Construction of Extended Steiner Systems for Information Retrieval

Eun-Young Park and Ian Blake

Department of Electrical and Computer Engineering
University of Toronto
Toronto, Ontario — Canada
ecpark@comm.utoronto.ca   ifblake@comm.utoronto.ca

Received: March 2, 2007
Accepted: August 30, 2007

ABSTRACT

A multiset batch code is a variation of information retrieval where a t-multiset of items can be retrieved by reading at most one bit from each server. We study a problem at the other end of the spectrum, namely that of retrieving a t-multiset of items by accessing exactly one server. Our solution to the problem is a combinatorial notion called an extended Steiner system, which was first studied by Johnson and Mendelsohn [11]. An extended Steiner system $\mathrm{ES}(t,k,v)$ is a collection of k-multisets (thus, allowing repetition of elements in a block) of a v-set such that every t-multiset belongs to exactly one block. An extended triple system, with $t = 2$ and $k = 3$, has been investigated and constructed previously [3, 11]. We study extended systems over v elements with $k = t+1$, denoted as $\mathrm{ES}(t,t+1,v)$. We show constructions of $\mathrm{ES}(t,t+1,v)$ for all $t \geq 3$ and $v \geq t+1$.

Key words: information retrieval, batch codes, combinatorial designs, Steiner systems.

2000 Mathematics Subject Classification: 05B05, 05E05, 62K10.

Introduction

Information retrieval in distributed systems addresses the problem of reconstructing data reliably in the occurrence of server failures, transmitting information securely in the presence of an adversary and making an efficient use of database storage. While Asmuth and Blakely [1] used the Chinese remainder theorem to reconstruct data, Rabin [13] devised an information dispersal algorithm in which a file is decomposed into n pieces and can be reconstructed from every m pieces, $m < n$. It uses an error-correcting code technique and is efficient in storage and reliable in transmission. This problem has been studied widely in different settings since then. (See, for example, [4–8, 12].)

Recently, a new combinatorial notion, called a batch code, was introduced in [10], which is a variation of the information retrieval problem. A batch code encodes v data items into N bits and distributes them into b servers such that any t (distinct) items can be retrieved by reading at most one bit from each server. If each server stores one bit, hence, $N = b$, it is called a primitive batch code. If t items can be a multiset, it is called a multiset batch code. The aim of [10] is to design a multiset primitive batch code with the minimum number of servers b and the maximum retrieval parameter t for a given size v of the database. The best known primitive batch code is a subset code [10]. It has $b \approx 2^{H(\alpha)l}$ servers for $v = \binom{l}{w}$ data items and is able to retrieve $t = 2^{\Omega(w)}$ multiset items where $0 < \alpha = w/l < 0.5$ and $H(\cdot)$ denotes a binary entropy function.

We observe that while the batch code resides at one extreme of a variation of information retrieval problem, at the other end of the spectrum, we face the problem of accessing exactly one server to retrieve a set of t items. In this case, clearly, several items are stored in each server. Note that a Steiner system, denoted as $\mathrm{S}(t, k, v)$, provides a natural solution to the problem if the set consists of t distinct items. Every t-subset of the v-set belongs to exactly one block (server).

Then, a collection of k-multisets (called blocks) from a v-set such that every t-multiset belongs to exactly one block would provide a natural solution to the analogous problem of a multiset-batch code. In the literature, this combinatorial object is known as an extended design [2, 3, 11].

An extended triple system was introduced in [11] as a collection of 3-multisets (called blocks) chosen from a v-set such that every 2-multiset belongs to exactly one block. Johnson and Mendelsohn [11] showed necessary conditions for the existence of extended triple systems and conjectured that necessary conditions are also sufficient [11]. In [3], Bennett and Mendelsohn proved the conjecture and showed various constructions. A striking characteristic of an extended design is that the number of blocks is not unique for the given parameters t, k, and v. Bennett and Mendelsohn's constructions in [3] show extended triple systems with different numbers of blocks for a given value of v. An extended $(2, 4)$-design was introduced in [2] as a collection of 4-multisets from a v-set such that every 2-multiset belongs to exactly one block.

