digital net*.

To reduce cyclic digital nets to the classical cyclic codes would require that α be a root of $x^s - 1$. However, this would imply some restrictions on s, and so the condition that $(x - \alpha)|x^s - 1$ is not imposed on α. The advantage of the construction of digital nets in this section is that it works for any prime power q and any integers $m \geq 1$ and $s \geq 2$.

3-2 Some constructions

Preliminary and basic definitions have been given in subsection 3-1. In this section, we introduce the relation between digital nets and linear codes in terms of parity-check matrices and introduce how to construct a digital $(t, m, s)-$net. We will introduce two ideas for the constructions of digital nets. The first method is to produce $(d, m, m, s)-$systems in terms of *impulse response sequences*, and the second method is to produce the subspace $M^{\perp}$ by *duality theory*.

3-2-1 $(d, m, m, s)-$systems and the impulse response sequences

Corresponding to the problem of finding good linear codes in terms of their parity-check matrices, a $(m - t, m, m, s)-$system over $GF(q)$ can be used to construct a digital $(t, m, s)-$net by the digital method as shown in Theorem 3.1 [8, Theorem 2.1; 5, Theorem 6.1]. The difference between digital nets and linear codes is to be constructed by $c_{i,j}, 1 \leq i \leq s, 1 \leq j \leq m$ and $s \times 1$ array, respectively (by [8]).

Proposition 3.1 [8, P.4] If there exists a $(d, k, 1, s)-$system $\{c_i \in GF(q) \mid i \leq s\}$ with $s > k$ over $GF(q)$, then we obtain a linear code of length s, with dimension at least $s - k$, and with minimum distance at least $d + 1$ by using $c_1^T, \cdots, c_s^T$ as the columns of the parity-check matrix of the linear code.

From the digital method, if we fix m, s for a digital $(t, m, s)-$net, then the quality parameter t depends only on the choice of the matrices $C_1, C_2, \cdots, C_s$. And the following theorem show that the quality parameter t can be determined by independency of the row vectors $c_{i,j} \in GF(q)^m, 1 \leq j \leq m$ of $C_i, 1 \leq i \leq s$.

Theorem 3.1 [8, Theorem 2.1; 5, Theorem 6.1] $P(GF(q)^m)$ constructed by the digital method is a digital $(t, m, s)-$net with $t = m - d$ if any subsystem $\{c_{i,j} \in GF(q)^m \mid 1 \le i \le s, 1 \le j \le d_i\}$ with $\sum_{i=1}^{s} d_i = d \le m$ is linearly independent, i.e., $C = \{c_{i,j} \in GF(q)^m \mid 1 \le i \le s, 1 \le j \le m\}$ is a $(m - t, m, m, s)-$system.

Proof: For any subinterval $J = \prod_{i=1}^{s} [\frac{a_i}{q^{d_i}}, \frac{(a_i+1)}{q^{d_i}})$, let $a_i = \sum_{j=1}^{d_i} a_{i,j} \cdot q^{d_i - j}$ with $a_{i,j} \in \{0, 1, \cdots, q-1\}, 1 \le i \le s$. Then the point $P(x) \in J$, i.e.,

$$\frac{a_i}{q^{d_i}} \le \sum_{j=1}^{m} \frac{\psi(c_{i,j} \cdot x)}{q^j} < \frac{(a_i + 1)}{q^{d_i}}, 1 \le i \le s.$$

Moreover,

$$\frac{\sum_{j=1}^{d_i} a_{i,j} \cdot q^{d_i - j}}{q^{d_i}} \le \sum_{j=1}^{m} \frac{\psi(c_{i,j} \cdot x)}{q^j} < \frac{\sum_{j=1}^{d_i} a_{i,j} \cdot q^{d_i - j}}{q^{d_i}} + \frac{1}{q^{d_i}},$$

i.e.,

$$\sum_{j=1}^{d_i} \frac{a_{i,j}}{q^j} \le \sum_{j=1}^{m} \frac{\psi(c_{i,j} \cdot x)}{q^j} < \sum_{j=1}^{d_i} \frac{a_{i,j}}{q^j} + \frac{1}{q^{d_i}} \text{(unique representation)}.$$

It implies that $\psi(c_{i,j} \cdot x) = a_{i,j}, i \le s, 1 \le j \le d_i$, i.e.,

$$\sum_{j=1}^{m} c_{i,jr} \cdot x_r = \psi^{-1}(a_{i,j}), 1 \le i \le s, 1 \le j \le d_i.$$

Hence there are q^t solutions. Q.E.D.

A method for constructing the system C is given in [6] in terms of the notion of impulse response sequences. We will show that the system C is a $(d, m, m, s)-$system for $\sum_{i=1}^{s} d_i = d$, which turns out to be a digital $(t, m, s)-$net by Theorem 3.1 [8, Theorem 2.1; 5, Theorem 6.1] as follows.

Definition 3.3 Let $g(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0$ be a monic polynomial of degree $n \ge 1$ over $GF(q)$. *The impulse response sequence* with characteristic polynomial g is defined by

$$w_i = \begin{cases} 0 & \text{, if } 1 \le i \le n-1, \\ 1 & \text{, if } i = n. \end{cases} \text{ (the initial condition), and}$$

$$w_{r+n} = a_{n-1}w_{r+n-1} + \cdots + a_0 w_r, r > 0.$$

Note that $g(x)\sum_{r=1}^{\infty} w_r x^{-r} = 1$ by a simple calculation such that $\sum_{r=1}^{\infty} w_r x^{-r} = \frac{1}{g(x)}$.

Let $p_1, p_2, \cdots$ be all monic irreducible polynomials over $GH(q)$ with $\deg(p_i) = e_i, 1 \le i \le s-1$. Let $w_i(j,r), r = 1, 2, \cdots$, be *the impulse sequence* with characteristic polynomial p_i^j, and define $c_{i,j} = (c_{i,j1}, \cdots, c_{i,jm}) \in GF(q)^m$ for $1 \le i \le s, 1 \le j \le m_i$, where $j - 1 = t_{i,j}e_i + u_{i,j}, 0 \le u_{i,j} < e_i$, and

$$c_{i,jr} = \begin{cases} w_i(t_{i,j}+1, r+u_{i,j}) & \text{, for } 1 \le i \le s-1, 1 \le j \le m_i, 1 \le r \le m, \\ \delta_{r-1,m-j} & \text{, for } 1 \le j \le m_s, 1 \le r \le m. \end{cases}$$

A lower bound for $R(GF(q)^m; m_1, \cdots, m_s)$ in terms of the impulse response sequence is given below:

Proposition 3.2 [6, Prop 1] $\rho(C) = \min \sum_{i=1}^{s} d_i \ge m + 1 - \sum_{i=1}^{s-1}(e_i - 1)$.

Proof: Suppose in contradiction that $\rho(C) \le m - \sum_{i=1}^{s-1}(e_i - 1)$, then there exists integers d_i's with $1 \le \sum_{i=1}^{s} d_i \le m - \sum_{i=1}^{s-1}(e_i - 1)$ such that the subsystem $\{c_{i,j} \in GF(q)^m \mid 1 \le i \le s, 1 \le j \le d_i\}$ is linearly dependent. We have a linear dependence relation

$$\sum_{i=1}^{s}\sum_{j=1}^{d_i} f_{i,j}c_{i,j} = 0 \in GF(q)^m,$$

where $f_{i,j}$ are not all 0, i.e., $\sum_{i=1}^{s}\sum_{j=1}^{d_i} f_{i,j}c_{i,jr} = 0, 1 \le r \le m$.

We then consider the power series

$$P = \sum_{r=1}^{\infty}(\sum_{i=1}^{s}\sum_{j=1}^{d_i} f_{i,j}c_{i,jr})x^{-r} = \sum_{j=1}^{d_s} f_{s,j}\sum_{r=1}^{\infty} c_{s,jr}x^{-r} + \sum_{i=1}^{s-1}\sum_{j=1}^{d_i} f_{i,j}\sum_{r=1}^{\infty} c_{i,jr}x^{-r}$$

$$= \sum_{j=1}^{d_s} f_{s,j}x^{-m+j-1} + \sum_{i=1}^{s-1}\sum_{j=1}^{d_i} f_{i,j}\sum_{r=1}^{\infty} w_i(t_{i,j}+1, r+u_{i,j})x^{-r},$$

where $\sum_{r=1}^{\infty} w_i(t_{i,j}+1, r+u_{i,j})x^{-r}$

$$= \sum_{r=u_{i,j}+1}^{\infty} w_i(t_{i,j}+1, r)x^{-r+u_{i,j}}$$

$= \sum_{r=1}^{\infty} w_i(t_{i,j}+1, r)x^{-r+u_{i,j}}$

(by the initial condition $w_i(t_{i,j}+1, r) = 0, 1 \le r \le u_{i,j} < e_i$)

$= x^{u_{i,j}} \sum_{r=1}^{\infty} w_i(t_{i,j}+1, r)x^{-r}$

$= \frac{x^{u_{i,j}}}{p_i(x)^{t_{i,j}+1}}$.

Since $j-1 = t_{i,j}e_i + u_{i,j}$, we define $0 \le t_{i,j} \le b_i = \frac{(d_i-1)}{e_i}$, and $0 \le u_{i,j} \le e_i - 1$. Thus,

$$P - \sum_{j=1}^{d_s} f_{s,j}x^{-m+j-1} = \sum_{i=1}^{s-1}\sum_{b=1}^{b_i} \frac{g_{ib}(x)}{p_i(x)^b}, \qquad (*)$$

where $g_{ib} \in GF(q)[x]$, and $\deg(g_{ib}) < e_i$. With $h = \prod_{i=1}^{s-1} p_i^{b_i+1}$, we have

$$\deg(h) = \sum_{i=1}^{s-1} e_i(b_i+1) \le \sum_{i=1}^{s-1}(d_i + b_i - 1) = \sum_{i=1}^{s-1} d_i + \sum_{i=1}^{s-1}(e_i - 1) \le m - d_s.$$

If we multiply (*) by h, then we get a polynomial on the right-hand side, while we only have negative powers of x on the left-hand side because $\deg(P) < -m$. This is possible if both sides of (*) are 0. By the uniqueness of the partial fraction decomposition, this implies $g_{ib} = 0$ for $1 \le i \le s-1, 1 \le b \le b_i + 1$, that is, $f_{i,j} = 0, 1 \le i \le s-1, 1 \le j \le d_i$. Then we get $f_{s,j} = 0, 1 \le j \le d_i$ by the equation $\sum_{i=1}^{s}\sum_{j=1}^{d_i} f_{i,j}c_{i,jr} = 0, 1 \le r \le m$. This contradiction proves the proposition. Q.E.D.

By the proof of Proposition 3.2 [6, Prop 1], we know that any subsystem $\{c_{i,j} \in GF(q)^m \mid 1 \le i \le s, 1 \le j \le d_i\}$ with $\sum_{i=1}^{s} d_i = d = m - \sum_{i=1}^{s-1}(e_i - 1)$ of the system C which is constructed from the impulse response sequence is linearly independent. Hence the system C is a $(d, m, m, s)-$system. Further, if we choose monic irreducible polynomials over $GF(q)$ for the impulse sequence with smallest degree, then we can get the larger value of $d = m - D_q(s-1)$ to construct a better digital net as follows. Let

$$M_q(n) = \sum_{h=1}^{n} N_q(h), D_q(t) = \sum_{h=1}^{n}(h-1)N_q(h) + (t - M_q(n))n,$$

where $N_q(n)$ be the number of monic irreducible polynomials over $GF(q)$ of degree n, and $n = n(q,t)$ is the largest integer with $M_q(n) \leq t$.

Theorem 3.2 [6, P.225∼P.226]

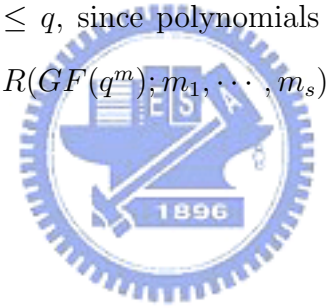
$R(GF(q^m); m_1, \cdots, m_s) \geq m + 1 - D_q(s-1)$ if $s \geq 2$ (Theorem 1),

$R(GF(q^m); m_1, \cdots, m_s) \geq 3$ if $m \geq 2$ and $s \leq \frac{q^m-1}{q-1}$ (Proposition 2),

$R(GF(q^m); m_1, \cdots, m_s) = 2$ if $s > \frac{q^m-1}{q-1}$ (Proposition 3).

