# q-analogs of covering designs and Steiner systems based on singular linear space

You Gao[a,*], Gang Wang[a], Yinghua Han[b]

[a] *College of Science, Civil Aviation University of China, Tianjin 300300, P.R.China*

[b] *College of Science, Tianjin University of Science & Technology, Tianjin 300222, P.R.China*

**Abstract:** In this paper, q-analogs of covering designs and Steiner systems based on the subspaces of type $(m,0)$ and the subspaces of type $(m_1,0)$ in singular linear space $\mathbb{F}_q^{(n+l)}$ over $\mathbb{F}_q$ are presented, $m_1 < m$. Then the properties about q-analogs of covering designs and Steiner systems are discussed.

**Keywords:** q-analog, covering designs, Steiner systems, singular linear space.

## §1 Introduction

Let $\mathbb{F}_q$ be a finite field with $q$ elements, where $q$ is a power of a prime and $\mathbb{F}_q^{(n)}$ is the $n$-dimensional row vector space over $\mathbb{F}_q$, where $n$ is a positive integer. The set of all the subspaces with dimension $k$ of $\mathbb{F}_q^{(n)}$ is called Grassmannian space over $\mathbb{F}_q$, denoted by $\mathcal{G}_q(n,k)$. For any two subspaces $U$ and $V$ in $\mathcal{G}_q(n,k)$, define the distance function between $U$ and $V$

$$d(U,V) = 2m - 2\dim(U \cap V).$$

The function above is proved a metric (see [1]), thus $\mathcal{P}_q(n)$ can be regarded as a metric space.

A nonempty collection $\mathbb{C}$ of $\mathcal{G}_q(n,k)$ is called a subspace code $(n,M,d,k)_q$ if the size is $M$ and the minimum distance is $d$.

Subspace code plays an important role in random network coding (see [2,3]). R.Koetter and F.R.Kschischang[4,5] defined an operator channel

*Corresponding author.
E-mail addresses: gao_you@263.net.

when they studied random network coding, meanwhile, they showed that the errors and erasures could be corrected by a subspace code $(n, M, d, k)_q$ over the operator channel if the sum of errors and erasures is less than $\frac{d}{2}$. These research results motivate great interests of more and more people in subspace codes (see [3]-[8]).

q-analogs of combinatoric designs are the necessary studied directions to subspace codes. Van lint J.H. and Wilson R.M.[9] present that various known combinatorial problems such as Sperner's Theorem have q-analogs. Braun M., Kerber A., laue R. and Suzuki H.[10] studied q-analogs of t-designs. Koetter R. and Kschischang F.R.[1] demonstrated the application of codes over the Grassmannian to error-correction in random network coding. schwartz M. and Etzion T.[11] present the codes and anticodes in the Grassman gragh. Etzion T. and Vardy A.[12] discussed the q-analogs of basic designs based on vector space of domension $n$. Etzion T.[13] discussed the covering of subspaces by subspaces about q-covering design $C_q[n, k, r]$.

In this paper, q-analogs of covering designs and Steiner systems based on singular linear space $\mathbb{F}_q^{(n+l)}$ over $\mathbb{F}_q$ are presented. Meanwhile, the properties about q-analogs of covering designs and Steiner systems are discussed.

## §2 Preliminaries

Let $\mathbb{F}_q$ be a finite field with $q$ elements, where $q$ is a prime power. $\mathbb{F}_q^{(n+l)}$ is the $(n+l)-$dimensional row vector space over $\mathbb{F}_q$, where $n$ and $l$ are two non-negative integers. The set of all $(n+l) \times (n+l)$ nonsingular matrices over $\mathbb{F}_q$ of the form

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

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

We have an action of $GL_{n+l,n}(\mathbb{F}_q)$ on $\mathbb{F}_q^{(n+l)}$ defined as follows:

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

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

The vector space $\mathbb{F}_q^{(n+l)}$, together with the above group action, is called the $(n+l)$-dimensional singular linear space over $\mathbb{F}_q$ (see [14]).

Let $e_i$ $(1 \leq i \leq n+l)$ be the row vector in $\mathbb{F}_q^{(n+l)}$ whose $i$-th coordinate is 1 and all other coordinates are 0. Denote by $E$ the $l$-dimensional subspace

of $\mathbb{F}_q^{(n+l)}$ generated by $e_{n+1}, e_{n+2}, \cdots, e_{n+l}$. An $m$-dimensional subspace $P$ of $\mathbb{F}_q^{(n+l)}$ is called a subspace of type $(m,k)$ if $\dim(P \cap E) = k$.