Since the number of blocks affects storage, we are interested in extended designs with minimum numbers of blocks. Hence, unlike previous work where the number of blocks was not the primary focus, we derive the minimum number of blocks for a given set of parameters and construct extended designs with minimum numbers of blocks.

While the information retrieval problems motivated this work, it has to be mentioned that both primitive batch codes and extended systems are far from practical at this point. It is nonetheless important to study them for the insight they provide for the problem.

In section 1, we introduce our notation and generalize an extended design to define an extended Steiner system. In section 2, we derive the minimum number of blocks in an extended triple system, $\mathrm{ES}(2,3,v)$. This shows that constructions in [3] give an extended triple system with the minimum number of blocks. In section 3, we study the conditions imposed on extended quadruple systems, $\mathrm{ES}(3,4,v)$ and compute the minimum number of blocks for this case. In section 4, we show a construction for a minimal extended quadruple system for all values of $v \geq 4$. This nice and simple construction was given by an anonymous referee. In section 5, we present a construction for an extended Steiner system $\mathrm{ES}(t,t+1,v)$ for all $v \geq t+1$. In section 6, we construct extended designs from finite projective planes for $t=2$, $k=q+2$ and $v=q^2+q+1$ for all prime powers q. This is a natural extension of the construction of $\mathrm{MES}(3,4,v)$ given by the anonymous referee. Then, we draw conclusions and suggest problems for further research in section 7.

1. Preliminaries

An extended triple system was defined in [11] and an extended $(2,4)$-design was defined in [2]. We generalize an extended design and define an extended Steiner system.

Definition 1.1. An extended Steiner system, denoted as $\mathrm{ES}(t,k,v)$, is a collection of k-multisets (called blocks) of a v-set such that every t-multiset belongs to exactly one block.

We note that an an $\mathrm{ES}(2,3,v)$ is called an extended triple system in [3, 11]. Similarly, we call an $\mathrm{ES}(3,4,v)$ an extended quadruple system.

Recall that a Steiner system $\mathrm{S}(t,k,v)$ is a collection of k-subsets (called blocks) of a v-set such that every t-subset belongs to exactly one block. The definition of an $\mathrm{ES}(t,k,v)$ is identical to that of a Steiner system except that the term, "subset," is replaced with "multiset." In spite of the similarity in definitions of these two systems, the presence of repeated elements in a block changes the object significantly. In particular, as mentioned earlier, the number of blocks in an extended Steiner system is not unique and this has been already shown in [3].

The minimum number of blocks b is a function of t, k and v. But this function itself changes and depends on v to make the number of blocks an integer. This will be discussed in detail in later sections.

The types of the blocks and t-multisets, the number of blocks and the number of t-multisets of a given type play an important role in determining the minimum number of blocks in an extended Steiner system.

With the exception of section 5, where we study $\mathrm{ES}(2,q+2,q^2+q+1)$, we study constructions of $\mathrm{E}(t,t+1,v)$ with an emphasis on extended triple systems and extended quadruple systems. We use round brackets to denote t-multiset types and square brackets to denote block types. Let $(1^{a_1}, 2^{a_2}, \dots, m^{a_m})$ be a t-multiset with m distinct elements, with the ith element repeated a_i times for all $i = 1, 2, \dots, m$. Hence, $a_1 + a_2 + \cdots + a_m = t$, $m \leq t$. Then, if $P_k(n)$ denotes the number of unordered partitions of n into k distinct parts, there are $\sum_{i=1}^{t} P_i(t)$ types of t-multisets. We say that a t-multiset is a $(1^{a_1}, 2^{a_2}, \dots, m^{a_m})$ t-multiset, if it is of the type $(1^{a_1}, 2^{a_2}, \dots, m^{a_m})$. We use this notation only to indicate the structure of a t-multiset. An actual t-multiset composed of elements, $\alpha_1, \alpha_2, \dots, \alpha_t$ will be denoted as $\{\alpha_1, \dots, \alpha_t\}$.