Proof: Let $p_1, p_2, \cdots$ be all monic irreducible polynomial over $GF(q)$ with increasing degrees. Put e_i =deg(p_i) for $1 \leq i \leq s-1$, so $\sum_{i=1}^{s-1}(e_i - 1) = D_q(s-1)$. By proposition 3.2 [6, Propostion 1], $R(GF(q^m); m_1, \cdots, m_s) \geq m+1-D_q(s-1)$. Q.E.D.

Note that $D_q(t) = 0, t \leq q$, since polynomials $x + a, a \in GF(q)$ are monic irreducible polynomials. Then $R(GF(q^m); m_1, \cdots, m_s) = m+1$ for $s \leq q+1$ by Theorem 3.2 [6, Theorem 1].



3-2-2 The duality theory

From above, we know the relation between digital nets and $(d, m, m, s)-$systems. Next, we introduce how to find the large possible value of d to construct good digital nets by duality theory [7, 8].

Proposition 3.3 [8, Prop 4.2; 7, Prop 1] For any nonzero subspace N of $GF(q)^{ms}$, we have $\delta_m(N) \leq ms + 1 - \dim(N)$.

Proof: Let $\dim(N) = h$, and the linear transformation $\pi : N \to GF(q)^h$ defined by $\pi(n_1, \cdots, n_{ms}) = (n_{ms-h+1}, \cdots, n_{ms})$. If π is surjective, then there is a nonzero vector $A_1 \in N$ such that $\pi(A_1) = (1, 0, \cdots, 0)$. So $V_m(A_1) \leq ms - h + 1$. Otherwise, there

is a nonzero vector $A_2 \in \ker(\pi)$ such that $\pi(A_2) = (0, 0, \cdots, 0)$. So $V_m(A_2) \leq ms - h$. Thus, $\delta_m(N) \leq ms + 1 - \dim(N)$. Q.E.D.

The following theorem for duality theory is related to Theorem 3.1 [8, Theorem 2.1; 5, Theorem 6.1]. The idea is that $P(GF(q)^m)$ is *a digital* $(t, m, s)-$*net* if and only if the system $C = \{C_1, C_2, \cdots, C_s\}$ *is a* $(d, m, m, s)-$*system* if and only if $\delta_m(M^{\perp}) \geq m + 1 - t$.

Theorem 3.3 [8, Theorem 4.3; 7, Theorem 1] The digital net $P(GF(q)^m)$ is a $(t, m, s)-$digital net over $GF(q)$ if and only if $\delta_m(M^{\perp}) \geq m + 1 - t$.

Proof: Let $m - t = d = \sum_{i=1}^{s} d_i$.
$(\Rightarrow)P(GF(q)^m)$ is a digital $(t, m, s)-$net if and only if the system $C = \{C_1, C_2, \cdots, C_s\}$ is a $(d, m, m, s)-$system. For any nonzero vector $A = (a_1, \cdots, a_s)$ for $a_i \in GF(q)^m$, and $v(a_i) = v_i$. Then $MA^T = 0 \in GF(q)^m$, i.e., $\sum_{i=1}^{s} \sum_{j=1}^{v_i} a_{ij} c_{i,j} = 0 \in GF(q)^m$. So $\{c_{i,j} \in GF(q)^m \mid 1 \leq i \leq s, 1 \leq j \leq v_i\}$ is dependent, i.e., $V_m(A) = \sum_{i=1}^{s} v_i \geq d + 1$. Thus, $\delta_m(M^{\perp}) \geq d + 1$.
$(\Leftarrow)$Suppose in contradiction that $P(GF(q)^m)$ is not a digital $(t, m, s)-$net. Then the subsystem $\{c_{i,j} \in GF(q)^m \mid 1 \leq i \leq s, 1 \leq j \leq d_i\}$ is dependent, i.e., $\sum_{i=1}^{s} \sum_{j=1}^{d_i} a_{ij} c_{i,j} = 0 \in GF(q)^m$ not all a_{ij} are zero. So $\sum_{i=1}^{s} \sum_{j=1}^{m} a_{ij} c_{i,j} = 0 \in GF(q)^m$, where $a_{ij} = 0, 1 \leq i \leq s, d_i < j \leq m$ such that $A = (a_1, \cdots, a_s) \in M^{\perp}$, and $V_m(A) \leq d$, i.e., $\delta_m(M^{\perp}) \leq d$ a contradiction, as required. Q.E.D.

The following procedure for constructing good digital nets on the basis of duality theory is based on Theorem 3.3 [8, Theorem 4.3; 7, Theorem 1]:
(i) construct a subspace N of $GF(q)^{ms}$ with $\dim(N) \geq ms - m$ and a value of $\delta_m(N)$. (compatible with Proposition [8, Prop 4.2])
(ii) dualize N to get M, the digital net is determines.

In the notation of Theorem 3.3 [8, Theorem 4.3; 7, Theorem 1] we have $N = M^{\perp}$. Note that trivially $\dim(N) \geq ms - m$, we have

$$\dim(N) = ms - \dim(M) \geq ms - m$$

as stated in (i). In the end, this procedure yield a digital $(t, m, s)-$net over $GF(q)$ with $t \geq m + 1 - \delta_m(\mathrm{N})$. For constructing good digital nets by the subspace N, we choose the small value of $t = m + 1 - \delta_m(N)$ such that the digital $(t, m, s)-$net with the stronger the uniform distribution property. It was summarized in the following corollary.

Corollary 3.1 [8, Cor 4.4] If the subspace N of $GF(q)^{ms}$ with $\dim(N) \geq ms - m$, then we can construct a digital $(t, m, s)-$net with $t = m + 1 - \delta_m(N)$.

In order to get better digital nets, we need to construct the subspace N with the maximum number $\delta_m(N)$. And by cyclic digital method in section 2, we can construct a subspace N of $GF(q)^{ms}$ with $\dim(N) = ms - m$, and then using Corollary 3.1 [8, Cor 4.4] helps to construct a good cyclic digital net over $GF(q)$.

Some examples of digital $(t, m, s)-$nets over $GF(q)$ with $q = 3, 4$ are given below for illustration purpose by the two methods introduced in subsection 3-2. We will construct a $(d, m, m, s)-$system by the response sequence in Examples 1 and 2, and the subspace $M^{\perp}$ by duality theory in Example 3.

$$GF(2^2) = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle = \{0, x, x^2, x^3\} = \{0, x, x+1, 1\}.$$

$$GF(3^2) = \mathbb{Z}_3[x]/\langle x^2 + 2x + 2\rangle = \{0, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8\}$$

$$= \{0, x, x{+}1, 2x{+}1, -1, 2x, 2x{+}1, x{+}2, 1\}.$$

Example 1 A digital $(1,3,5)-$net over $GF(3)$ constructed by a $(2,3,3,5)-$system.

Let $s=5, m=3, GF(q)=\mathbb{Z}_3$, and let monic polynomials

$$p_1=x, p_2=x-1, p_3=x-2, p_4=x^2+1.$$

Thus, there is a $(2,3,3,5)-$system as follows: (Appendix 1)

	C_1			C_2			C_3			C_4			C_5		
$c_{i,1}$	1	0	0	1	1	1	1	2	1	0	1	0	0	0	1
$c_{i,2}$	0	1	0	0	1	2	0	1	1	1	0	2	0	1	0
$c_{i,3}$	0	0	1	0	0	1	0	0	1	0	0	0	1	0	0

The point set for the digital $(1,3,5)-$net over $GF(3)$ constructed by the $(2,3,3,5)-$system is shown in Appendix 2.

Example 2 A digital $(0,3,5)-$net over $GF(2^2)$ constructed by a $(3,3,3,5)-$system.

Let $s=5, m=3, GF(2^2)=\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$, and let monic polynomials

$$p_1(y)=y, p_2(y)=y+x, p_3(y)=y+(x+1), p_4(y)=y+1.$$

Thus, there is a $(3,3,3,5)-$system as follows:

	C_1			C_2			C_3			C_4			C_5		
$c_{i,1}$	1	0	0	1	x	$x+1$	1	$x+1$	x	1	1	1	0	0	1
$c_{i,2}$	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0
$c_{i,3}$	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0

The point set for the digital $(0,3,5)-$net over $GF(2^2)$ constructed by the $(3,3,3,5)-$system is shown in Appendix 3.

Example 3 A digital $(2,3,5)-$net over $GF(2^2)$ constructed by the duality theory for a subspace $M^\perp$ with $\dim(M^\perp)=ms-m=12$.

Let $s=5, m=3, GF(2^2)=\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$, and $M^\perp=\langle e_2, e_5, e_6, \cdots, e_{15}\rangle$. Hence $\delta_m(M^\perp)=2$ such that $t=m+1-\delta_m(M^\perp)=2$, the system chosen from

$C = \{C_1, C_2, \cdots, C_5\}$ is as follows:

	C_1			C_2			C_3			C_4			C_5		
$c_{i,1}$	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
$c_{i,2}$	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
$c_{i,3}$	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0

The point set for the digital $(2, 3, 5)-$net over $GF(2^2)$ constructed by the duality theory for the subspace $M^{\perp}$ is shown in Appendix 4.

4 Disjunct, Separable Matrices with Error Tolerance

In this thesis, we treat *superimposed codes* (or *superimposed designs*) as matrices of order $t \times N$ with columns of M as their code words, i.e., the column-indexed by *the object* to be tested and the row-indexed by *the test*. And we call the matrix M *a disjunct matrix* (or *a separable matrix*).

Some papers about disjunct matrices and separable matrices will be reviewed in subsection 4-1. The minimum Hamming distance over all boollean sums of m columns e_m (respectively of at least m columns $e_{\leq m}$) for some matrices will be evaluated some examples of disjunct matrices and separable matrices in subsection 4-2. Moreover, we will introduce some generalizations of disjunct matrices and separable matrices, their relations which inherit relations of $(s, l)-$disjunct matrices and $(s, l)-$separable matrices, and the concatenated construction in subsection 4-3. Some relationship between $(d, k, m, s)-$systems and superimposed codes are given in section 4-4, i.e., superimposed $(a, b)-$codes can be constructed by $(d, k, m, s)-$systems.

4-1 Disjunct matrices and separable matrices

The notions of $d-$disjunct, $d-$separable, and $\bar{d}-$separable will be introduced first, and followed by a survey of related results in the literature.

Definition 4.1 ($d-$disjunct, $d-$separable, and $\bar{d}-$separable)

1. M is $d-$disjunct if no column is contained in the union of any other d columns.
2. M is $d-$separable if no two unions of d columns are identical.
3. M is $\bar{d}-$separable if no two unions of at most d columns are identical.

In biological experiments, we want to save money and time, so we hope to identify

the larger objects with as few group tests as possible. And it is important to save time that all test subsets are specified before any testing is done, known as *nonadaptive group testing*, ex. DNA, blood testing. And disjunct matrices and separable matrices are tools for nonadaptive group testing. So the maximum number N and the minimum number t for the disjunct matrix (or the separable matrix) M of order $t \times N$ is considered with interests.

The definitions of *superimposed* $(s,1)-$*codes* and $d-$*separable matrices* were first introduced in 1964 by Kautz and Singleton [3]. The relations between superimposed $(s,1)-$codes and $d-$separable matrices was considered, i.e.,

$$\text{si}(s,1) - \text{codes} \Rightarrow s - \text{separable matrices} \Rightarrow \text{si}(s-1,1) - \text{codes},$$

and the maximum number N of code words for superimposed $(s,1)-$codes (or superimposed $(s,1)-$designs) was with interests, i.e., the maximum number N of columns for the matrix M of order $t \times N$. Moreover, the paper [2] introduced the constructions of superimposed codes and superimposed designs, for instance, the constructions for superimposed codes based on q_0-*ary codes* (the concatenated construction) and for superimposed designs based on parity-check matrices and on graphical construction.