Introduce the anzahl formulas (see [14]) and use the Gaussian coefficient[15] for brevity

$$\begin{bmatrix} m_2 \\ m_1 \end{bmatrix}_q = \frac{\prod_{t=m_2-m_1+1}^{m_2} (q^t - 1)}{\prod_{t=1}^{m_1} (q^t - 1)}.$$

By convenience $\begin{bmatrix} m_2 \\ 0 \end{bmatrix}_q = 1$ and $\begin{bmatrix} m_2 \\ m_1 \end{bmatrix}_q = 0$ whenever $m_1 < 0$ and $m_2 < m_1$.

Denote the set of all the subspaces of type $(m,s)$ in $\mathbb{F}_q^{(n+l)}$ by $\mathcal{M}(m,s;n+l,n)$ and let

$$N(m,s;n+l,n) = |\mathcal{M}(m,s;n+l,n)|.$$

It is verified that $\mathcal{M}(m,s;n+l,n)$ is non-empty if and only if

$$0 \le s \le l \text{ and } 0 \le m-s \le n.$$

Moreover, if $\mathcal{M}(m,s;n+l,n)$ is non-empty, then

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

Let $P$ be a given subspace of type $(m,s)$ in $\mathbb{F}_q^{(n+l)}$. Denote by $\mathcal{M}(m_1,s_1;m,s;n+l,n)$ the set of all the subspaces of type $(m_1,s_1)$ contained in $P$. Let

$$N(m_1,s_1;m,s;n+l,n) = |\mathcal{M}(m_1,s_1;m,s;n+l,n)|.$$

It is verified that $\mathcal{M}(m_1,s_1;m,k;n+l,n)$ is non-empty if and only if

$$0 \le s_1 \le k \le l \text{ and } 0 \le m_1 - s_1 \le m - s \le n.$$

Moreover, if $\mathcal{M}(m_1,s_1;m,s;n+l,n)$ is non-empty, then

$$N(m_1,s_1;m,s;n+l,n) = q^{(m_1-s_1)(s-s_1)} \begin{bmatrix} m-s \\ m_1-s_1 \end{bmatrix}_q \begin{bmatrix} s \\ s_1 \end{bmatrix}_q.$$

Let $P$ a given subspace of type $(m_1,s_1)$ in $\mathbb{F}_q^{(n+l)}$. Denote by $\mathcal{M}'(m_1,s_1;m,s;n+l,n)$ the set of all the subspaces of type $(m,s)$ containing $P$. Let

$$N'(m_1,s_1;m,s;n+l,n) = |\mathcal{M}'(m_1,s_1;m,s;n+l,n)|.$$

It is verified that $\mathcal{M}'(m_1,s_1;m,s;n+l,n)$ is non-empty if and only if

$$0 \le s_1 \le s \le l \text{ and } 0 \le m_1 - s_1 \le m - s \le n.$$

Moreover, if $\mathcal{M}'(m_1, s_1; m, s; n+l, n)$ is non-empty, then $N'(m_1, s_1; m, s; n+l, n)$

$$= q^{(l-s)(m-s-m_1+s_1)} \begin{bmatrix} n-(m_1-s_1) \\ (m-s)-(m_1-s_1) \end{bmatrix}_q \begin{bmatrix} (l-s_1) \\ (s-s_1) \end{bmatrix}_q .$$

A Steiner structure $S_q[(m_1,0),(m,0),n+l]$ is a collection $\mathbb{S}$ of elements from $\mathcal{M}(m,0;n+l,n)$ satisfying that each element from $\mathcal{M}(m_1,0;n+l,n)$ is contained in exactly one element of $\mathbb{S}$.

A q-covering design $C_q[n+l,(m,0),(m_1,0)]$ is a collection $\mathbb{S}$ of elements from $\mathcal{M}(m,0;n+l,n)$ satisfying that each element from $\mathcal{M}(m_1,0;n+l,n)$ is contained in at least one element of $\mathbb{S}$.

A q-Turán design $T_q[n+l,(m,0),(m_1,0)]$ is a collection $\mathbb{S}$ of elements from $\mathcal{M}(m_1,0;n+l,n)$ satisfying that each element of $\mathcal{M}(m,0;n+l,n)$ contains at least one element from $\mathbb{S}$.