Similarly, let $[1^{d_1}, 2^{d_2}, \dots, l^{d_l}]$ be a block (a $(t+1)$-multiset) with l distinct elements, with the jth element repeated d_j times where $d_j > 0$ for all $j = 1, 2, \dots, l$. Hence, $d_1 + d_2 + \cdots + d_l = t + 1$, $l \leq t + 1$. Therefore, there are $\sum_{i=1}^{t+1} P_i(t+1)$ types of blocks. We say that B is a $[1^{d_1}, 2^{d_2}, \dots, l^{d_l}]$ block if a block B is of the type $[1^{d_1}, 2^{d_2}, \dots, l^{d_l}]$. Again, this notation is only to indicate the structure of the block ($(t+1)$-multiset). An actual block composed of the elements, α_1, α_2, …, α_{t+1} will be denoted as $\{\alpha_1, \alpha_2, \dots, \alpha_{t+1}\}$ where of course these $t+1$ elements need not be distinct.

We use $[v]$ to denote the set $\{0, 1, \dots, v-2, v-1\}$.

2. A minimal extended triple system

In this section, we define a minimal extended triple system and determine the minimum number of blocks for an extended triple system for a given v. We show that constructions in [3] are minimal. We denote an extended triple system over v elements as $\mathrm{ES}(2, 3, v)$ and a minimal extended triple system over v elements as $\mathrm{MES}(2, 3, v)$.

2.1. The minimum number of blocks in an extended triple system and the construction

Given an $\mathrm{S}(2, 3, v)$, an extended triple system can be trivially constructed by adding v blocks of the type $[1^3]$. Addition of v blocks of type $[1^3]$ of the form $\{i, i, i\}$ to $\mathrm{S}(2, 3, v)$, $1 \leq i \leq v$, generates an extended triple system with

$$\frac{\binom{v}{2}}{3} + v = \frac{v(v+5)}{6}$$

blocks.

However, it is possible to have a smaller number of blocks than in the above construction. In particular, we are interested in constructions with the minimum number of blocks. In an extended triple system, there can be three types of blocks: $[1^3]$, $[1^2, 2]$, and $[1, 2, 3]$. Let b_1 denote the number of blocks of the type $[1^3]$, b_2 the number of the blocks of the type $[1^2, 2]$, b_3 the number of the blocks of the type $[1, 2, 3]$.

Let p_1 be the number of pairs of the type (1^2) and p_2 be the number of pairs of the type $(1, 2)$. Then, a $[1^3]$ block contains one (1^2) pair; a $[1^2, 2]$ block contains

Table 1 – Pairs in each type of blocks

Number of Blocks	Block Type	p_1	p_2
b_1	$[1^3]$	1	0
b_2	$[1^2, 2]$	1	1
b_3	$[1, 2, 3]$	0	3
Total Number of Pairs		v	$\binom{v}{2}$

one (1^2) pair and one $(1, 2)$ pair; a $[1, 2, 3]$ block contains three $(1, 2)$ pairs. Table 1 shows the types and the number of pairs each block type contains.

Since there are v pairs of identical elements and $\binom{v}{2}$ pairs of distinct elements,

$$b_1 + b_2 = v,$$
$$b_2 + 3b_3 = \binom{v}{2}.$$

Then,

$$b_1 = v - b_2, \quad b_3 = \frac{\binom{v}{2} - b_2}{3},$$

Hence,

$$b = b_1 + b_2 + b_3 = -\frac{b_2}{3} + v + \frac{v(v-1)}{6}, \quad \text{given } b_1, b_2, b_3 \geq 0$$

is minimized by maximizing b_2 while satisfying the above conditions. Hence, the minimum number of blocks is given by

$$b_1 = 0, \quad b_2 = v, \quad b_3 = \frac{v(v-3)}{6},$$

and the total number of blocks b equals

$$b = b_1 + b_2 + b_3 = \frac{v(v+3)}{6}.$$

Since the number of blocks of different types b_1, b_2, b_3 must all be integers, v must be a multiple of 3.

When v is not a multiple of 3, the maximum value of b_2 which leads to an integer solution is $b_2 = v - 1$. Note that b_1 and b_3 are also integers when $b_2 = v - 1$ for $v \not\equiv 0 \pmod 3$. Hence, the minimum number of blocks for $v \equiv 1, 2 \pmod 3$ is given by

$$b_1 = 1, \quad b_2 = v - 1, \quad b_3 = \frac{(v-1)(v-2)}{6},$$

and the total number of blocks b equals

$$b = b_1 + b_2 + b_3 = \frac{(v+1)(v+2)}{6}.$$

Now we give the definition of a minimal extended triple system over v elements.