The definition of d^e-*disjunct matrices* was first given in 1997 by A. Macula [4], i.e., error-correcting codes for $d-$disjunct matrices. The minimum Hamming distance $d_H(B_d(M))$ over the set of the boolean sums of any at most d columns of the d^e-disjunct matrix M was also considered. Moreover, it provided the construction of d^e-disjunct matrices.

The definition of $(s,l)-$*superimposed codes* and *superimposed* $(s,l)-$*designs* were defined in 2002 by A. D'yachkov and P. Vilenkin, A. Macula, D. Torney [2]. As the pa-

per by Kautz and Singleton [3], this paper gave a construction based on $q_0-ary\ codes$ and considered the bound of the maximum number N for superimposed $(s,l)-$codes M of order $t \times N$. Moreover, it also discuss the construction based on *MDS-codes* and the bound of the minimum number t.

Separable matrix(or disjunct) M of order $t \times N$ with N as large as possible are of interests for practical purpose. It was introduced in 1964 by Kautz and Singleton [3] to construct $2-$separable matrices M with constant columns weight 2 by BIBID and graphical constructions as follows.

1. The split-field case of M of order $t \times N$ by BIBD construction: two ones are separated into the upper portion and the lower portion.

Let the upper portion contain the first v rows of M, and the lower portion contain the last b rows of M such that $v + b = t$. Then the matrix M is transformed to the binary matrix Z of order $v \times b$ with $Z(i,j) = 1$ if and only if there is a column of M with two ones in the ith row of the upper portion and jth row of the lower portion. So N is equal to two the number of ones in Z. Note that if M is $2-$separable, then Z have no pair rows have two ones in the same column. Hence we seek for Z with interests to contain a maximum number N of ones and with the dot product of any two rows does not exceed 1.

Moreover, Z is allowed to be a incidence matrix of a BIBD(v,k,b,r,λ), where $t = v + b, N = kb, \lambda = 1$. Since the equalities $bk = vr, r(k-1) = \lambda(v-1)$ hold for BIBD, N will be maximized for fix t as $v = b$ and $k = r$. Thus, Z is a incidence matrix of a symmetric BIBD(v,k,b,r,λ), where $t = 2v = 2(k^2-k+1), N = kv = k(k^2-k+1))$ and $k-1$ is a prime power, i.e., $N = \frac{t}{4}(1+\sqrt{2t-3})$.

2. Consider the case that two ones are not restricted to separable portions of M by graphical construction.

Let each of the t rows in M be represented as a vertex of a graph with t vertices. There is an edge between vertex i and j if and only if there is a column with two ones in the ith and the jth row. So N is equal to the number of edges in the graph. Note that if M is $2-$separable, then no pair adjacent-edges are incident with the same set of vertices as other pair adjacent-edges, i.e., there is no cycles of length less than 5. Thus, we seek for a $t-$vertex graph containing maximum N edges with no closed cycles of length < 5. Complete regular graphs of this type are called *Moore graphs*, and all possible Moore graphs are as follows:

degree(d)	vertex number (t)	edge number (N)	graph
2	5	5	C_5
3	10	15	Peterson graph
7	50	175	Hoffman-Singleton graph
57	3250	92625	undecided

And the parameters t, N are related to the degree d such that $t = 1 + d^2$, and $N = \frac{td}{2} = \frac{d(1+d^2)}{2}$, i.e., $N = \frac{t\sqrt{t-1}}{2}$.

4-2 The parameters $e_m, e_{\leq m}$ and its $q-$analogue for error tolerance

$\bar{d}-$separable matrices was introduced in subsection 4-1, and we will consider the error tolerance of the boolean sums of any at most d columns in the matrix over the Johnson schemes and the Grassmann schemes in subsection 4-2-2.

Definition 4.2 $(d_H(M), B_d(M))$

$d_H(M)$ = the minimum over Hamming distances between pairs of columns of M.

$B_d(M)$ = the binary matrix whose columns consist exactly of all the Boolean sums

$\bigcup_{j\in S} c_j(M)$ over all subsets S of $[n]$ with size at most d.

The minimum Hamming distance $d_H(B_d(M)) \geq 2e$ over the set of the boolean sums of any at most d columns of a $d^{(e-1)}-$disjunct matrix M (a $(d,1;e)-$disjunct matrix) [4, Proposition 3]. And the similar parameters e_m and $e_{\leq m}$ over the Johnson schemes, the Grassmann schemes are counted in this section.

4-2-1 The parameters e_m and $e_{\leq m}$

Let $1 < d < n$ be positive integers, and let M be the matrix row-indexed (resp. column-indexed) by all $d-$subsets (resp. all $k-$subsets) of such that $M(A,B) = 1$ if $A \subseteq B$ and 0 otherwise. For a subfamily $D \subseteq \begin{pmatrix} [n] \\ k \end{pmatrix}$, let $B(D)$ be the *boolean sum* of those columns of M corresponding to those $k-$subsets in D. Similarly, we consider its $q-$analogue as follows, and let M_q be the $(0,1)-$matrix row-indexed (resp. column-indexed) by all $d-$subspaces (resp. all $k-$subspaces) of $GF(q)^n$ such that $M_q(A,B) = 1$ if $A \subseteq B$ and 0 otherwise.

Define

$$\begin{aligned} &d_H(B(D), B(D')) = \text{the number of different symmetric of } B(D) \text{ and } B(D') \\ &= |\{C \subseteq \begin{pmatrix} [n] \\ d \end{pmatrix} \text{ or } \begin{bmatrix} n \\ d \end{bmatrix}_q \mid C \text{ is conatined in some member of } D \text{ (or } D'), \\ &\qquad\qquad \text{but not in each member of } D' \text{ (or } D')\}|, \end{aligned}$$

and

$$\begin{aligned} e_m &= \min_{|D| = |D'| = m} d_H(B(D), B(D')), \\ e_{\leq m} &= \min_{\text{antichain } D, D' \text{ with } |D| = |D'| \leq m} d_H(B(D), B(D')). \end{aligned}$$

The parameters $e_m, e_{\leq m} > 0$ for the matrix M imply that the matrix M is $m-$separable and $\bar{m}-$separable, respectively. In general, the matrix M is $(m,1;e)-$separable

as $0 < e \leq \frac{e_{\leq m}}{2}$, and strictly it is also $(m, 1; e)-$disjunct as $0 < e \leq \frac{e_{\leq m}}{2}$. So the larger parameter $e_{\leq m}$ implies the better error tolerance is over the matrix M over the Johnson schemes and the Grassmann schemes. And we will consider how the parameters d, k, m are related to e_m (or $e_{\leq m}$) as follows.

4-2-2 The Parameters over the Johnson schemes and the Grassmann schemes

An elegant proof of Theorem 4.1 is given in this section. Its $q-$analog is given in Theorem 4.2, and an asympototic approximation for the bound is of its own interests. We will consider the number $d_H(B(D), B(D'))$ for specific examples before deriving the parameters $e_m, e_{\leq m}$ over the *Johnson schemes* and the *Grassmann schemes*.

Let $D = \{D_1, D_2, \cdots, D_m\}$ and $D' = \{D'_1, D'_2, \cdots, D'_m\} \subseteq \begin{pmatrix} [n] \\ k \end{pmatrix}$. By the definition,

$$\begin{aligned} e_m = & \min_{|D| = |D'| = m} d_H(B(D), B(D')) \\ & \geq \min|\{C \mid C \subseteq D_i \text{ for some } i \in [m] \text{ and } C \nsubseteq D'_j \text{ for all } j \in [m]\}| \\ & + \min|\{C \mid C \subseteq D'_i \text{ for some } i \in [m] \text{ and } C \nsubseteq D_j \text{ for all } j \in [m]\}| \\ & = 2 \cdot \min|\{C \mid C \subseteq D_i \text{ for some } i \in [m] \text{ and } C \nsubseteq D'_j \text{ for all } j \in [m]\}| \\ & \quad \text{(by the symmetry)} \\ & = 2 \cdot \min|\{C \mid C \subseteq D_i \text{ for some } i \in [m] \text{ and } C \nsubseteq D_i \cap D'_j \text{ for all } j \in [m]\}|. \end{aligned}$$

Hence $d_H(B(D), B(D'))$ for sets D, D' achieve e_m when the choices of i is as few as possible and the number of $|D_i \cap D'_j|$ for all $j \in [m]$ is as large as possible.The following examples provided partial information for the parameter under consideration. Similar results hold for the Grassmann schemes, too.

Example 1 For $m \leq k$, $D_0 = \{\hat{1}, \hat{2}, \cdots, m\hat{-}1, \hat{k}\}$, and $D_0' = \{\hat{1}, \hat{2}, \cdots, m\hat{-}1, k\hat{+}1\}$ of $k-$subsets of $[n]$, where $\hat{i} = [k+1] - \{i\}$ for $1 \leq i \leq k+1$. Then

$$\begin{aligned}
&d_H(B(D_0), B(D_0')) \\
&= |\{C \mid C \in \begin{bmatrix} [k] \\ d \end{bmatrix}, C \nsubseteq \hat{1}, \hat{2}, \cdots, m\hat{-}1, \hat{k}\}| \\
&+|\{C \mid C \in \begin{bmatrix} \hat{k} \\ d \end{bmatrix}, C \nsubseteq \hat{1}, \hat{2}, \cdots, m\hat{-}1, k\hat{+}1\}| \\
&= 2 \cdot |\{C \mid \{1, 2, \cdots, m-1, k\} \subseteq C \in \begin{bmatrix} [k] \\ d \end{bmatrix}\}| \\
&= \begin{cases} 2 \cdot \begin{bmatrix} k-m \\ d-m \end{bmatrix} & \text{, if } m \leq d, \\ 0 & \text{, if } d < m \leq k. \end{cases}
\end{aligned}$$

Example 2 For $m > k$, $D_0 = \{\hat{1}, \hat{2}, \cdots, k\hat{-}1, \hat{k}, D_{k+1}, D_{k+2}, \cdots, D_m\}$, and $D_0' = \{\hat{1}, \hat{2}, \cdots, k\hat{-}1, k\hat{+}1, D_{k+1}, D_{k+2}, \cdots, D_m\}$ of $k-$subsets of $[n]$, where $\hat{i} = [k+1]-\{i\}$ for $1 \leq i \leq k+1$ and $D_{k+1}, D_{k+2}, \cdots, D_m \in \begin{bmatrix} [n] \\ k \end{bmatrix}$. Then

$$\begin{aligned}
&d_H(B(D_0), B(D_0')) \\
&= 2 \cdot |\{C \mid C \in \begin{bmatrix} [k] \\ d \end{bmatrix}, C \nsubseteq \hat{1}, \hat{2}, \cdots, k\hat{-}1, k\hat{+}1, D_{k+1}, D_{k+2}, \cdots, D_m\}| \\
&\leq 2 \cdot |\{C \mid C \in \begin{bmatrix} [k] \\ d \end{bmatrix}, C \nsubseteq \hat{1}, \hat{2}, \cdots, k\hat{-}1, k\hat{+}1\}| \\
&\leq 2 \cdot |\{C \mid \{1, 2, \cdots, k-1, k\} \subseteq C \in \begin{bmatrix} [k] \\ d \end{bmatrix}\}| \\
&= 0 \text{ (for } d < k).
\end{aligned}$$

The above two examples show that the parameter $d_H(B(D_0), B(D_0'))$ is actually equal to e_m (or $e_{\leq m}$) in Theorem 4.1. Similar arguments work well for the Grassmann schemes, and we will show them in Lemma 4.1 and Lemma 4.2.