Let the q-covering number $C_q(n+l,(m,0),(m_1,0))$ be the minimum number of a q-covering design $C_q[n+l,(m,0),(m_1,0)]$ and let the q-Turán number $T_q(n+l,(m,0),(m_1,0))$ be the minimum number of a q-Turán design $T_q[n+l,(m,0),(m_1,0)]$. It is clear that a Steiner structure $S_q[(m_1,0),(m,0),n+l]$ is the smallest q-covering design $C_q[n+l,(m,0),(m_1,0)]$, that is,

$$|S_q[(m_1,0),(m,0),n+l]| = C_q(n+l,(m,0),(m_1,0)).$$

# §3 q-analogs of covering designs

**Definition 3.1** A q-covering design $C_q[n+l,(m,0),(m_1,0)]$ is a collection $\mathbb{S}$ of elements from $\mathcal{M}(m,0;n+l,n)$ satisfying that each element from $\mathcal{M}(m_1,0;n+l,n)$ is contained in at least one element of $\mathbb{S}$.

**Definition 3.2** A q-Turán design $T_q[n+l,(m,0),(m_1,0)]$ is a collection $\mathbb{S}$ of elements from $\mathcal{M}(m_1,0;n+l,n)$ satisfying that each element of $\mathcal{M}(m,0;n+l,n)$ contains at least one element from $\mathbb{S}$.

Given a set $\mathbb{S} \subseteq \mathcal{M}(m,0;n+l,n)$, define the following set $\mathbb{S}^\perp$, the orthogonal complement of $\mathbb{S}$:

$$\mathbb{S}^\perp = \{A^\perp : A \in \mathbb{S}\},$$

where $A^\perp \in \mathcal{M}(n+l-m,l;n+l,n)$ is the orthogonal complement of the subspace $A$ of type $(m,0)$ in $\mathbb{F}_q^{(n+l)}$.

**Theorem 3.1** $\mathbb{S}$ is a q-covering design $C_q[n+l,(m,0),(m_1,0)]$ if and only if $\mathbb{S}^\perp$ is a q-Turán design $T_q[n+l,(n+l-m_1,l),(n+l-m,l)]$.

**Proof** Let $\mathbb{S}$ be a q-covering design $C_q[n+l,(m,0),(m_1,0)]$. By the definition of $\mathbb{S}^\perp$ , $\mathbb{S}^\perp$ is a set of elements from $\mathcal{M}(n+l-m,l;n+l,n)$. For each element

$$A \in \mathcal{M}(n+l-m_1,l;n+l,n),$$

$A^\perp$ is a subspace of type $(m_1,0)$ in $\mathbb{F}_q^{(n+l)}$. Since $\mathbb{S}$ is a q-covering design $C_q[n+l,(m,0),(m_1,0)]$, there exist at least one element $B \in \mathbb{S}$ satisfying that

$$A^\perp \subseteq B, \ .$$

that is,

$$A \supseteq B^\perp \in \mathbb{S}^\perp.$$

Hence, each element of $\mathcal{M}(n+l-m_1,l;n+l,n)$ contains at least one element from $\mathbb{S}^\perp$. Thus, $\mathbb{S}^\perp$ is a q-Turán design

$$T_q[n+l,(n+l-m_1,l),(n+l-m,l)].$$

Similarly, if $\mathbb{S}$ is a q-Turán design

$$T_q[n+l,(n+l-m_1,l),(n+l-m,l)],$$

$\mathbb{S}^\perp$ is a q-covering design

$$C_q[n+l,(m,0),(m_1,0)]. \ \square$$

**Corollary 3.1** $C_q(n+l,(m,0),(m_1,0)) = T_q(n+l,(n+l-m_1,l),(n+l-m,l))$.

**Theorem 3.2** $C_q(n+l,(m,0),(m_1,0)) \geq \frac{q^{n+l}-q^l}{q^m-1} C_q(n+l-1,(m-1,0),(m_1-1,0))$.

**Proof** Let $\mathbb{S}$ be a optimal q-covering design $C_q[n+l,(m,0),(m_1,0)]$, that is, the number of subspaces of type $(m,0)$ in the q-covering design $C_q[n+l,(m,0),(m_1,0)]$ is