Definition 2.1. An $\mathrm{MES}(2,3,v)$ (a minimal extended triple system) for $v \equiv 0 \pmod 3$ is an extended triple system with $\frac{v(v+3)}{6}$ blocks. An $\mathrm{MES}(2,3,v)$ for $v \equiv 1,2 \pmod 3$ is an extended triple system with $\frac{(v+1)(v+2)}{6}$ blocks.

In [3], the authors proved the existence of $\mathrm{ES}(2,3,v)$ by showing various constructions for all v. It turns out that these constructions include constructions of $\mathrm{MES}(2,3,v)$. Therefore, we refer to the original construction in [3] for the constructions of $\mathrm{MES}(2,3,v)$.

Theorem 2.2 ([3, Theorem 3.1])**.** *A minimal extended triple system* $\mathrm{MES}(2,3,v)$ *exists for all* $v \geq 3$.

3. The minimal number of blocks in an extended quadruple system

In this section, we compute the minimum number of blocks in an extended quadruple system over v elements, denoted as $\mathrm{ES}(3,4,v)$. First, we note that an $\mathrm{ES}(3,4,v)$ exists for all $v \equiv 2,4 \pmod 6$.

Theorem 3.1. *An* $\mathrm{ES}(3,4,v)$ *exists for all* $v \equiv 2,4 \pmod 6$.

Proof. Hanani showed that an $\mathrm{S}(3,4,v)$ exists if and only if $v \equiv 2$ or $4 \pmod 6$ [9]. Given an $\mathrm{S}(3,4,v)$, add $\binom{v}{2}$ blocks of the form $\{i,i,j,j\}$ and v blocks of the form $\{i,i,i,i\}$, for all $i,j \in [v]$, $i \neq j$. Every triple of the type $(1,2,3)$ belongs to exactly one block in an $\mathrm{S}(3,4,v)$. Every triple of the type $(1^2,2)$ belongs to exactly one block of the form $\{i,i,j,j\}$ and every triple of the type (1^3) belong to exactly one block of the form $\{i,i,i,i\}$. Hence we have an $\mathrm{ES}(3,4,v)$ with

$$\frac{\binom{v}{3}}{4} + \binom{v}{2} + v = \frac{v(v+2)(v+7)}{24}$$

blocks. □

But this construction by no means yields the minimum possible number of blocks. In fact, it can be trivially reduced to $\frac{v(v^2+9v+2)}{24}$ blocks. Remove all $[1^4]$ blocks and the blocks $\{2i+1,2i+1,2i+2,2i+2\}$, $0 \leq i \leq \frac{v-2}{2}$. Then, insert the set of new blocks $\{2i+1,2i+1,2i+1,2i+2\}$ and $\{2i+2,2i+2,2i+2,2i+1\}$, $0 \leq i \leq \frac{v-2}{2}$. Clearly, this is an $\mathrm{ES}(3,4,v)$ with

$$\frac{v(v+2)(v+7)}{24} - \frac{v}{2} = \frac{v(v^2+9v+2)}{24}$$

blocks.

Since we are interested in an $\mathrm{ES}(3,4,v)$ with the minimum number of blocks, we develop notation and necessary conditions for the existence of $\mathrm{ES}(3,4,v)$.

3.1. Notation for $\mathbf{ES(3,4,v)}$

In preparation for defining a minimal ES$(3,4,v)$, we define some notation.

If repeated elements are allowed in a triple (3-multiset), there are three possible types of triples, (1^3), $(1^2,2)$, and $(1,2,3)$.

- Let T_1 denote the set of all triples of the form (1^3); then, $|T_1| = v$.
- Let T_2 denote the set of all triples of the form $(1^2,2)$; then, $|T_2| = 2\binom{v}{2}$.
- Let T_3 denote the set of all triples of the form $(1,2,3)$; then, $|T_3| = \binom{v}{3}$.