Example 3 For $V \in \begin{bmatrix} n \\ k+1 \end{bmatrix}_q$, $m \leq q+k-1$, $D_0 = \{D_1, D_2, \cdots, D_{m-1}, D_m\}$ and $D_0' = \{D_1, D_2, \cdots, D_{m-1}, D_{m+1}\}$ of $k-$subspaces of $GF(q)^n$, where $D_1, \cdots, D_m, D_{m+1} \in \begin{bmatrix} V \\ k \end{bmatrix}_q$, and the dimension of any intersection of $r \leq k+1$ subspaces $D_i, 1 \leq i \leq m$ is $k-r+1$. So

$d_H(B(D_0), B(D_0'))$
$= |\{C \mid C \in \begin{bmatrix} D_m \\ d \end{bmatrix}_q C \nsubseteq D_1, D_2, \cdots, D_{m-1}, D_{m+1}\}|$
$+|\{C \mid C \in \begin{bmatrix} D_{m+1} \\ d \end{bmatrix}_q, C \nsubseteq D_1, D_2, \cdots, D_{m-1}, D_m\}|$
$= 2(\begin{bmatrix} k \\ d \end{bmatrix}_q - \begin{pmatrix} m \\ 1 \end{pmatrix} \begin{bmatrix} k-1 \\ d \end{bmatrix}_q + \begin{pmatrix} m \\ 2 \end{pmatrix} \begin{bmatrix} k-2 \\ d \end{bmatrix}_q - \cdots + (-1)^{k-d} \begin{pmatrix} m \\ k-d \end{pmatrix} \begin{bmatrix} k-(k-d) \\ d \end{bmatrix}_q)$
$= 2 \cdot \sum_{i=0}^{k-d} (-1)^i \begin{pmatrix} m \\ i \end{pmatrix} \begin{bmatrix} k-i \\ d \end{bmatrix}_q.$

Example 4 For $m > \begin{bmatrix} k+1 \\ k \end{bmatrix}_q - \begin{bmatrix} k+1-d \\ k-d \end{bmatrix}_q$, $D_0 = \{D_1, D_2, \cdots, D_{m-1}, D_m\}$ and $D_0' = \{D_1, D_2, \cdots, D_{m-1}, D_{m+1}\} \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$. Then the parameter $d_H(B(D_0), B(D_0')) = 0$ by Lemma 4.2.

Theorem 4.1 ($e_m, e_{\leq m}$ over the Johnson schemes)

1. $e_m = \min_{|D| = |D'| = m} d_H(B(D), B(D')) = \begin{cases} 2 \cdot \begin{pmatrix} k-m \\ d-m \end{pmatrix} & \text{, if } m \leq d, \\ 0 & \text{, otherwise.} \end{cases}$

2. $e_{\leq m} = \min_{\text{antichain } D, D' \text{ with } |D| = |D'| \leq m} d_H(B(D), B(D')) = e_m$

Proof:

1. Since $e_m \leq 2 \cdot \begin{pmatrix} k-m \\ d-m \end{pmatrix}$ if $m \leq d$ and $e_m = 0$ if $m > d$ as shown in Examples 1 and 2, it suffices to show that it is also a lower bound for $m \leq d$. We identify $D = \{D_1, D_2, \cdots, D_m\}$ and $D' = \{D_1', D_2', \cdots, D_m'\} \subseteq \begin{pmatrix} [n] \\ k \end{pmatrix}$. Since $|D \cap D'| \leq m-1$ and $m \leq d$, without loss of generality, we assume that $D_m \notin D'$ and $D_m' \notin D$. For each $i \in [m]$, there is an element $x_i \in D_m \setminus D_i'$, so $\{x_i\}_{i \in [m]} \subseteq D_m$ consists of at most m elements, but $\{x_i\}_{i \in [m]} \nsubseteq D_j', j = 1, 2, \cdots, m$. Hence there are at least $\begin{pmatrix} k-m \\ d-m \end{pmatrix}$ $d-$subsets contained in $B(D)$, but not in $B(D')$. By the symmetry argument, we get $e_m \geq 2 \cdot \begin{pmatrix} k-m \\ d-m \end{pmatrix}$, and it follows that $e_m = 2 \cdot \begin{pmatrix} k-m \\ d-m \end{pmatrix}$ whenever $m \leq d$ and $e_m = 0$ otherwise.

2. Since $e_{\leq m} \leq e_m$, $e_{\leq m} \leq \begin{pmatrix} k-m \\ d-m \end{pmatrix}$ if $m \leq d$ and $e_{\leq m} = 0$ if $m > d$. So we just prove the lower bound of $e_{\leq m}$ for $m \leq d$ as follows.

We identify two antichains $D = \{D_1, \cdots, D_r\}$ and $D' = \{D'_1, \cdots, D'_s\} \subseteq \begin{pmatrix} [n] \\ k \end{pmatrix}$, $r, s \leq m$. Since $|D \cap D'| \leq \min\{r-1, s-1\}$ and $m \leq d$, we assume that $D_r \notin D'$ and $D'_s \notin D$. For each $i \in [s]$, there is an element $x_i \in D_r \setminus D'_i$ such that $\{x_i\}_{i\in[s]}$ consisting of at most s elements with $\{x_i\}_{i\in[s]} \subseteq D_r$ and $\{x_i\}_{i\in[s]} \nsubseteq D'_j, j = 1, 2, \cdots, s$. So there are at least $\begin{pmatrix} k-s \\ d-s \end{pmatrix}$ $d-$subsets contained in $B(D)$, but not in $B(D')$. By the symmetry argument, we get $e_{\leq m} \geq \begin{pmatrix} k-s \\ d-s \end{pmatrix} + \begin{pmatrix} k-r \\ d-r \end{pmatrix}, r, s \leq m$ such that $e_{\leq m} \geq 2 \cdot \begin{pmatrix} k-m \\ d-m \end{pmatrix}$, and it follows that $e_{\leq m} = 2 \cdot \begin{pmatrix} k-m \\ d-m \end{pmatrix}$ whenever $m \leq d$ and $e_{\leq m} = 0$ otherwise. Q.E.D.

Similar arguments work for the Grassmann schemes with some technical difficulties shown in Lemmas 4.1 and 4.2 for finding the number $d_H(B(D_0), B(D'_0)) = e_m$ for sets D_0, D'_0 of examples 3 and 4. The precise expression for e_m as $k+q \leq m \leq \begin{bmatrix} k+1 \\ k \end{bmatrix}_q - \begin{bmatrix} k+1-d \\ k-d \end{bmatrix}_q$ is remained open.

Lemma 4.1 Let $2 \leq r \leq k+1$. Suppose V is a $(k+1)-$dimensional vector space over $GF(q)$, and F_k is a family of $k-$dimensional subspaces of V such that the dimension of any intersection of r subspaces of F_k is $k-r+1$, then $|F_k| \leq k+q$ is a sharp bound.

Proof: By the induction on k for $|F_k| \leq k+q$. When $k = 2$, for a given $D_1 \in F_k \subseteq \begin{bmatrix} V \\ 2 \end{bmatrix}_q$, each lines in D_1 is at most contained in one $D_i \in F_k, i \neq 1$ such that $|F_2| \leq \begin{bmatrix} 2 \\ 1 \end{bmatrix}_q + 1 = \frac{q^2-1}{q-1} + 1 = (q+1) + 1 = q+2$. Suppose $k = \beta > 2$, $|F_\beta| \leq \beta + q$. Assume $k = \beta + 1$, for a given $D_1 \in F_{\beta+1} \subseteq \begin{bmatrix} V \\ \beta+1 \end{bmatrix}_q$, each $\beta-$dimension subspace in D_1 is contained in at most one $D_i \in F_{\beta+1}, i \neq 1$. So we can reduce the problem to $k = \beta$ such that $|F_{\beta+1}| \leq |F_\beta| + 1 \leq (q+\beta) + 1 = q + (\beta+1)$. Q.E.D.

Lemma 4.2 Suppose V is a $(k+1)-$dimensional vector space over $GF(q)$, and let $\{D_1, D_2, \cdots, D_{m+1}\} \subseteq \begin{bmatrix} V \\ k \end{bmatrix}_q$. There is at least one $d-$subspace $C \subseteq D_{m+1}$ such that $C \nsubseteq D_i$ for all $i \in [m]$. Then $m \leq \begin{bmatrix} k+1 \\ k \end{bmatrix}_q - \begin{bmatrix} k+1-d \\ k-d \end{bmatrix}_q$ is a sharp bound.

Proof: For any $d-$subspace $C \subseteq D_{m+1}$, C is not contained in $\begin{bmatrix} k+1 \\ k \end{bmatrix}_q - \begin{bmatrix} k+1-d \\ k-d \end{bmatrix}_q$ $k-$subspaces of V. So if $m > \begin{bmatrix} k+1 \\ k \end{bmatrix}_q - \begin{bmatrix} k+1-d \\ k-d \end{bmatrix}_q$, then for each $d-$subspace $C \subseteq D_{m+1}$, there is at least one $D_i, i \in [m]$ such that $C \subseteq D_i$ a contradiction, as required. Q.E.D.

Theorem 4.2 ($e_m, e_{\leq m}$ over the Grassmann schemes)

$$e_m = e_{\leq m} = \begin{cases} 2 \cdot \sum_{i=0}^{k-d} (-1)^i \begin{pmatrix} m \\ i \end{pmatrix} \begin{bmatrix} k-i \\ d \end{bmatrix}_q & \text{, if } m \leq q+k-1, \\ 0 & \text{, if } m > \begin{bmatrix} k+1 \\ k \end{bmatrix}_q - \begin{bmatrix} k+1-d \\ k-d \end{bmatrix}_q \end{cases}$$

Proof:

1. An upper bound for e_m is obtained by the specific examples above. We show it is equal to e_m as follows. For $D = \{D_1, \cdots, D_m\}$ and $D' = \{D'_1, \cdots, D'_m\} \subseteq \begin{bmatrix} n \\ k \end{bmatrix}_q$

$$\begin{aligned} e_m &= 2 \cdot \min|\{C \in \begin{bmatrix} n \\ d \end{bmatrix}_q \mid C \nsubseteq D_1, \cdots, D_m, C \subseteq D'_j \text{ for some } j\}| \\ &= 2 \cdot \min|\{C \in \begin{bmatrix} n \\ d \end{bmatrix}_q \mid C \subseteq D'_m, C \nsubseteq D_i \cap D'_m, i \in [m] \text{ with } |D \cap D'| = m-1\}| \\ &= 2 \cdot \min(|\{C \subseteq D'_m\}| - |\{C \subseteq D_1 \cap D'_m\}| - (|\{C \subseteq D_2 \cap D'_m\}| - \\ &\quad |\{C \subseteq D_1 \cap D_2 \cap D'_m\}|) - (|\{C \subseteq D_3 \cap D'_m\}| - |\{C \subseteq D_1 \cap D_2 \cap D_3 \cap D'_m\}|) - \cdots) \\ &= 2 \cdot \min(|\{C \subseteq D'_m\}| - (|\{C \subseteq D_1 \cap D'_m\}| + |\{C \subseteq D_2 \cap D'_m\}| + \cdots) + \\ &\quad (|\{C \subseteq D_1 \cap D_2 \cap D'_m\}| + |\{C \subseteq D_1 \cap D_2 \cap D_3 \cap D'_m\}| + \cdots)). \end{aligned}$$

Hence we can consider $D = \{D_1, \cdots, D_m\}$ and $D' = \{D_1, \cdots, D_{m-1}, D'_m\} \subseteq \begin{bmatrix} k+1 \\ k \end{bmatrix}_q$ such that $\dim(D_i \cap D'_m) = k-1$ is largest and the dimension of any intersection of D_i's as small as possible. Then

$$e_m \geq 2 \cdot (\begin{bmatrix} k \\ d \end{bmatrix}_q - \begin{pmatrix} m \\ 1 \end{pmatrix} \begin{bmatrix} k-1 \\ d \end{bmatrix}_q + \cdots + (-1)^{k-d} \begin{pmatrix} m \\ k-d \end{pmatrix} \begin{bmatrix} k-(k-d) \\ d \end{bmatrix}_q)$$

$= d_H(B(D_0), B(D'_0))$ for $m \leq q+k-1$ in Example 3,

and $e_m = 0$ for $m > \begin{bmatrix} k+1 \\ k \end{bmatrix}_q - \begin{bmatrix} k+1-d \\ k-d \end{bmatrix}_q$ in Example 4, as required.