$$C_q(n+l,(m,0),(m_1,0)).$$

For each subspace of type $(m,0)$ in $\mathbb{S}$, there are

$$N(1,0;m,0;n+l,n) = \frac{q^m-1}{q-1}$$

subspaces of type $(1,0)$ contained in such subspace of type $(m,0)$. The total number of subspaces of type $(1,0)$ in $\mathbb{F}_q^{(n+l)}$ is

$$N(1,0;n+l,n) = \frac{q^{n+l}-q^l}{q-1}.$$

Therefore, there exists a subspace $P$ of type $(1,0)$ in $\mathbb{F}_q^{(n+l)}$ and the subspace $P$ is contained in at most

$$\frac{q^m-1}{q^{n+l}-q^l}C_q(n+l,(m,0),(m_1,0))$$

elements of $\mathbb{S}$. Suppose that the above subspace $P$ is contained in $r$ elements of $\mathbb{S}$. Clearly,

$$r \leq \frac{q^m-1}{q^{n+l}-q^l}C_q(n+l,(m,0),(m_1,0)).$$

Let $\mathbb{F}_q^{(n+l)} = P \oplus Q$, where $Q$ is a subspace of type $(n+l-1,l)$ of $\mathbb{F}_q^{(n+l)}$. Define

$$\mathbb{S}' = \{Y \cap Q : Y \in \mathbb{S} \text{ and } P \subseteq Y\},$$

then there are $r$ subspaces of type $(m-1,0)$ in $\mathbb{S}'$.

Let $A$ be a subspace of type $(m_1-1,0)$ of $Q$, and then $P \oplus A$ is a subspace of type $(m_1,0)$. Therefore, there is at least one $X \in \mathbb{S}$ satisfying that

$$P \oplus A \subseteq X.$$

Furthermore,

$$A = (P \oplus A) \cap Q \subseteq X \cap Q.$$

Clearly, $X \cap Q \in \mathbb{S}'$, that is, each subspace of type $(m_1-1,0)$ in $\mathbb{F}_q^{(n+l-1)}$ is contained in at least one subspace from $\mathbb{S}'$. Thus,

$$\mathbb{S}' = \{Y \cap Q : Y \in \mathbb{S} \text{ and } P \subseteq Y\}$$

is a q-covering design $C_q[n+l-1,(m-1,0),(m_1-1,0)]$, then

$$C_q(n+l-1,(m-1,0),(m_1-1,0)) \leq r \leq \frac{q^m-1}{q^{n+l}-q^l}C_q(n+l,(m,0),(m_1,0)).$$

the Theorem 3.2 follows immediately. □

**Theorem 3.3** $C_q(n+l,(m,0),(m_1,0)) \geq q^{m_1 l}\frac{\begin{bmatrix} n \\ m_1 \end{bmatrix}_q}{\begin{bmatrix} m \\ m_1 \end{bmatrix}_q}$.

**Proof** Let $\mathbb{S}$ be a q-covering design $C_q[n+l,(m,0),(m_1,0)]$. For a fixed subspace $P$ of type $(m,0)$ of $\mathbb{S}$, there are

$$N(m_1,0;m,0;n+l,n) = \begin{bmatrix} m \\ m_1 \end{bmatrix}_q$$

subspaces of type $(m_1,0)$ which are contained in the fixed subspace $P$. The total number of subspaces of type $(m_1,0)$ in $\mathbb{F}_q^{(n+l)}$ is

$$N(m_1,0;n+l,n) = q^{m_1 l}\begin{bmatrix} n \\ m_1 \end{bmatrix}_q.$$

Thus

$$|\mathbb{S}| \geq q^{m_1 l} \frac{\begin{bmatrix} n \\ m_1 \end{bmatrix}_q}{\begin{bmatrix} m \\ m_1 \end{bmatrix}_q}$$

Furthermore, if

$$|\mathbb{S}| = q^{m_1 l} \frac{\begin{bmatrix} n \\ m_1 \end{bmatrix}_q}{\begin{bmatrix} m \\ m_1 \end{bmatrix}_q},$$

each subspace of type $(m_1, 0)$ in $\mathbb{F}_q^{(n+l)}$ is exactly contained in one subspace of type $(m, 0)$ from $\mathbb{S}$. If so, $\mathbb{S}$ is called the Steiner structure $S[(m_1, 0), (m, 0), n + l]$. □