Note that there are five possible block types in ES$(3,4,v)$: $[1^4]$, $[1^3,2]$, $[1^2,2^2]$, $[1^2,2,3]$, and $[1,2,3,4]$. Throughout the paper, let $\mathcal{B}_1$ denote the set of all $[1^4]$ blocks, $\mathcal{B}_2$ the set of all $[1^3,2]$ blocks, $\mathcal{B}_3$ the set of all $[1^2,2^2]$, $\mathcal{B}_4$ the set of all $[1^2,2,3]$ blocks, and $\mathcal{B}_5$ the set of all $[1,2,3,4]$ blocks. Let b_i denote the cardinality of $\mathcal{B}_i$.

Definition 3.2. The element α is called the head of a triple if it is repeated in a triple. The triple $\{\alpha,\alpha,\beta\}$ is is called a headed pair and is said to be headed by α. In this case, α heads the element β.

Remark 3.3. Every element, $\alpha \in [v]$, must head $(v-1)$ headed pairs, (α,α,β), $\beta \in [v] \setminus \{\alpha\}$.

Definition 3.4. The element α is called the head of the block if it is repeated in the block. The block $\{\alpha,\alpha,\beta,\gamma\}$ is said to be headed by α.

Remark 3.5. Every block in $\mathcal{B}_3$ (the set of $[1^2,2^2]$ blocks) has two heads while every block in $\mathcal{B}_2$ and $\mathcal{B}_4$ has one head.

3.2. The minimum number of blocks in an $\mathbf{ES(3,4,v)}$ *if* $v \equiv 0 \pmod 2$

The type and the number of triples in each block depends on the block type.

- A $[1^4]$ block contains one (1^3) only.
- A $[1^3,2]$ block contains one (1^3) and one $(1^2,2)$.
- A $[1^2,2^2]$ block contains two $(1^2,2)$ 3-multisets.
- A $[1^2,2,3]$ block contains two $(1^2,2)$ and one $(1,2,3)$.
- Lastly, a $[1,2,3,4]$ block contains four $(1,2,3)$.

Table 2 summarizes this.

Recall that b_1 denotes the number of blocks of type $[1^4]$, b_2 type $[1^3,2]$, b_3 type $[1^2,2^2]$, b_4 type $[1^2,2,3]$, and b_5 type $[1,2,3,4]$. Then, in any given construction of

Table 2 – Triples in Each Type of Block

Number of Blocks	Type	t_1	t_2	t_3
b_1	$[1^4]$	1	0	0
b_2	$[1^3, 2]$	1	1	0
b_3	$[1^2, 2^2]$	0	2	0
b_4	$[1^2, 2, 3]$	0	2	1
b_5	$[1, 2, 3, 4]$	0	0	4
total number of triples		v	$2\binom{v}{2}$	$\binom{v}{3}$

ES$(3, 4, v)$, we must have

$$b_1 + b_2 = v, \tag{1}$$

$$b_2 + 2b_3 + 2b_4 = 2\binom{v}{2}, \tag{2}$$

$$b_4 + 4b_5 = \binom{v}{3}, \tag{3}$$

and we are interested in integer solutions to these equations that minimize the total number of blocks

$$b = b_1 + b_2 + b_3 + b_4 + b_5.$$

Note that

$$b_2 = v - b_1, \quad b_4 = \binom{v}{2} + \frac{(b_1 - 2b_3) - v}{2}, \quad b_5 = \frac{2\binom{v}{3} - 2\binom{v}{2} + v - (b_1 - 2b_3)}{8}.$$

Since

$$b_1 + b_2 + b_3 + b_4 + b_5 = \frac{1}{8}\left(2\binom{v}{3} + 6\binom{v}{2} + 5v + 3b_1 + 2b_3\right), \tag{4}$$

minimizing the total number of blocks is equivalent to minimizing $3b_1 + 2b_3$ given $b_1, b_2, b_3,\ b_4, b_5 \geq 0$. Hence, the solution is given by

$$b_1 = 0, \quad b_2 = v, \quad b_3 = 0, \quad b_4 = \frac{v(v-2)}{2}, \quad b_5 = \frac{v(v-2)(v-4)}{24}, \tag{5}$$

resulting in the total number of blocks of

$$b = b_1 + b_2 + b_3 + b_4 + b_5 = \frac{v(v+2)(v+4)}{24}. \tag{6}$$

Since the number of blocks, b_1, b_2, b_3, b_4, and b_5 must all be integers, v must be even. In addition, this is the unique solution for the minimum number of blocks for v even since $3b_1 + 2b_3$ is uniquely minimized by setting $b_1 = b_3 = 0$ and the values of the other parameters are determined by equations (1)–(3) as a result.