2. Since

$$\begin{aligned} e_{\leq m} &= \min|\{C \in \begin{bmatrix} n \\ d \end{bmatrix}_q \mid C \nsubseteq D_1, \cdots, D_r, r \leq m, C \subseteq D'_j \text{ for some } j\}| \\ &\quad + \min|\{C \in \begin{bmatrix} n \\ d \end{bmatrix}_q \mid C \nsubseteq D'_1, \cdots, D'_s, s \leq m, C \subseteq D_j \text{ for some } j\}| \\ &= 2 \cdot \min|\{C \in \begin{bmatrix} n \\ d \end{bmatrix}_q \mid C \nsubseteq D'_1, \cdots, D'_m, C \subseteq D_j \text{ for some } j\}| \\ &= e_m, \text{ as required.} \qquad \text{Q.E.D.} \end{aligned}$$

Remarks 4.1 The parameters $e_m = e_{\leq m}$ for the Johnson schemes and the Grassmann schemes as shown in the proofs of Theorem 4.1 and 4.2; moreover $d_H(B(D_0)B(D'_0)) = e_m$ whenever $|D_0 \cap D'_0| = m-1$ such that $e_i \leq e_j$ for $i > j$. Hence

$$2 \cdot \sum_{i=0}^{k-d} (-1)^i \begin{pmatrix} m \\ i \end{pmatrix} \begin{bmatrix} k-i \\ d \end{bmatrix}_q \leq e_m \leq e_{k+q-1} = 2 \cdot \sum_{i=0}^{k-d} (-1)^i \begin{pmatrix} k+q-1 \\ i \end{pmatrix} \begin{bmatrix} k-i \\ d \end{bmatrix}_q,$$

for $k+q \leq m \leq 2 \cdot \sum_{i=0}^{k-d} (-1)^i \begin{pmatrix} m \\ i \end{pmatrix} \begin{bmatrix} k-i \\ d \end{bmatrix}_q$ over the Grassmann schemes.

4-3 $(s, l; e)-$Disjunct matrices and $(s, l; e)-$separable matrices

The notion of superimposed codes and superimposed designs are generalizations of those of $d-$disjunct and $\bar{d}-$separable matrices, respectively.

4-3-1 Some parameters

For a binary matrix M, we define two parameters $d_{s,l}(M), \partial_{s,l}(M)$ first as follows:

Let M be a binary matrix of order $t \times N$. For disjoint $S, L \subset [N]$, we define

$$d(S, L) = |\{\alpha \mid \alpha \in [t] \text{ for which } M(\alpha, l) = 1 \text{ for each } l \in L,$$

$$\text{and } M(\alpha, s) = 0 \text{ for each } s \in S\}|.$$

The pair (S, L) is called *disjunctive* if $d(S, L) \geq 1$, or equivalently, the intersection of those sets corresponding to L is not proper contained in the union of those sets corresponding to S. We further define

$$\begin{aligned} d_{s,l}(M) = &\text{ the minimum } d(S, L) \text{ over all pairs } (S, L) \\ &\text{with disjoint } S, L \subset [N], \text{ and } |S| = s, |L| = l. \end{aligned}$$

The notion of was first defined in 1989 by Dyachkov et.al [1].

For an *antichain* $\rho = \{P_1, \cdots, P_k\}$ over N, we define a binary vector

$$r(\rho, M) = [r_1, r_2, \cdots, r_t]^T,$$

where $r_i = 1$ if there is some P_j such that $M(i, P_j) = 1$ and 0 otherwise. We define

$$\begin{aligned} \partial_{s,l}(M) = &\text{ the minimum of } d_H(r(\rho, M), r(\rho', M)) \\ &\text{over all pairs of distinct } \textit{antichains } \rho = \{P_1, \cdots, P_k\} \\ &\text{and } \rho' = \{P'_1, \cdots, P'_m\} \text{ in } \wp([N]) \text{ with } k, m \leq s \\ &\text{and with } |P_i|, |P'_j| \leq l \text{ for each } i, j. \end{aligned}$$

Definition 4.3

1. A binary matrix M is called *a $(s, l; e)-$disjunct matrix* if $d_{s,l}(M) \geq e$. A *set system* $(X, \mathcal{F})$ is called *a $(s, l; e)-$disjunct family* (or *a $(s, l; e)-$cover free family*) if the corresponding incidence matrix of $(X, \mathcal{F})$ is $(s, l; e)-$disjunct.

2. A binary matrix M is called *a* $(s,l;e)-$*separable matrix* if $\partial_{s,l}(M) \geq e$. A *set system* $(X,\mathcal{F})$ is called *a* $(s,l;e)-$*separable family* if the corresponding incidence matrix of $(X,\mathcal{F})$ is $(s,l;e)-$separable.

Equivalently, we can define set systems $(X,\mathcal{F})$ of $(s,l;e)-$disjunct matrices and $(s,l;e)-$separable matrices as follows. Those $q-$analog of $(s,l;e)-$disjunct matrices is considered in Definition 4.5 for constructing $(s,l;e)-$disjunct matrices and $(s,l;e)-$separable matrices.

Definition 4.4 [9, Def 1.1]

1. A *set system* $(X,\mathcal{F})$ is called *a* $(s,l;e)-$*cover free family* if for any blocks $B_1,\cdots,B_l$ and other blocks $A_1,\cdots,A_s \in F$, we have that

$$|\bigcap_{i=1}^{l} B_i \setminus \bigcup_{j=1}^{s} A_j\ | \geq e.$$

2. A *set system* $(X,\mathcal{F})$ is called *a* $(s,l;e)-$*separable family* if for any two antichains $\mathcal{A}=\{A_1,\cdots,A_k\},\mathcal{B}=\{B_1,\cdots,B_m\}$ where $A_i,B_j \subseteq \mathcal{F}, |A_i|,|B_j| \leq l$, and $k,m \leq s$, then the symmetric difference of $\bigcup_{i=1}^{k}\bigcap_{A_{i_x}\in A_i} A_{i_x}$ and $\bigcup_{j=1}^{m}\bigcap_{B_{j_x}\in B_j} B_{j_x}$ contains at least e elements, i.e.,

$$|\ (\bigcup_{i=1}^{k}\bigcap_{A_{i_x}\in A_i} A_{i_x})\triangle(\bigcup_{j=1}^{k}\bigcap_{B_{j_x}\in B_j} B_{j_x})\ | \geq e.$$

Remarks 4.2

1. A $(s,l;e)-$*disjunct matrix* is called

   (i) a $d-$*disjunct matrix* if $(s,l;e)=(d,1;1)$ in [3, P.364],

   (ii) a $d^{(e-1)}-$*disjunct matrix* if $(s,l)=(d,1)$ in [4, Def 2], and

   (iii) a *superimposed* $(s,l)-$*code* if $e=1$ in [2, Def 1.2].

A binary matrix M is a $(s,l;e)-$disjunct matrix if and only if $\overline{M} := J - M$ is a $(l,s;e)-$disjunct matrix (Symmetry). Without loss of generality, we may just consider

$(s, 1; e)-$disjunct matrix, but no $(1, l; e)-$disjunct matrices.

Some trivial examples of $(s, 1; e)-$disjunct matrices [2, P.201]:
(i) $l \leq w \leq N - s$, the matrix M of order $\begin{pmatrix} N \\ w \end{pmatrix} \times N$ whose rows are all those binary vectors of length N and weight w.
(ii) $N = s + l$, the matrix M of order $\begin{pmatrix} N \\ l \end{pmatrix} \times N$ whose rows are all those binary vectors of length N and weight l.

2. A $(s, l; e)-$separable matrix is called
(i) a $\bar{d}-$separable matrix if $(s, l; e) = (d, 1; 1)$, and
(ii) a superimposed $(s, l)-$design if $e = 1$.

For any two antichains $\rho = \{P_1, \cdots, P_k\}$ and $\rho' = \{P'_1, \cdots, P'_m\} \in \wp([N])$ with $k, m \leq s$ and $|P_i|, |P'_j| \leq l$ for each i, j, there at least one antichain ρ (or ρ') contains a member P_i (or P'_j) which does not contain any member of another antichain ρ' (or ρ).

3. A $(s, l; e)-$disjunct matrix (resp. $(s, l; e)-$separable matrix) is also a $(i, j; u)-$disjunct matrix (resp. $(i, j; u)-$separable matrix) whenever $1 \leq i \leq s, 1 \leq j \leq l$, and $1 \leq u \leq e$.

4. The notion of superimposed $(s, l)-$ designs is a generalization of *separable systems* and it provides a right model for *setwise group testing* (i.e., *set group testing* by Torney [2], and *group testing on complexes* by Macula [2]).

It was shown in Proposition 1.1 [2, P.196] that superimposed $(s, l)-$codes are superimposed $(s, l)-$designs, and similar results hold for $(s, l; e)-$disjunct matrices.

Proposition 4.1

1. A $(s,l;e)-$disjunct matrix is a $(s,l;e)-$separable matrix.

2. A $(s,l;e)-$separable matrix is a $(s-1,l;e)-$disjunct matrix and a $(s,l-1;e)-$disjunct matrix.

Proof:

1. Suppose in contradiction that there exists a $(s,l;e)-$disjunct matrix which is not a $(s,l;e)-$separable matrix, i.e., there exist two antichains $\rho = \{P_1,\cdots,P_k\}$ and $\rho' = \{P'_1,\cdots,P'_m\}$ with $k,m \leq s$ and $|P_i|,|P'_j| \leq l$ for each i,j such that $d_H(r(\rho,M),r(\rho',M)) < e$. Without loss of generality, we may assume that $P'_j \nsubseteq P_1$ for each $j \in [m]$. Choose $a_j \in P'_j \setminus P_1$ for each j, and let $A = \{a_1,\cdots,a_m\}$, then $1 \leq |A| \leq m \leq s$; further let $B = P_1$, then $|B| = |P_1| \leq l$. Because M is $(s,l;e)-$disjunct, $d(A,B) \geq e$, i.e., there exist at least e rows i of M such that $M(i,j) = 1$ for each $j \in B$ and $M(i,j') = 0$ for each $j' \in A$. It implies that $d_H(r(\rho,M),r(\rho',M)) \geq e$, a contradiction, as required.

2. Suppose in contradiction that there exists a $(s,l;e)-$separable matrix which is not a $(s-1,l;e)-$disjunct matrix, i.e., there exist two disjoint sets $A,B \subseteq [N]$, say $A = \{a_1,\cdots,a_{s-1}\}$ and $B = \{b_1,\cdots,b_l\}$ such that $d(A,B) < e$. Let $\rho = \{a_1,\cdots,a_{s-1}\}$ and $\rho' = \{a_1,\cdots,a_{s-1},B\}$. Since M is a $(s,l;e)-$separable matrix, $d_H(r(\rho,M),r(\rho',M)) \geq e$. It implies $d(A,B) \geq e$, a contradiction, as required.

Suppose in contradiction that there exists a $(s,l;e)-$separable matrix which is not a $(s,l-1;e)-$disjunct matrix, i.e., there exist two disjoint sets $A,B \subseteq [N]$, say $A = \{a_1,\cdots,a_s\}$ and $B = \{b_1,\cdots,b_{l-1}\}$ such that $d(A,B) < e$. Let $\rho = \{B \cup a_1,\cdots,B \cup a_s\}$ and $\rho' = \{B\}$. Since M is a $(s,l;e)-$separable matrix, $d_H(r(\rho,M),r(\rho',M)) \geq e$. It implies $d(A,B) \geq e$, a contradiction, as required. Q.E.D.

Alternative proof:

1. For *any two antichains* $\rho = \{P_1, \cdots, P_k\}$ and $\rho' = \{P'_1, \cdots, P'_m\}$ with $k, m \leq s$ and $|P_i|, |P'_j| \leq l$, without loss of generality, we may assume that $P'_j \nsubseteq P_1$ for each $j \in [m]$. Choose $a_j \in P'_j \setminus P_1$ for each j, and let $A = \{a_1, \cdots, a_m\}$, then $1 \leq |A| \leq m \leq s$; further let $B = P_1$, then $|B| = |P_1| \leq l$. Because M is $(s, l; e)-$disjunct, $d(A, B) \geq e$, i.e., there exist at least e rows i of M such that $M(i, j) = 1$ for each $j \in B$ and $M(i, j') = 0$ for each $j' \in A$. It implies that $d_H(r(\rho, M), r(\rho', M)) \geq e$.

