THE RESULTS ON OPTIMAL VALUES OF SOME COMBINATORIAL BATCH CODES

YUEBO SHEN
Information Department
Children’s Hospital of Hebei Province, Shijiazhuang 050031, China

DONGDONG JIA AND GENGSHENG ZHANG∗
College of Mathematics and Information Science
Hebei Normal University, Shijiazhuang 050024, China

(Communicated by Vitaly Skachek)

Abstract. An \((n, N, k, m)\)-combinatorial batch code (CBC) was defined by Paterson, Stinson and Wei as a purely combinatorial version of batch codes which were first proposed by Ishai, Kushilevitz, Ostrovsky and Sahai. It is a system consisting of \(m\) subsets of an \(n\)-element set such that any \(k\) distinct elements can be retrieved by reading at most one (or in general, \(t\)) elements from each subset and the number of total elements in \(m\) subsets is \(N\). For given parameters \(n, k, m\), the goal is to determine the minimum \(N\), denoted by \(N(n, k, m)\).

So far, for \(k \geq 5\), \(m + 3 \leq n < (m_k - 2)\), precise values of \(N(n, k, m)\) have not been established except for some special parameters. In this paper, we present a lower bound on \(N(m + 4, 5, m)\), which is tight for some \(n\) and \(k\). Based on this lower bound, the monotonicity of optimal values of CBC and several constructions, we obtain \(N(m + 4, 5, m)\), \(N(m + 4, 6, m)\) and \(N(m + 3, 7, m)\) in different ways.

1. Introduction

Batch codes were introduced by Ishai, Kushilevitz, Ostrovsky and Sahai [7]. A batch code specifies a method to distribute a database of \(n\) items among \(m\) servers in such a way that any \(k\) items can be retrieved by reading at most \(t\) items from each server, and the total number of items stored in \(m\) servers is \(N\). It can be employed in a distributed database scenario for load balancing. The goal is to minimize the total storage, which is interesting and practically important.

Batch codes can be defined as follows:

**Definition 1.1.** (cf. [7] Section 1.1) An \((n, N, k, m, t)\) batch code over an alphabet \(\sum\) encodes a string \(x \in \sum^n\) into an \(m\)-tuple of strings \(y_1, y_2, \ldots, y_m \in \sum^∗\) (also referred to as servers) of total length \(N\), such that for each \(k\)-tuple (batch) of distinct indices \(i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}\), the entries \(x_{i_1}, x_{i_2}, \ldots, x_{i_k}\) from \(x\) can be decoded by reading at most \(t\) symbols from each server.

2010 Mathematics Subject Classification: Primary: 05B30, 05D05; Secondary: 68P20, 68P30.
Key words and phrases: Set system, optimal CBC, monotonicity, distributed storage.

This research is partially supported by National Natural Science Foundation of China (Grant No. 11571091), Natural Science Foundation of Hebei Education Department (Grant No. ZD2016096) and Research Project of Health Commission of Hebei Province (Grant No. 20160419).

∗ Corresponding author: Gengsheng Zhang.
General batch codes allow encoding/decoding during the storage/retrival process. A simplified version, called replication-based batch code\cite{7}, is where each server stores a subset of items and decoding simply means reading items from servers. Paterson, Stinson and Wei \cite{9} call this construct a combinatorial batch code. They introduce the study of this family of batch codes.

Combinatorial batch codes can be defined as follows:

\textbf{Definition 1.2.} (\cite{9} Definition 1.3) An \((n, N, k, m, t)\) combinatorial batch code (CBC) is a set system \((X, \mathcal{B})\), where \(X\) is a set of \(n\) elements (called points), \(\mathcal{B}\) is a collection of \(m\) subsets of \(X\) (called blocks) and \(N = \sum_{B \in \mathcal{B}} |B|\), such that for each \(k\)-subset \(\{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\} \subseteq X\), there exists a subset \(C_i \subseteq B_i\), where \(|C_i| \leq t\), \(i = 1, 2, \ldots, m\), such that \(\{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\} = \bigcup_{i=1}^{m} C_i\).

In this definition, the points (elements of \(X\)) and blocks (subsets in \(\mathcal{B}\)) correspond to items and servers, respectively, and \(t\) serves to balance the load among servers. We will only consider the case \(t = 1\) in this paper. Such a batch code permits at most one item to be retrieved from each server. We follow the convention as given in \cite{9}, and denote \((n, N, k, m, 1)\)-CBC by \((n, N, k, m)\)-CBC or \((n, k, m)\)-CBC.