Definition 3.6. An MES$(3,4,v)$ (a minimal extended quadruple system over v elements), $v \equiv 0 \pmod 2$ is an ES$(3,4,v)$ with $\frac{v(v+2)(v+4)}{24}$ blocks.

3.3. The minimum number of blocks in an ES$(3,4,v)$ *if* $v \equiv 1 \pmod 2$

For an odd value of v, the number of blocks given by the equations (5) and (6) is not an integer. Moreover, note that by equation (2), b_2 must be an even integer. Since v is an odd integer and $b_1 = v - b_2$, b_1 must be an odd integer. In particular, $b_1 \neq 0$. Recall that the total number of blocks b is minimized by minimizing $3b_1 + 2b_3$ as shown in equation (4). Let H denote the set of the head elements in $[1^3, 2]$ blocks. Since there are $b_2 = v - b_1$ $[1^3, 2]$ blocks and each of these blocks has a unique head, the cardinality of H is b_2. Recall that in ES$(3,4,v)$, each element must head $(v-1)$ headed pairs as observed in Remark 3.3. Consider an arbitrary element $h \in H$. Then, h heads an even number of elements in $\mathcal{B}_4$. Also, h heads exactly one element in $\mathcal{B}_2$. Since h must head $v-1$ elements, which is an even integer, h must head an odd number of elements in $\mathcal{B}_3$. Therefore, at least one block of $\mathcal{B}_3$ is headed by each $h \in H$. Since there are two head elements in a $[1^2, 2^2]$ block, $b_3 \geq b_2/2$. Therefore,

$$3b_1 + 2b_3 \geq 3b_1 + b_2 = 3b_1 + v - b_1 = 2b_1 + v.$$

But since b_1 must be an odd integer, $b_1 \geq 1$. Hence,

$$3b_1 + 2b_3 \geq 2b_1 + v \geq 2 + v.$$

Therefore, the minimum possible number of blocks is obtained by setting

$$b_1 = 1, \quad b_3 = \frac{v-1}{2},$$

which achieves the bound with equality and the number of blocks b_i being integers.

Therefore, for v odd, the minimum number of blocks is given by

$$b_1 = 1, \quad b_2 = v - 1, \quad b_3 = \frac{v-1}{2}, \quad b_4 = \frac{(v-1)(v-2)}{2}, \quad b_5 = \frac{\binom{v-1}{3}}{4},$$

which leads the total number of blocks to be

$$b = b_1 + b_2 + b_3 + b_4 + b_5 = \frac{\binom{v+3}{3}}{4}.$$

Note that this is the minimum possible number of blocks for v odd. Since $b_1 = 1$ and $b_3 = (v-1)/2$ uniquely minimizes $3b_1 + 2b_3$ and determines the values of other parameters, this is a unique solution to the minimum possible number of blocks for ES$(3,4,v)$ with v odd.

Definition 3.7. An MES$(3,4,v)$ (a minimal extended quadruple system over v elements), $v \equiv 1 \pmod 2$ is an ES$(3,4,v)$ with $\frac{\binom{v+3}{3}}{4}$ blocks.

We have calculated the minimum possible number of blocks for v odd. In later sections, we show a construction of ES$(3,4,v)$ which meets these figures for v odd.

4. A construction of MES$(3, 4, v)$

The following theorem shows the existence of MES$(3, 4, v)$ for all $v \geq 4$. This simple and nice construction was given by an anonymous referee.

Theorem 4.1. *An* MES$(3, 4, v)$ *exists for all* $v \geq 4$.