2. For *any two disjoint sets* $A, B \subseteq [N]$, say $A = \{a_1, \cdots, a_{s-1}\}$ and $B = \{b_1, \cdots, b_l\}$, let $\rho = \{a_1, \cdots, a_{s-1}\}$ and $\rho' = \{a_1, \cdots, a_{s-1}, B\}$ with $\rho \subseteq \rho'$ such that $r(\rho, M) \subseteq r(\rho', M)$. Since M is a $(s, l; e)-$separable matrix, $d_H(r(\rho, M), r(\rho', M)) \geq e$. It implies there exist at least e rows of M such that $M(i, b_j) = 1$ and $M(i, a_u) = 0$ for each $j \in [l], u \in [s-1]$, i.e., $d(A, B) \geq e$.

For *any two disjoint sets* $A, B \subseteq [N]$, say $A = \{a_1, \cdots, a_s\}$ and $B = \{b_1, \cdots, b_{l-1}\}$, let $\rho = \{B \cup a_1, \cdots, B \cup a_s\}$ and $\rho' = \{B\}$ such that $r(\rho, M) \subseteq r(\rho', M)$. Since M is a $(s, l; e)-$separable matrix, $d_H(r(\rho, M), r(\rho', M)) \geq e$. It implies there exist at least e rows i of M such that $M(i, b_j) = 1$ and $M(i, a_u) = 0$ for each $j \in [l-1], u \in [s]$, i.e., $d(A, B) \geq e$. Q.E.D.

Remarks 4.3

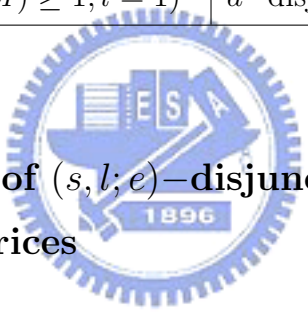
The conditions of disjunct matrices are stronger than those of separable matrices such that disjunct matrices are also separable matrices by Proposition 4.1. But on decoding the *defective* (*positive*) *set*, the complexity of separable matrices is more than the complexity of disjunct matrices as follows:

Let $\mathbf{P} = \{P_1, P_2, \cdots, P_m\} \in \wp([N])$ be a positive set with $k \leq s, |P_i| \leq l$ for all i, and we will decode the unknown $\mathbf{P}$ by using the vector $r(\mathbf{P}, M)$. For a testing group G, the test result $r(G) = 1$ if $P_i \subseteq G$ for some i and 0 otherwise. And the positive set can be decoded if and only if each outcome vector $r(\rho, M)$ of any

antichain $\rho = \{P_1, P_2, \cdots, P_m\} \in \wp([N])$ with $m \leq s$ and $|P_i| \leq l$ for each i is distinct. Then the decoding complexity for a superimposed $(s,l)-$design is at least $\left(\begin{pmatrix} t \\ l \end{pmatrix} \atop s \right) \sim \frac{t^{sl}}{s!(l!)^s}$. But the decoding complexity for a superimposed $(s,l)-$code is $\begin{pmatrix} N \\ 1 \end{pmatrix} + \begin{pmatrix} N \\ 2 \end{pmatrix} + \cdots + \begin{pmatrix} N \\ l \end{pmatrix} \sim \frac{N^l}{l!}$ (Since $\mathbf{P}$ is composed of all minimal P_i with $|P_i| \leq l$ and $\bigcap_{j \in P_i} M(j) \subseteq r(\mathbf{P}, M)$, where $M(j)$ is j-th column of M).

Separable matrices and disjunct matrices

$(s,l;e)-$separable matrix ($\partial_{s,l}(M) \geq e$) $(s,l;e)-$separable family	$(s,l;e)-$disjunct matrix ($d_{s,l}(M) \geq e$) $(s,l;e)-$disjunct family $(s,l;e)-$cover free family
superimposed $(s,l)-$design ($\partial_{s,l}(M) \geq 1$)	superimposed $(s,l)-$code ($d_{s,l}(M) \geq 1$)
$\overline{d}-$separable matrix ($\partial_{s,1}(M) \geq 1, l = 1$)	$d-$disjunct matrix ($d_{s,1}(M) \geq 1$)



4-3-2 Constructions of $(s,l;e)-$disjunct matrices and $(s,l;e)-$separable matrices

The constructions of superimposed $(s,l)-$codes and $(s,l;e)-$disjunct matrices were considered by A. D'yachkov and P. Vilenkin, A. Macula, D. Torney [2, 2002], and by D.R. Stinson, R. Wei [3, 2004], respectively. We will generalize the techniques of constructing $(s,l;e)-$disjunct matrices to construct $(s,l;e)-$separable matrices in this section.

Constructions of $(s,l;e)-$disjunct matrices

Two methods to construct $(s,l;e)-$disjunct matrices [2, 9] will be considered in the following:

The first simple construction of $(s,l;e)-$disjunct matrices is based on $(s,1;1)-$disjunct matrices. Let a matrix M of order $t \times N$ be a $(s,1;1)-$disjunct matrix with rows $m_i, i \in [t]$, and construct a $(s,l;e)-$disjunct matrix M' whose rows m'_τ correspond to nonempty subsets $\tau \subset [t], |\tau| \leq l$ with the form $m'_\tau = \bigcup_{i\in\tau} m_i$. And then we can construct a $(s,l;e)-$disjunct matrix by taking $e-$copies rows of M'.

The notions of $q_0-ary\ (s,l;e)-separating\ matrices$ and a $q_0-ary\ (s,l;e)-perfect\ matrix$ will be used in the 2nd method of construction.

Definition 4.5

A matrix $M = [M(i,j)]_{t\times N}$ is a $q_0-ary\ (s,l;e)-separating\ matrix$ if for any two disjoint sets $A, B \subseteq [N]$ with $|A| = s, |B| = l$, there exist at least e rows $i \in [t]$ such that $A_i = \{M(i,j) \mid j \in A\}, B_i = \{M(i,j) \mid j \in B\} \subseteq \{1, 2, \cdots, q_0\} = [q_0]$ are disjoint.
2. A $q_0-ary\ (w;e)-perfect\ matrix$, for any sets $C \subseteq [N], |C| = w$, there exists at least e rows $i \in [t]$ whose elements in $C_i = \{M(i,j) \mid j \in C\} \subseteq [q_0]$ are distinct.

A $q_0-ary\ (s,l;e)-separating\ matrix$ of order $t \times N$ can be described as a set F of t functions $f : [N] \to [q_0]$, and for any disjoint pairs $A, B \subseteq [N]$, $|A| = s, |B| = l$, there exist at least e functions $f \in F$ such that $f(A) \cap f(B) = \emptyset$. Similarily, a $q_0-ary\ (w;e)-perfect\ matrix$ can be described as for $C \subseteq [N], |C| = w$, there exist at least e functions which are bijective on C. Hence a q_0-ary $(s+l;e)-$perfect matrix is stronger than a q_0-ary $(s,l;e)-$separating matrix. As constructing $(s,l;e)-$disjunct matrices by using q_0-ary $(s,l;e)-$separating matrices by Theorem 4.3, they also can be constructed by using q_0-ary $(s+l;e)-$perfect matrices.

Theorem 4.3 (Concatenated Construction) [9, Theorem 3.3]
If there exists a $(s,l;e_1)-$disjunct matrix of order $t\times q_0$ and a q_0-ary $(s,l;e_2)-$separating matrix of order $T \times N$, then there exists a $(s,l;e_1e_2)-$disjunct matrix of order $Tt \times N$.

Proof: We replace each element $x \in [q_0]$ of a q_0-ary $(s,l;e_2)-$separating matrix of order $T \times N$ by the $x-th$ column vector of a $(s,l;e_1)-$disjunct matrix of order $t \times q_0$. Thus, we can get a $(s,l;e_1e_2)-$disjunct matrix of order $Tt \times N$. Q.E.D.

Based on the above theorem, many disjunct matrices can be obtained from trivial disjunct matrices, q_0-ary separating matrices in terms of the above recursive method. Since there is an infinite class of q_0-ary $(s,l;e_2)-$separating matrices of order $T \times N$ for which $T = O((sl)^{log^*N}(logN))$ [6] (and q_0-ary $(w;e_2)-$perfect matrices of order $T \times N$ existing for which $T = O(logN)$[7]), and let M be a trivial $(s,l;e_1)-$disunct matrix of order $e_1 \begin{pmatrix} s+l \\ l \end{pmatrix} \times (s+l)$ whose rows m_i are e_1-copy of all binary vectors of weight l. Thus, we can construct a $(s,l;e_1e_2)-$disjunct matrix of order $Te_1 \begin{pmatrix} s+l \\ l \end{pmatrix} \times N$ for which $T = O((sl)^{log^*N}(logN))$.

Constructions of $(s,l;e)-$separable matrices

Similar to the construction of $(s,l;e)-$disjunct matrices, two methods for constructions of $(s,l;e)-$separable matrices are considered in the following.

Two methods to construct $(s,l;e)-$separable matrices:

1. The trivial construction of $(s,l;e)-$separable matrices is based on $(s,l;1)-$separable matrices. And then we can construct a $(s,l;e)-$separable matrix by taking $e-$copies rows of a $(s,l;1)-$separable matrix.

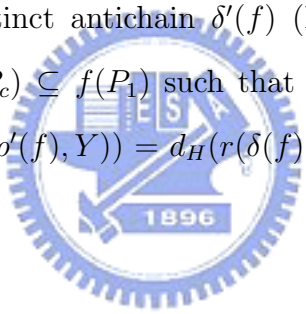
2. By q_0-ary $(s,l;e_2)-$separating matrices, $(s,l;e_1)-$separable matrices, and concatenated construction, we can construct $(s,l;e_1e_2)-$separable matrices as follows.

Theorem 4.4 (Concatenated Construction)

If there exists a $(s,l;e_1)-$separable matrix of order $t \times q_0$ and a q_0-ary $(s,l;e_2)-$separating matrix of order $T \times N$, then there exists a $(s,l;e_1e_2)-$separable matrix of order $Tt \times N$.

Proof: The matrix M is obtained by replacing each element $x \in [q_0]$ of a q_0-ary $(s,l;e_2)-$separating matrix X of order $T \times N$ by the $x-th$ column vector of a $(s,l;e_1)-$separable matrix Y of order $t \times q_0$. Then we will prove the matrix M is $(s,l;e_1e_2)-$separable in the following.

For *any two antichains* $\rho = \{P_1, \cdots, P_k\}$ and $\rho' = \{P'_1, \cdots, P'_m\}$ with $k, m \leq s$ and $|P_i|, |P'_j| \leq l$, without loss of generality, we may assume that $P'_j \nsubseteq P_1$ for each $j \in [m]$. Choose $a_j \in P'_j \setminus P_1$ for each j, and let $A = \{a_1, \cdots, a_m\}$, then $1 \leq |A| \leq m \leq s$; further let $B = P_1$, then $|B| = |P_1| \leq l$. Since X is a q_0-ary $(s,l;e_2)-$separating matrix, there exist at least e_2 functions $f \in F$ with $f(A) \cap f(B) = \emptyset$ such that $f(P_1) \cap f(A) = \emptyset$. Then we get an antichain $\delta(f)$ from $\rho(f) = \{f(P_1), \cdots, f(P_k)\}$ by canceling all members $f(P_j)$ containing other member in $\rho(f)$ such that $r(\delta(f), Y) = r(\rho(f), Y)$ and similarly we can get a distinct antichain $\delta'(f)$ (Because there is at least a member $f(P_c)$ in $\delta(f)$ with $f(P_c) \subseteq f(P_1)$ such that $f(P_c) \cap f(A) = \emptyset$. Then $f(P_c) \notin \delta'(f)$.) So $d_H(r(\rho(f), Y), r(\rho'(f), Y)) = d_H(r(\delta(f), Y), r(\delta'(f), Y)) \geq e_1$, as required. Q.E.D.



4-4 The relation of $(d,k,m,s)-$systems and superimposed $(s,l)-$codes

The relation of $(d,k,m,s)-$systems with $d \leq k$ and superimposed codes will be considered in this section, i.e., using $(d,k,1,s)-$systems to construct superimposed $(a,b)-$codes. And binary codes are also useful to construct superimposed $(a,b)-$codes. Moreover, we can also use $(d,k,m,s)-$systems with $m \geq 2$ to construct superimposed $(a,b)-$codes.