**Theorem 3.4** $C_q(n+l, (m,0), (m_1,0)) \leq C_q(n+l-1, (m-1,0), (m_1,0))$.

**Proof** Let $\mathbb{S}$ be a q-covering design $C_q[n + l - 1, (m - 1, 0), (m_1, 0)]$, that is,

$$\mathbb{S} = \{(P \vdots 0) \subset \mathbb{F}_q^{(n+l-1)} : \dim(P \vdots 0) = m - 1 \text{ and } \dim((P \vdots 0) \cap E) = 0\}.$$

Construct the following set $\mathbb{S}'$ from $\mathbb{S}$:

$$\mathbb{S}' = \{P' = \begin{pmatrix} P & \vdots 0 & \vdots 0 \\ 0 & \vdots 1 & \vdots 0 \end{pmatrix} \subset \mathbb{F}_q^{(n+l)}\},$$

where $\dim P' = m$ and $\dim(P' \cap E) = 0$.

Let $P_1$ be a subspace of type $(m_1, 0)$ in $\mathbb{F}_q^{(n+l)}$ and denote also by $P_1$ a matrix representation of the vector subspace $P_1$, i.e.,

$$P_1 = \begin{pmatrix} R_1 & x_1 & \vdots 0 \\ R_2 & x_2 & \vdots 0 \end{pmatrix}.$$

If $x_1 = x_2 = 0$, then $\begin{pmatrix} R_1 & \vdots 0 \\ R_2 & \vdots 0 \end{pmatrix}$ is a subspace of type $(m_1, 0)$ in $\mathbb{F}_q^{(n+l-1)}$. Since $\mathbb{S}$ is a q-covering design $C_q[n+l-1, (m-1, 0), (m_1, 0)]$, there exist at least one subspace $(P \vdots 0) \in \mathbb{S}$ such that $\begin{pmatrix} R_1 & \vdots 0 \\ R_2 & \vdots 0 \end{pmatrix} \subset (P \vdots 0)$.

Define

$$P' = \begin{pmatrix} P & \vdots 0 & \vdots 0 \\ 0 & \vdots 1 & \vdots 0 \end{pmatrix} \in \mathbb{S}'$$

and clearly $P_1 \subset P'$.

If $\text{rank}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 1$, without loss of generality, let $x_1 = 0$, $x_2 = 1$, then

$$P_1 = \begin{pmatrix} R_1 & 0 & \vdots\, 0 \\ R_2 & 1 & \vdots\, 0 \end{pmatrix},$$

furthermore,

$$P_1 = \begin{pmatrix} R_1 & 0 & \vdots\, 0 \\ 0 & 1 & \vdots\, 0 \end{pmatrix}.$$

Since $(R_1 \vdots 0)$ is a subspace of type $(m_1 - 1, 0)$ in $\mathbb{F}_q^{(n+l-1)}$, there is a subspace $R_3$ of type $(m_1, 0)$ in $\mathbb{F}_q^{(n+l-1)}$ such that $(R_1 \vdots 0) \subset R_3$. Next, there exist at least one subspace $(P \vdots 0) \in \mathbb{S}$ such that $R_3 \subset (P \vdots 0)$. Define

$$P' = \begin{pmatrix} P & \vdots\, 0 & \vdots\, 0 \\ 0 & \vdots\, 1 & \vdots\, 0 \end{pmatrix} \in \mathbb{S}'$$

and clearly $P_1 \subset P'$.

Hence $\mathbb{S}'$ is a q-covering design $C_q[n+l, (m,0), (m_1,0)]$, i.e.,

$$C_q(n+l, (m,0), (m_1,0)) \leq C_q(n+l-1, (m-1,0), (m_1,0)). \quad \square$$

Suppose that $m = n - t$,

$$C_q(n+l, (n-t,0), (m_1,0)) \leq C_q(n+l-1, (n-1-t,0), (m_1,0))$$

from Theorem 3.4, that is, the value of $C_q(n+l, (n-t,0), (m_1,0))$ is a non-increasing sequence of positive integers as $n$ increases for any fixed and $l$, $t$ and $m_1$. Hence, there is a constant $C_{l,t,m_1}$ such that

$$C_q(n+l, (n-t,0), (m_1,0)) = C_{l,t,m_1}$$

whenever $n$ is sufficiently large.