Proof. Take the set of all quadruples $\{x_1, x_2, x_3, x_4\}$ for which $x_1 + x_2 + x_3 + x_4 \equiv 1 \pmod v$. Since every three multiset appears in exactly one quadruple, this set is an extended Steiner system ES$(3, 4, v)$.

First, suppose that v is even. Then, in this set, $b_1 = 0$ since there is no solution x to the equation $4x \equiv 1 \pmod v$. Note that similarly, $b_3 = 0$ since there is no solution x to the equation $2x + 2y \equiv 1 \pmod v$ for any given y. But this set is an extended quadruple system and b_1, b_2, b_3, b_4 and b_5 satisfy the equations (1)–(3). Since $b_1 = 0$ and $b_3 = 0$, this set gives an MES$(3, 4, v)$.

Second, suppose that v is odd. Then, there is a unique solution to the equation $4x \equiv 1 \pmod v$, hence, $b_1 = 1$ for the set. Similarly, for any given y, there is a unique solution x to the equation $2x + 2y \equiv 1 \pmod v$. Note that there are exactly $v - 1$ y's such that $x \not\equiv y$. Hence, $b_3 = \frac{v-1}{2}$. Then, the equations (1)–(3) determine the values of b_2, b_4, and b_5 and this set gives an MES$(3, 4, v)$. □

5. A construction of ES$(t, t + 1, v)$

The simple construction for an MES$(3, 4, v)$ suggests a general approach to the construction of MES$(t, t + 1, v)$. We present a construction of ES$(t, t + 1, v)$, which is a natural consequence of the construction of MES$(3, 4, v)$ given to us by an anonymous referee.

Theorem 5.1. *An* ES$(t, t + 1, v)$ *exists for all* $t \geq 2$ *and* $v \geq t + 1$.

Proof. Take the set of all $(t+1)$-tuples $(x_1, x_2, \dots, x_{t+1})$ such that $x_1+x_2+\cdots+x_{t+1} \equiv m \pmod v$ for some fixed residue m. Clearly, this is an ES$(t, t + 1, v)$ since every t-tuple belongs to exactly one $(t + 1)$-tuple in the set. □

We believe that $m = 1$ gives an MES$(t, t + 1, v)$ but we could not find a simple proof for all t and v.

6. Extended Steiner systems ES$(2, q + 2, q^2 + q + 1)$

In this section, we show a construction of a special subset of ES(t, k, v)s with $k > t+1$. An ES$(2, q + 2, q^2 + q + 1)$ is easily constructed from a finite projective plane.

Definition 6.1. A finite projective plane of order n is an S$(2, q + 1, q^2 + q + 1)$.

It is well known that finite projective plane of order q exists for all prime power q. In a finite projective plane, the number of elements equals the number of blocks in the system.

Theorem 6.2. *An* $\mathrm{ES}(2, q+2, q^2+q+1)$ *exists for prime power* q.

Proof. Recall that given a collection of m subsets $A_1, A_2, \dots, A_m$ of a set X, a set of m distinct elements of X, one from each A_i, $i = 1, 2, \dots, m$, is called a set of distinct representatives. Note that any set of k blocks contains $k(q+1)$ point occurrences. Since each point occurs in at most $q+1$ of these blocks, there must be at least k distinct points covered. Then, by applying Hall's theorem, we have a system of distinct representatives with q^2+q+1 elements from the set of blocks. Note that the block size is $q+2$ (not $q+1$) because we repeat one element (namely, the representative) of the block. This gives a simple construction of an $\mathrm{ES}(2, q+2, q^2+q+1)$. □

7. Conclusions

An extended Steiner system $\mathrm{ES}(t, k, v)$ is a collection of k-multisets (called blocks) of a v-set S such that every t-multiset belongs to exactly one block. It provides a trade-off between storage and the number of accessed servers for retrieving a multiset of items. In this paper, we considered constructions of extended Steiner systems $\mathrm{ES}(t, t+1, v)$ and $\mathrm{ES}(2, q+2, q^2+q+1)$ for prime powers q. Both $\mathrm{ES}(2, 3, v)$ and $\mathrm{ES}(2, q+2, q^2+q+1)$ require $O(v^2)$ servers for a retrieval of 2-multisets. Generally, an $\mathrm{ES}(t, t+1, v)$ requires $O(v^t)$ servers for a retrieval of t-multisets. The total number of data items equals v. Only one server access is necessary for an $\mathrm{ES}(t, k, v)$ for a retrieval of t-multisets where each server stores k bits. We note that the best known primitive batch code requires $O(2^{H(\alpha)l})$ storage for $v = \binom{l}{w}$ where $0 < \alpha = w/l < 0.5$ and each server stores only one bit. It can retrieve a multiset of $t = 2^{\Omega(w)}$ items where each server access acquires at most one bit.