Using $(d,k,1,s)-$system as a parity-check matrix, we can obtain a linear code of

length s with dimension $\geq s-k$, and with minimum distance $\geq d+1$ by Proposition 3.1.

Theorem 4.5 Suppose C is a binary linear code with a $(d,k,1,s)-$system as its parity-check matrix, then the length of C is s, the dimension of C is at least $s-k$, and its minimum distance is at least d+1. Moreover, if $s-k \geq a+b$ and $s \geq ab(s-d-1)+1$, then the generator matrix of the linear code C is a superimposed $(a,b)-$code or a superimposed $(b,a)-$code.

Proof: Suppose in contradiction that there is two disjoint subsets $A, B \subset [s-k]$ with $|A| = a, |B| = b$ such that no row i in the generator matrix M of C with properties:

$$M(i,j) = 1 \text{ for all } j \in A, M(i,j') = 0 \text{ for all } j' \in B \text{ or}$$
$$M(i,j) = 0 \text{ for all } j \in A, M(i,j') = 1 \text{ for all } j' \in B.$$

That is, for each row i there is at least a pair $j \in A, j' \in B$ such that $M(i,j) = M(i,j')$. Since $s \geq ab(s-d-1)+1$, and by the pigeonhole theorem, there is at least a pair $j \in A, j' \in B$ with at least $s-d$ rows i such that $M(i,j) = M(i,j')$. So the minimum distance of C at most $s-(s-d) = d$, a contradiction as required. Q.E.D.

Remark 4.4 Fix s,k,d, then a,b satisfy (1) if and only if they satisfy (2), where

$$s-k \geq a+b, \text{ and } s \geq ab(s-d-1)+1 \textbf{ (1)}$$
$$a+b+k \leq s \leq d+1+\tfrac{d}{ab-1}, \text{ and } s \geq d+1 \textbf{ (2)}$$

We consider for some s,k,a,b, the maximum number d such that $(d,k,1,s)-$system can form superimposed $(a,b)-$codes or superimposed $(b,a)-$codes.

$a+b \leq s-k = 2 \Rightarrow (a,b) = (1,1)$					
s	3	4	5	6	7
k	1	2	3	4	5
$s-1-\frac{s-1}{ab}$	0	0	0	0	0
$s-1-\frac{s-1}{ab} \leq d \leq k$	1	2	3	4	5

$a+b \le s-k=3 \Rightarrow (a,b)=(1,1),(1,2),(2,1)$					
$(a,b)=(1,1)$					
s	4	5	6	7	8
k	1	2	3	4	5
$s-1-\frac{s-1}{ab}$	0	0	0	0	0
$s-1-\frac{s-1}{ab} \le d \le k$	1	2	3	4	5
$(a,b)=(1,2)$ or $(2,1)$					
s	4	5	6	7	8
k	1	2	3	4	5
$s-1-\frac{s-1}{ab}$	1.5	2	2.3	3	3.5
$s-1-\frac{s-1}{ab} \le d \le k$	1	2	3	3,4	4,5

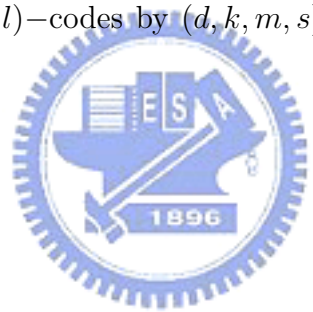
$a+b \le s-k=4 \Rightarrow (a,b)=(1,1),(1,2),(1,3),(2,1),(2,2),(3,1)$					
$(a,b)=(1,1)$					
s	5	6	7	8	9
k	1	2	3	4	5
$s-1-\frac{s-1}{ab}$	0	0	0	0	0
$s-1-\frac{s-1}{ab} \le d \le k$	1	2	3	4	5
$(a,b)=(1,2)$ or $(2,1)$					
s	5	6	7	8	9
k	1	2	3	4	5
$s-1-\frac{s-1}{ab}$	2	2.5	3	3.5	4
$s-1-\frac{s-1}{ab} \le d \le k$	/	/	3	4	4,5
$(a,b)=(1,3)$ or $(3,1)$					
s	5	6	7	8	9
k	1	2	3	4	5
$s-1-\frac{s-1}{ab}$	2.67	3.33	4	4.67	5.33
$s-1-\frac{s-1}{ab} \le d \le k$	/	/	/	/	/
$(a,b)=(2,2)$					
s	5	6	7	8	9
k	1	2	3	4	5
$s-1-\frac{s-1}{ab}$	3	3.75	4.5	5.25	6
$s-1-\frac{s-1}{ab} \le d \le k$	/	/	/	/	/

Corollary 4.1 Suppose $r \ge a+b$ and $n \ge ab(n-d-1)+1$, the generator matrix of the binary linear code with $l(C)=n$, $\dim(C)=r$ and minimum distance$(C) \ge d+1$ is a superimposed $(a,b)-$code or superimposed $(b,a)-$code.

Remarks 4.5

For a $(d,k,2,s)-$system $\{c_{i,j} \in GF(q)^k \mid 1 \leq i \leq s, 1 \leq j \leq 2\}$, $\{c_{i,1} \in GF(q)^k \mid 1 \leq i \leq s\}$ is a $(d,k,1,s)-$system, and $\{c_{i,2} \in GF(q)^k \mid 1 \leq i \leq s\}$ is a $(\frac{d}{2},k,1,s)-$system by definition. Using them as parity-check matrices, we can obtain two code C_1 and C_2, where C_1 is a linear code of length s, with dimension $n_1 \geq s-k$, and with minimum distance$\geq d+1$, and another linear code C_2 of length s, with dimensional $n_1 \geq s-k$, and with minimum distance$\geq \frac{d}{2}+1$. This gives a matrix $G = \begin{bmatrix} G_1 \\ G_2 \end{bmatrix}_{2s \times min\{n_1,n_2\}}$ with minimum distance$\geq d+\frac{d}{2}+2$, where G_1, G_2 are sub-matrices of generator matrices of C_1, C_2.

Similarly to Theorem 4.5, if $s-k \geq a+b$ and $s \geq ab(2s-d-\frac{d}{2}-2)+1$, then the matrix G is a superimposed $(a,b)-$code or superimposed $(b,a)-$code. Moreover, we can construct superimposed $(s,l)-$codes by $(d,k,m,s)-$systems under some constraints over s,l.



References

[1] A.G. Dyachkov, V.V. Rykov, A.M. Rashad, Superimposed distance codes, Problems Control Inform. Theory/ Problemy Upravlen. Teor. Inform. 18 (4) (1989) 237-250.

[2] A. D'yachkov and P. Vilenkin, A. Macula, D. Torney, Families of finite sets in which no intersection of l sets is covered by the union of s others, J. Combin. Theory Ser. A 99(2002), 195-218.

[3] W. H. Kautz, R. C. Singleton, Nonrandom binary superimposed codes, IEEE Trans. Inform. Theory 10 (1964), 363-377.

[4] A. Macula, Error-correcting nonadaptive group testing with d^e-disjunct matrices, Discrete Applied Math. 80 (1997), 217-222.

[5] H. Niederreiter, Point sets and sequences with small discrepancy, Monatsh. Math. 104 (1987), 273-337.

[6] H. Niederreiter, A combinatorial problem for vector spaces over finite fields, Discrete Math. 96(1991), 221-228.

[7] H. Niederreiter, G. Pirsic, Duality for digital nets and its applications, Acta Arith. 97 (2001), 173-182.

[8] H. Niederreiter, Digital nets and coding theory, Fukuoka Conference, 2003.

[9] D.R. Stinson, R. Wei, Generalized cover-free families, Discrete Math. 272(2004), 463-477.

[10] H. Wang, C. Xing, Explicit constructions of perfect hash families from algebraic curves over finite fields, J. Combin. Theory Ser. A 93 (2001), 112-124.

Appendix

1. The $(2,3,3,5)-$system in terms of the impulse response sequence in Example 1 of subsection 3-2-2 is constructed as follows.

$\frac{1}{p_1^1}=\frac{1}{x}, \frac{1}{p_1^2}=\frac{1}{x^2}, \frac{1}{p_1^3}=\frac{1}{x^3}$.

$\frac{1}{p_2^1}=\frac{1}{x-1}=\frac{1}{x}+\frac{1}{x^2}+\frac{1}{x^3}+\frac{1}{x^4}+\frac{1}{x^5}+O(\frac{1}{x^6}), \frac{1}{p_2^2}=\frac{1}{(x-1)^2}=\frac{1}{x^2}+\frac{2}{x^3}+\frac{1}{x^5}+O(\frac{1}{x^6}),$

$\frac{1}{p_2^3}=\frac{1}{(x-1)^3}=\frac{1}{x^3}+O(\frac{1}{x^6})$.

$\frac{1}{p_3^1}=\frac{1}{x-2}=\frac{1}{x}+\frac{2}{x^2}+\frac{1}{x^3}+\frac{2}{x^4}+\frac{1}{x^5}+O(\frac{1}{x^6}), \frac{1}{p_3^2}=\frac{1}{(x-2)^2}=\frac{1}{x^2}+\frac{1}{x^3}+\frac{2}{x^5}+O(\frac{1}{x^6}),$

$\frac{1}{p_3^3}=\frac{1}{(x-2)^3}=\frac{1}{x^3}+O(\frac{1}{x^6})$.

$\frac{1}{p_4^1}=\frac{1}{x^2+1}=\frac{1}{x^2}+\frac{2}{x^4}+O(\frac{1}{x^6}), \frac{1}{p_4^2}=\frac{1}{(x^2+1)^2}=\frac{1}{x^4}+O(\frac{1}{x^6}), \frac{1}{p_4^3}=\frac{1}{(x^2+1)^3}=O(\frac{1}{x^6})$.

Since $c_{i,jr}=\begin{cases} w_i(t_{i,j}+1, r+u_{i,j}) & \text{, for } 1\le i\le s-1, 1\le j\le m, 1\le r\le m, \\ \delta_{r-1,m-j} & \text{, for } i=s, 1\le j\le m, 1\le r\le m, \end{cases}$

and $j-1=t_{i,j}e_i+u_{i,j}, 0\le u_{i,j}<e_i$.

$t_{1,1}=0, u_{1,1}=0 \Rightarrow c_{1,1r}=w_1(1,r) \Rightarrow c_{1,1}=(1,0,0)$.

$t_{1,2}=1, u_{1,2}=0 \Rightarrow c_{1,2r}=w_1(2,r) \Rightarrow c_{1,2}=(0,1,0)$.

$t_{1,3}=2, u_{1,3}=0 \Rightarrow c_{1,3r}=w_1(3,r) \Rightarrow c_{1,3}=(0,0,1)$.

$t_{2,1}=0, u_{2,1}=0 \Rightarrow c_{2,1r}=w_2(1,r) \Rightarrow c_{2,1}=(1,1,1)$.

$t_{2,2}=1, u_{2,2}=0 \Rightarrow c_{2,2r}=w_2(2,r) \Rightarrow c_{2,2}=(0,1,2)$.

$t_{2,3}=2, u_{2,3}=0 \Rightarrow c_{2,3r}=w_2(3,r) \Rightarrow c_{2,3}=(0,0,1)$.

$t_{3,1}=0, u_{3,1}=0 \Rightarrow c_{3,1r}=w_3(1,r) \Rightarrow c_{3,1}=(1,2,1)$.

$t_{3,2}=1, u_{3,2}=0 \Rightarrow c_{3,2r}=w_3(2,r) \Rightarrow c_{3,2}=(0,1,1)$.

$t_{3,3}=2, u_{3,3}=0 \Rightarrow c_{3,3r}=w_3(3,r) \Rightarrow c_{3,3}=(0,0,1)$.

$t_{4,1}=0, u_{4,1}=0 \Rightarrow c_{4,1r}=w_4(1,r) \Rightarrow c_{4,1}=(0,1,0)$.

$t_{4,2}=0, u_{4,2}=1 \Rightarrow c_{4,2r}=w_4(1,r+1) \Rightarrow c_{4,2}=(1,0,2)$.

$t_{4,3}=1, u_{4,3}=0 \Rightarrow c_{4,3r}=w_4(2,r) \Rightarrow c_{4,3}=(0,0,0)$.