**Lemma 3.1** $C_q(n+l, (m,0), (1,0)) = |S_q[(1,0), (m,0), n+l]| = \frac{q^l(q^n-1)}{q^m-1}$, whenever $m$ divides $n$.

**Lemma 3.2** If $\delta \geq 0$, then $C_q(n+l+\delta, (m+\delta,0), (m_1,0)) \leq C_q(n+l, (m,0), (m_1,0))$.

**Theorem 3.5** If $n \leq 2m$, then $C_q(n+l, (m,0), (1,0)) = q^l \lceil \frac{q^n-1}{q^m-1} \rceil$.

**Proof** By lemma 3.1,
$C_q(2(n-m)+l,(n-m,0),(1,0))$

$$= \frac{q^l(q^{2(n-m)}-1)}{q^{n-m}-1} = q^l(q^{n-m}+1) = q^l\lceil\frac{q^n-1}{q^m-1}\rceil.$$

By lemma 3.2,

$$C_q(n+l,(m,0),(1,0)) = C_q(2(n-m)+2m-n+l,(n-m+(2m-n),0),(1,0))$$

$$\leq C_q(2(n-m)+l,(n-m,0),(1,0)) = q^l\lceil\frac{q^n-1}{q^m-1}\rceil.$$

Note that

$$C_q(n+l,(m,0),(1,0)) \geq q^l\lceil\frac{q^n-1}{q^m-1}\rceil$$

from Theorem 3.3. From the above two aspects,

$$C_q(n+l,(m,0),(1,0)) = q^l\lceil\frac{q^n-1}{q^m-1}\rceil, \text{ if } n \leq 2m. \quad \square$$

**Theorem 3.6** $T_q(n+l,(m,l),(m_1,l)) \leq \begin{bmatrix} n-m+m_1 \\ m_1-l \end{bmatrix}_q$, $l \leq m_1 \leq m$.

**Proof** Let $Q$ be a subspace of type $(n+l-m+m_1,l)$ in $\mathbb{F}_q^{(n+l)}$ and $\mathbb{S}$ is the set of all the subspaces of type $(m_1,l)$ contained in the subspace $Q$. From the anzahl formulas,

$$|\mathbb{S}| = N(m_1,l;n+l-m+m_1,l;n+l,n) = \begin{bmatrix} n-m+m_1 \\ m_1-l \end{bmatrix}_q.$$

Let $P$ be a subspace of type $(m,l)$. Since

$$\dim Q + \dim P = n+l-m+m_1+m = n+l+m_1,$$

$$\dim(P \cap Q) \geq m_1.$$

Therefore, the subspace $P$ contains at least one subspace of type $(m_1,l)$ of $\mathbb{S}$. By the definition of q-Turán design, $\mathbb{S}$ is a q-Turán design $T_q[n+l,(m,l),(m_1,l)]$, which implies that

$$T_q(n+l,(m,l),(m_1,l)) \leq |\mathbb{S}| = \begin{bmatrix} n-m+m_1 \\ m_1-l \end{bmatrix}_q. \quad \square$$

# §4 q-analog of Steiner systems

**Definition 4.1** A Steiner structure $S_q[(m_1,0),(m,0),n+l]$ is a collection $\mathbb{S}$ of elements from $\mathcal{M}(m,0;n+l,n)$ satisfying that each element from $\mathcal{M}(m_1,0;n+l,n)$ is contained in exactly one element of $\mathbb{S}$. The subspaces of type $(m,0)$ in the Steiner structure $S_q[(m_1,0),(m,0),n+l]$ are called blocks.

**Lemma 4.1** The total number of blocks in the Steiner structure $S_q[(m_1,0),(m,0),n+l]$ is $q^{m_1 l}\frac{\begin{bmatrix} n \\ m_1 \end{bmatrix}_q}{\begin{bmatrix} m \\ m_1 \end{bmatrix}_q}$.

**Theorem 4.1** If the Steiner structure $S_q[(m_1,0),(m,0),n+l]$ exists, $m_1 \geq 2$, then the Steiner structure $S_q[(m_1-1,0),(m-1,0),n+l-1]$ exists.