Unlike ordinary designs, the number of blocks in an extended Steiner system is not unique. This leads to the definition of a minimal extended Steiner system. We have shown the following:

(i) A minimal extended triple system over v elements exists for all v and the constructions are in [3].

(ii) A minimal extended quadruple system over v elements exists for all v.

(iii) An $\mathrm{ES}(t, t+1, v)$ exists for all $v \geq t+1$.

(iv) An $\mathrm{ES}(2, q+2, q^2+q+1)$ is easily constructed by repeating an element in every block in a finite projective plane of order q where q is a prime power.

A number of interesting questions are open to be explored.

First, it is not known whether $m = 1$ gives a construction of an $\mathrm{MES}(t, t+1, v)$ for all t and v in Theorem 6.2. Second, Bennett and Mendelsohn investigated $\mathrm{ES}(2, 4, v)$

and we gave a construction of $\mathrm{ES}(2, q+2, q^2+q+1)$ but general construction of $\mathrm{ES}(t, k, v)$ is unknown for $k > t+1$. We believe that construction and analysis of extended Steiner systems will prove to be an interesting field for further exploration.

Acknowledgement. We would like to thank anonymous referees of this paper for pointing out references [2, 3, 11] and giving the construction for Theorem 4.1 and Theorem 6.2 which improved the first version of this paper.

References

[1] C. Asmuth and G. Blakely, *Pooling splitting and restituting information to overcome total failure of some channels of communication*, Proceedings of the Symposium on Security and Privacy, IEEE Society, 1982, pp. 156–169.

[2] F. E. Bennett and E. Mendelsohn, *Extended* (2, 4)*-designs*, J. Combin. Theory Ser. A **29** (1980), no. 1, 74–86.

[3] F. E. Bennett and N. S. Mendelsohn, *On the existence of extended triple systems*, Utilitas Math. **14** (1978), 249–267.

[4] W. Burkhard and J. Menon, *Disk array storage system reliability*, Proceedings of Symposium of Fault-Tolerant Computing **23** (1993), 432–441.

[5] J. Byers, J. Considine, M. Mitzenmacher, and S. Rost, *Informed content delivery across adaptive overlay networks*, IEEE/ACM Trans. Netw. **12** (2004), no. 5, 767–780.

[6] J. Byers, M. Luby, and M. Mitzenmacher, *A digital fountain approach to asynchronous reliable multicast*, IEEE Journal on Selected Areas in Communications **20** (2004), no. 8, 1528–1540.

[7] J. Byers, M. Luby, M. Mitzenmacher, and A. Rege, *A digital fountain approach to reliable distribution of bulk data*, Proceedings of ACM Sigcomm **28** (1998), no. 4, 56–57.

[8] J. Garay, R. Gennaro, C. Jutla, and T. Rabin, *Secure distributed storage and retrieval*, Lecture Notes in Computer Science, vol. 1320, pp. 275–289.

[9] H. Hanani, *On quadruple systems*, Canad. J. Math. **12** (1960), 145–157.

[10] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, *Batch codes and their applications*, 6th Annual ACM Symposium on Theory of Computing, ACM, New York, 2004, pp. 262–271 (electronic).

[11] D. M. Johnson and N. S. Mendelsohn, *Extended triple systems*, Aequationes Math. **8** (1972), 291–298.

[12] T. Leighton, *Methods for message routing in parallel machines*, Proceedings of the Annual ACM Symposium on Theory of Computing, 1992, pp. 77–96.

[13] M. O. Rabin, *Efficient dispersal of information for security, load balancing, and fault tolerance*, J. Assoc. Comput. Mach. **36** (1989), no. 2, 335–348.