Recall that \(N\) is the total number of items stored in \(m\) servers. To save the total storage, we want \(N\) to be as small as possible. An \((n, N, k, m)\)-CBC is optimal \cite{9} if \(N \leq N'\) for all \((n, N', k, m)\)-CBC. We denote the minimum of \(N\) by \(N(n, k, m)\). Given \(n, k, m\), the objective is to determine \(N(n, k, m)\) and to give an explicit construction of an optimal CBC with corresponding parameters.

Precise values of \(N(n, k, m)\) have been given for the majority of parameters. Some known results are summarized as follows:

(i) (\cite{9} Theorem 2.9) If \(n \geq (k - 1)\binom{m}{k-1}\), then

\[ N(n, k, m) = kn - (k - 1)\binom{m}{k-1}. \]

(ii) (\cite{1} Theorem 3.2, \cite{4} Theorem 1 and \cite{10} Theorem 3) If \(\binom{m}{k-2} \leq n \leq (k - 1)\binom{m}{k-1}\), then

\[ N(n, k, m) = (k - 1)n - \left\lfloor \frac{(k-1)\binom{m}{k-1} - n}{m - k + 1} \right\rfloor. \]

Therefore, the problem of determining \(N(n, k, m)\) has been totally solved when \(n \geq \binom{m}{k-2}\). For small \(n\), the case of \(n = m\) is trivial and \(N(n, k, m) = n\) (\cite{9} Theorem 2.1). In \cite{9}, Paterson et al. obtain an optimal solution for the special case \(m = k\). They also give a construction of \((n, N, k, m)\)-CBC when \(n\) is not too much bigger than \(m\), and prove the construction is optimal in the case \(n = m + 1\).

(iii) (\cite{9} Theorem 2.2 and Theorem 2.5) \(N(n, k, k) = kn - k(k - 1)\). \(N(m + 1, k, m) = m + k\).

Brualdi et al. \cite{2, 3} explore the connection between combinatorial batch codes and transversal matroids. By applying various properties of the latter and analyzing the case of optimality, they determine the function \(N(m + 2, k, m)\). And Bujtás et al. \cite{5} obtain \(N(m + 2, k, m)\) by a purely combinatorial proof and several explicit constructions.
(iv) ([2] Theorem 4 and [5] Theorem 2) For any two integers $m$ and $k$, if $k \leq m \leq k + \sqrt{k}$, then

$$N(m+2,k,m) = 2m + \left\lfloor \frac{k}{m-k+1} \right\rfloor.$$  

If $m > k + \sqrt{k}$, then

$$N(m+2,k,m) = m + k - 2 + \left\lceil 2\sqrt{k} + k \right\rceil.$$  

Besides, $N(n,k,m)$ with fixed $k$ is also interesting. The case of $k=1$ is trivial and $N(n,1,m) = n$. From (i) and (ii), we can easily obtain $N(n,2,m)$ and $N(n,3,m)$. The value of $N(n,4,m)$ is presented in [4], which turns out to be more complex than that of $N(n,3,m)$.

Apart from the above results, Silberstein and Gál [11] provide an optimal $(q^2 + q - 1, q^3 - q, q^2 - q, q^2 - q)$-CBC based on resolvable transversal designs, i.e.

$$N(q^2 + q - 1, q^2 - q - 1, q^2 - q) = q^3 - q,$$

where $q \geq 3$ is a prime power. Chen et al. [6] show the monotonicity of optimal values of CBC. By using the monotonicity and some constructions, Jia, Zhang and Yuan [8] obtain the following results.

$$N(m+3,5,m) = m + 11 \ (m \geq 7), \ N(9,5,6) = 18.$$  

$$N(m+3,6,m) = m + 13 \ (m \geq 8), \ N(10,6,7) = 21.$$  

In this paper, we obtain the following conclusions in different ways.

$$N(m+4,5,m) = m + 13 \ (m \geq 8), \ N(m+4,5,m) = 21 \ (m = 6, 7).$$  

$$N(m+4,6,m) = m + 16 \ (m \geq 8), \ N(11,6,7) = 25.$$  

$$N(m+3,7,m) = m + 14 \ (m \geq 9), \ N(11,7,8) = 24.$$  

Now we present some lemmas we need in the rest of the paper.

Let $(X, B)$ be a set system. For $x \in X$, we call the number of blocks $B \in B$ containing $x$ the degree of $x$.

**Lemma 1.3.** ([6] Corollary 2.2) Let $(X, B)$ be an optimal $(n,N,k,m)$-CBC. If $2 \leq k \leq m < n$, then there exists at least one point in $X$ whose degree is greater than 1. Furthermore, the blocks containing a point of degree greater than 1 have length greater than 1.