**Proof** Let $\mathbb{S}$ be the Steiner structure $S_q[(m_1,0),(m,0),n+l]$ and denote $\mathbb{F}_q^{(n+l)}$ by the following form:

$$\mathbb{F}_q^{(n+l)} = U_{n+l-1} \oplus U_1,$$

where $U_{n+l-1}$ is the subspace of type $(n+l-1,l)$ of $\mathbb{F}_q^{(n+l)}$ and $U_1$ is the subspace of type $(1,0)$ of $\mathbb{F}_q^{(n+l)}$. Define the set $\mathbb{S}'$:

$$\mathbb{S}' = \{W \cap U_{n+l-1} | W \in \mathbb{S},\ U_1 \subseteq W\}.$$

Clearly

$$W \cap U_{n+l-1}$$

of $\mathbb{S}'$ are the subspaces of type $(m-1,0)$ of $\mathbb{F}_q^{(n+l-1)}$.

For each subspace $Y$ of type $(m_1-1,0)$ of $\mathbb{F}_q^{(n+l-1)}$, $Y \oplus U_1$ is a subspace of type $(m_1,0)$ of $\mathbb{F}_q^{(n+l)}$. Therefore, $Y \oplus U_1$ is exactly contained in one subspace $W$ of type $(m,0)$ of $\mathbb{S}$, that is, $Y$ is exactly contained in one subspace

$$W \cap U_{n+l-1}$$

of $\mathbb{S}'$.

Therefore, $\mathbb{S}'$ is the Steiner structure $S_q[(m_1-1,0),(m-1,0),n+l-1]$, $m \geq 2$. □

**Corollary 4.1** If the Steiner structure $S_q[(m_1,0),(m,0),n+l]$ exists, then $\frac{\begin{bmatrix} n-i \\ m_1-i \end{bmatrix}_q}{\begin{bmatrix} m-i \\ m_1-i \end{bmatrix}_q}$ $(0 \leq i \leq m_1-1)$ is integer.

There are at least two trivial Steiner structures $S_q[(m_1,0),(n,0),n+l]$ and $S_q[(m_1,0),$
$(m_1,0),n+l]$.

**Theorem 4.2** If $n \leq 2m-m_1$, there only exists the trivial Steiner structure $S_q[(m_1,0),(n,0),n+l]$.

**Proof** Let $\mathbb{S}$ be the Steiner structure $S_q[(m_1,0),(m,0),n+l]$, $n \leq 2m-m_1$ and suppose that there are two different subspaces $W_1$ and $W_2$ of type

$(m,0)$ in $\mathbb{S}$. By the definition of the Steiner structure $S_q[(m_1,0),(m,0),n+l]$,

$$\dim(W_1 \cap W_2) \leq m_1 - 1,$$

that is,

$$\dim(W_1 + W_2) = 2m - \dim(W_1 \cap W_2) \geq 2m - m_1 + 1 \geq n + 1 > n,$$

a contradiction to $\mathbb{F}_q^{(n+l)}$.

Therefore, $\mathbb{S}$ is the Steiner structure $S_q[(m_1,0),(n,0),n+l]$, a trivial Steiner structure. □

**Theorem 4.3** If $2m - m_1 < n < 2m$, there only exists the trivial Steiner structure $S_q[(m_1,0),(m_1,0),n+l]$.

**Proof** Let $\mathbb{S}$ be the Steiner structure $S_q[(m_1,0),(m,0),n+l]$, $2m-m_1 < n < 2m$. Any subspace of type $(2m-m_1,0)$ in $\mathbb{F}_q^{(n+l)}$ contains at most one subspace of type $(m,0)$ of $\mathbb{S}$. Otherwise, suppose that the subspace of type $(2m-m_1,0)$ in $\mathbb{F}_q^{(n+l)}$ contains at least two different subspaces $W_1$ and $W_2$ of type $(m,0)$. By

$$\dim(W_1 + W_2) \leq 2m - m_1,$$

$$\dim(W_1 \cap W_2) \geq m_1,$$

a contradiction to the definition of the Steiner structure $S_q[(m_1,0),(m,0),n+l]$.