$c_{5,1}=(0,0,1), c_{5,2}=(0,1,0), c_{5,3}=(1,0,0)$.

2. The point set for the digital $(1,3,5)-$net over $GF(3)$ constructed by the system in Example 1 of subsection 3-2-2 is shown by the digital method as follows (ψ =id).

$p[1] = [0,0,0,0,0]$

$p[2] = [1/27, 16/27, 13/27, 2/9, 1/3]$

$p[3] = [2/27, 23/27, 26/27, 1/9, 2/3]$

$p[4] = [1/9, 4/9, 7/9, 1/3, 1/9]$

$p[5] = [4/27, 19/27, 7/27, 5/9, 4/9]$

$p[6] = [5/27, 8/27, 11/27, 4/9, 7/9]$

$p[7] = [2/9, 8/9, 5/9, 2/3, 2/9]$

$p[8] = [7/27, 4/27, 19/27, 8/9, 5/9]$

$p[9] = [8/27, 11/27, 5/27, 7/9, 8/9]$

$p[10] = [1/3, 1/3, 1/3, 1/9, 1/27]$

$p[11] = [10/27, 25/27, 22/27, 0, 10/27]$

$p[12] = [11/27, 5/27, 8/27, 2/9, 19/27]$

$p[13] = [4/9, 7/9, 1/9, 4/9, 4/27]$

$p[14] = [13/27, 1/27, 16/27, 1/3, 13/27]$

$p[15] = [14/27, 17/27, 20/27, 5/9, 22/27]$

$p[16] = [5/9, 2/9, 8/9, 7/9, 7/27]$

$p[17] = [16/27, 13/27, 1/27, 2/3, 16/27]$

$p[18] = [17/27, 20/27, 14/27, 8/9, 25/27]$

$p[19] = [2/3, 2/3, 2/3, 2/9, 2/27]$

$p[20] = [19/27, 7/27, 4/27, 1/9, 11/27]$

$p[21] = [20/27, 14/27, 17/27, 0, 20/27]$

$p[22] = [7/9, 1/9, 4/9, 5/9, 5/27]$

$p[23] = [22/27, 10/27, 25/27, 4/9, 14/27]$

$p[24] = [23/27, 26/27, 2/27, 1/3, 23/27]$

$p[25] = [8/9, 5/9, 2/9, 8/9, 8/27]$

$p[26] = [25/27, 22/27, 10/27, 7/9, 17/27]$

$p[27] = [26/27, 2/27, 23/27, 2/3, 26/27]$

3. The point set for the digital $(0, 3, 5)-$net over $GF(2^2)$ constructed by the system in Example 2 of subsection 3-2-2 is shown is by the digital method as follows ($\psi(0) = 0, \psi(x^k) = k \in \{1, 2, 3\}$).

$p[1] = [0, 0, 0, 0, 0]$

$p[2] = [1/64, 49/64, 33/64, 17/64, 1/4]$

$p[3] = [1/32, 9/32, 25/32, 17/32, 1/2]$

$p[4] = [3/64, 35/64, 19/64, 51/64, 3/4]$

$p[5] = [3/16, 3/16, 15/16, 15/16, 3/16]$

$p[6] = [13/64, 61/64, 29/64, 45/64, 7/16]$

$p[7] = [7/32, 15/32, 7/32, 15/32, 11/16]$

$p[8] = [15/64, 47/64, 47/64, 15/64, 15/16]$

$p[9] = [0, 3/4, 3/4, 0, 0]$

$p[10] = [1/64, 1/64, 17/64, 17/64, 1/4]$

$p[11] = [1/32, 17/32, 1/32, 17/32, 1/2]$

$p[12] = [3/64, 19/64, 35/64, 51/64, 3/4]$

$p[13] = [3/16, 15/16, 3/16, 15/16, 3/16]$

$p[14] = [13/64, 13/64, 45/64, 45/64, 7/16]$

$p[15] = [7/32, 23/32, 31/32, 15/32, 11/16]$

$p[16] = [15/64, 31/64, 31/64, 15/64, 15/16]$

$p[17] = [3/4, 3/4, 3/4, 3/4, 3/64]$

$p[18] = [49/64, 1/64, 17/64, 33/64, 19/64]$

$p[19] = [25/32, 17/32, 1/32, 9/32, 35/64]$

$p[20] = [51/64, 19/64, 35/64, 3/64, 51/64]$

$p[21] = [15/16, 15/16, 3/16, 3/16, 15/64]$

$p[22] = [61/64, 13/64, 45/64, 29/64, 31/64]$

$p[23] = [31/32, 23/32, 31/32, 23/32, 47/64]$

$p[24] = [63/64, 31/64, 31/64, 63/64, 63/64]$

$p[25] = [3/4, 0, 0, 3/4, 3/64]$

$p[26] = [49/64, 49/64, 33/64, 33/64, 19/64]$

$p[27] = [25/32, 9/32, 25/32, 9/32, 35/64]$

$p[28] = [51/64, 35/64, 19/64, 3/64, 51/64]$

$p[29] = [15/16, 3/16, 15/16, 3/16, 15/64]$

$p[30] = [61/64, 61/64, 29/64, 29/64, 31/64]$

$p[31] = [31/32, 15/32, 7/32, 23/32, 47/64]$

$p[32] = [63/64, 47/64, 47/64, 63/64, 63/64]$

$p[33] = [0, 0, 0, 0, 0]$

$p[34] = [1/64, 49/64, 33/64, 17/64, 1/4]$

$p[35] = [1/32, 9/32, 25/32, 17/32, 1/2]$

$p[36] = [3/64, 35/64, 19/64, 51/64, 3/4]$

$p[37] = [3/16, 3/16, 15/16, 15/16, 3/16]$

$p[38] = [13/64, 61/64, 29/64, 45/64, 7/16]$

$p[39] = [7/32, 15/32, 7/32, 15/32, 11/16]$

$p[40] = [15/64, 47/64, 47/64, 15/64, 15/16]$

$p[41] = [0, 3/4, 3/4, 0, 0]$

$p[42] = [1/64, 1/64, 17/64, 17/64, 1/4]$

$p[43] = [1/32, 17/32, 1/32, 17/32, 1/2]$

$p[44] = [3/64, 19/64, 35/64, 51/64, 3/4]$

$p[45] = [3/16, 15/16, 3/16, 15/16, 3/16]$

$p[46] = [13/64, 13/64, 45/64, 45/64, 7/16]$

$p[47] = [7/32, 23/32, 31/32, 15/32, 11/16]$

$p[48] = [15/64, 31/64, 31/64, 15/64, 15/16]$

$p[49] = [3/4, 3/4, 3/4, 3/4, 3/64]$

$p[50] = [49/64, 1/64, 17/64, 33/64, 19/64]$

$p[51] = [25/32, 17/32, 1/32, 9/32, 35/64]$

$p[52] = [51/64, 19/64, 35/64, 3/64, 51/64]$

$p[53] = [15/16, 15/16, 3/16, 3/16, 15/64]$

$p[54] = [61/64, 13/64, 45/64, 29/64, 31/64]$

$p[55] = [31/32, 23/32, 31/32, 23/32, 47/64]$

$p[56] = [63/64, 31/64, 31/64, 63/64, 63/64]$

$p[57] = [3/4, 0, 0, 3/4, 3/64]$

$p[58] = [49/64, 49/64, 33/64, 33/64, 19/64]$

$p[59] = [25/32, 9/32, 25/32, 9/32, 35/64]$

$p[60] = [51/64, 35/64, 19/64, 3/64, 51/64]$

$p[61] = [15/16, 3/16, 15/16, 3/16, 15/64]$

$p[62] = [61/64, 61/64, 29/64, 29/64, 31/64]$

$p[63] = [31/32, 15/32, 7/32, 23/32, 47/64]$

$p[64] = [63/64, 47/64, 47/64, 63/64, 63/64]$

4. The point set for the digital $(2, 3, 5)-$net over $GF(2^2)$ constructed by the duality theory for the subspace $M^{\perp}$ in Example 3 of subsection 3-2-2 is shown by the digital method as follows ($\psi(0) = 0, \psi(x^k) = k \in \{1, 2, \cdots, 8\}$).

$p[1] = [0, 0, 0, 0, 0]$

$p[2] = [1/16, 0, 0, 0, 0]$

$p[3] = [1/8, 0, 0, 0, 0]$

$p[4] = [3/16, 0, 0, 0, 0]$

$p[5] = [0, 0, 0, 0, 0]$

$p[6] = [1/16, 0, 0, 0, 0]$

$p[7] = [1/8, 0, 0, 0, 0]$

$p[8] = [3/16, 0, 0, 0, 0]$

$p[9] = [0, 0, 0, 0, 0]$

$p[10] = [1/16, 0, 0, 0, 0]$

$p[11] = [1/8, 0, 0, 0, 0]$

$p[12] = [3/16, 0, 0, 0, 0]$

$p[13] = [0, 0, 0, 0, 0]$

$p[14] = [1/16, 0, 0, 0, 0]$

$p[15] = [1/8, 0, 0, 0, 0]$

$p[16] = [3/16, 0, 0, 0, 0]$

$p[17] = [3/4, 3/4, 0, 0, 0]$

$p[18] = [13/16, 3/4, 0, 0, 0]$

$p[19] = [7/8, 3/4, 0, 0, 0]$

$p[20] = [15/16, 3/4, 0, 0, 0]$

$p[21] = [3/4, 3/4, 0, 0, 0]$

$p[22] = [13/16, 3/4, 0, 0, 0]$

$p[23] = [7/8, 3/4, 0, 0, 0]$

$p[24] = [15/16, 3/4, 0, 0, 0]$

$p[25] = [3/4, 3/4, 0, 0, 0]$

$p[26] = [13/16, 3/4, 0, 0, 0]$

$p[27] = [7/8, 3/4, 0, 0, 0]$

$p[28] = [15/16, 3/4, 0, 0, 0]$

$p[29] = [3/4, 3/4, 0, 0, 0]$

$p[30] = [13/16, 3/4, 0, 0, 0]$

$p[31] = [7/8, 3/4, 0, 0, 0]$

$p[32] = [15/16, 3/4, 0, 0, 0]$

$p[33] = [0, 0, 0, 0, 0]$

$p[34] = [1/16, 0, 0, 0, 0]$

$p[35] = [1/8, 0, 0, 0, 0]$

$p[36] = [3/16, 0, 0, 0, 0]$

$p[37] = [0, 0, 0, 0, 0]$

$p[38] = [1/16, 0, 0, 0, 0]$

$p[39] = [1/8, 0, 0, 0, 0]$

$p[40] = [3/16, 0, 0, 0, 0]$

$p[41] = [0, 0, 0, 0, 0]$

$p[42] = [1/16, 0, 0, 0, 0]$

$p[43] = [1/8, 0, 0, 0, 0]$

$p[44] = [3/16, 0, 0, 0, 0]$

$p[45] = [0, 0, 0, 0, 0]$

$p[46] = [1/16, 0, 0, 0, 0]$

$p[47] = [1/8, 0, 0, 0, 0]$

$p[48] = [3/16, 0, 0, 0, 0]$

$p[49] = [3/4, 3/4, 0, 0, 0]$

$p[50] = [13/16, 3/4, 0, 0, 0]$

$p[51] = [7/8, 3/4, 0, 0, 0]$

$p[52] = [15/16, 3/4, 0, 0, 0]$

$p[53] = [3/4, 3/4, 0, 0, 0]$

$p[54] = [13/16, 3/4, 0, 0, 0]$

$p[55] = [7/8, 3/4, 0, 0, 0]$

$p[56] = [15/16, 3/4, 0, 0, 0]$

$p[57] = [3/4, 3/4, 0, 0, 0]$

$p[58] = [13/16, 3/4, 0, 0, 0]$

$p[59] = [7/8, 3/4, 0, 0, 0]$

$p[60] = [15/16, 3/4, 0, 0, 0]$

$p[61] = [3/4, 3/4, 0, 0, 0]$

$p[62] = [13/16, 3/4, 0, 0, 0]$

$p[63] = [7/8, 3/4, 0, 0, 0]$

$p[64] = [15/16, 3/4, 0, 0, 0]$