There are

$$N'(m,0;2m-m_1,0;n+l,n) = q^{ml-m_1l} \begin{bmatrix} n-m \\ m-m_1 \end{bmatrix}_q$$

subspaces of type $(2m-m_1,0)$ in $\mathbb{F}_q^{(n+l)}$ containing a given subspace of type $(m,0)$ of $\mathbb{S}$. Note that the total number of subspaces of type $(2m-m_1,0)$ in $\mathbb{F}_q^{(n+l)}$ is

$$N(2m-m_1,0;n+l,n) = q^{2ml-m_1l} \begin{bmatrix} n \\ 2m-m_1 \end{bmatrix}_q.$$

Hence,

$$q^{ml-m_1l} \begin{bmatrix} n-m \\ m-m_1 \end{bmatrix}_q \cdot |\mathbb{S}|$$

$$= q^{ml-m_1l} \begin{bmatrix} n-m \\ m-m_1 \end{bmatrix}_q \cdot q^{m_1l} \frac{\begin{bmatrix} n \\ m_1 \end{bmatrix}_q}{\begin{bmatrix} m \\ m_1 \end{bmatrix}_q} \leq q^{2ml-m_1l} \begin{bmatrix} n \\ 2m-m_1 \end{bmatrix}_q.$$

Since $2m - m_1 < n < 2m$,

$$\frac{(q^{n-m_1+1}-1)(q^{n-m_1+2}-1)\cdots(q^{2m-m_1}-1)}{(q^{n-m+1}-1)(q^{n-m+2}-1)\cdots(q^m-1)} \cdot \frac{1}{q^{(m-m_1)l}} \leq 1,$$

furthermore,

$$\frac{(q^{n-m_1+1}-1)(q^{n-m_1+2}-1)\cdots(q^{2m-m_1}-1)}{(q^{n-m+1}-1)(q^{n-m+2}-1)\cdots(q^m-1)} \leq 1,$$

that is,

$$m = m_1.$$

Therefore, $\mathbb{S}$ is the Steiner structure $S_q[(m_1,0),(m_1,0),n+l]$, a trivial Steiner structure. □

**Corollary 4.2** If there exists a nontrivial Steiner structure $S_q[(m_1,0),(m,0),n+l]$, $n \geq 2m$.


# Acknowledgements

This work is supported by the National Natural Science Foundation of China under Grant No.61179026 and the Fundamental Research Funds for the Central Universities under Grant No.SY-1416.


# References


[1] Koetter R., Kschischang F.R. Coding for errors and erasures in random network coding. IEEE Trans. Inf. Theory, 2008, 54(8): 3579-3591.

[2] Ahlswede R., Cai N., Li S.Y.R., Yeung R.W. Network information flow. IEEE Trans. Inf. Theory, 2000, 46(4): 1204-1216.

[3] Gadouleau M., Yan Z. Packing and covering properties of subspace codes for error control in random linear network coding. IEEE Trans. Inf. Theory, 2010, 56(5): 2097-2108.

[4] Koetter R., Kschischang F.R. Error correction in random netwok. presented at the 2nd Annual Workshop on Information Theory and Applications, La Jolla, CA, 2007.

[5] Ho T., Medard M., Koetter R., Karger D., Effros M., Shi J., Leong B. A random linear network coding approach to multicast. IEEE Trans. Inf. Theory, 2006, 52(10): 4413-4430.

[6] Silva D., Kschischang F.R., Koetter R. rank-metric approach to error control in random network coding. IEEE Trans. Inf. Theory, 54(9): 3951-3967.

[7] Gabidulin E. Bossert M. Codes for network coding. in Proc. IEEE Int. Symp. Information Theory, Toronto, ON, Canada, 2008.

[8] Gadouleau M., Yan Z. Constant-rank codes. in Proc. IEEE Int. Symp. Information Theory, Toronto, ON, Canada, 2008.

[9] Van lint J.H., Wilson R.M. A course in combinatorics. Cambridge University Press, 1992.

[10] Braun M., Kerber A., Laue R. Systematic construction of q-analogs of t-(v,k,$\lambda$)-designs. Designs, Codes and Cryptography, 2005, 34(1): 55-70.

[11] Schwartz M., Etzion T. Codes and anticodes in the Grassmann graph. J. Combin. Theory, ser. A, 2002, 97(1): 27-42.

[12] Etzion T., Vardy A. On q-analogs for Steiner systems and covering designs. Math. Commum, 2011, 5(2): 161-176.

[13] Etzion T. Covering of subspaces by subspaces, Designs. Codes and Cryptography, 2012, 72(2): 405-421.

[14] Wang Kaishun, Guo Jun, Li Fenggao. Singular linear space and its applications. Finite Fields Appl, 2011, 17(5): 395-406.

[15] Wan Zhexian, Geometry of Classical Groups Over Finite Fields, Science Press, Beijing, China, 2nd edition, 2002.