**Lemma 1.4.** ([5] Corollary 2) For $1 \leq k \leq m \leq n$, $N(n+1,k,m+1) \leq N(n,k,m)+1$.
By repeatedly applying Lemma 1.4, we have
\begin{equation}
N(n + p, k, m + p) \leq N(n, k, m) + p,
\end{equation}
where \( p \) is a non-negative integer. In fact, add \( p \) new points and \( p \) singletons to an optimal \((n, N, k, m)\)-CBC such that each new point belongs to a unique singleton. Then the system derived is an \((n + p, N + p, k, m + p)\)-CBC.

Lemma 1.3 implies that the number of blocks in an optimal \((n + 1, N, k, m)\)-CBC will not be decreased if we delete a point of degree \( d \) (\( d \geq 2 \)) from the point set and the blocks containing it. Furthermore, the system derived is an \((n, N - d, k, m)\)-CBC. Hence we have

**Lemma 1.5.** ([8] Corollary 2.5) If there exists a point of degree \( d \) (\( d \geq 2 \)) in an optimal \((n + 1, N, k, m)\)-CBC, then
\[ N(n + 1, k, m) \geq N(n, k, m) + d. \]

**Lemma 1.6.** ([6] Theorem 2.6) For \( n \geq m \geq k \geq 2 \), \( N(n, k - 1, m) \leq N(n, k, m) \).

To complete the proof of the main theorems in Section 5, we need to improve the bound in Lemma 1.6.

**Theorem 1.7.** Suppose that \((X, B)\) is an optimal \((n, N_1, k, m)\)-CBC, where \( k \geq 2 \) and \( N_1 = N(n, k, m) \). If there exists a point of degree one which belongs to a block of length \( s \), then
\[ N(n, k - 1, m) \leq N(n, k, m) - s + 1. \]

**Proof.** Let \( x \in X \) be a point of degree one, \( x \in B \in B \) and \( |B| = s \). If \( s = 1 \), then from Lemma 1.6, the proof is completed. Next we suppose that \( s \geq 2 \). Notice that if \( B \) contains another point \( y \) of degree one, then the two points \( x, y \) only can be retrieved from the unique block \( B \). Since \( k \geq 2 \), it follows that each point in \( B \) except for \( x \) has degree at least two, which implies that replacing \( B \) with \( \{x\} \) will not decrease the cardinality of \( \bigcup_{B \in B} B \) which equals \( |X| \).

Define \((X, B')\) as the set system obtained from \((X, B)\) by replacing \( B \) with \( B' = \{x\} \). We claim that \((X, B')\) is an \((n, N_1 - s + 1, k - 1, m)\)-CBC. In fact, for any \((k - 1)\)-subset \( X_1 \) of \( X \), if \( x \in X_1 \), then \( X_1 \) can be retrieved in \( B' \) by the same way as that in \( B \). If \( x \) does not belong to \( X_1 \), then \( \{x\} \cup X_1 \) is a \( k \)-subset of \( X \) and can be retrieved in \( B \) in such a way that \( x \) is obtained from \( B \) and \( X_1 \) is obtained from \( B \setminus \{B\} \). Hence \( X_1 \) can be retrieved in \( B' \).

This paper is organized as follows. In Section 2, we provide a lower bound on \( N(n, k, k + 1) \), which is tight for some \( n \) and \( k \). By employing this lower bound, some results on the monotonicity of optimal values and several constructions, we determine \( N(m + 4, 5, m) \) and \( N(m + 3, 7, m) \) in Section 3 and 5, respectively. In Section 4, we study the condition for which the conclusion in Lemma 1.4 is an equality if \( n = m + 4, k = 6 \). Furthermore, we obtain \( N(m + 4, 6, m) \).

2. A LOWER BOUND ON \( N(n, k, k + 1) \)

To complete the results in the following sections, we provide a lower bound on \( N(n, k, k + 1) \) in this section.

**Theorem 2.1.** Let \( n, k \) be integers and \( n > k \geq 2 \). If \( n - k \) is odd, then
\[ N(n, k, k + 1) \geq \frac{(n - k + 3)(k + 1)}{2} - \left\lfloor \frac{2n}{n - k + 1} \right\rfloor. \]
If $n - k$ is even and $n - k \geq 4$, then
\[ N(n, k, k + 1) \geq \frac{(n - k + 2)(k + 1)}{2}. \]

Proof. Let $(X, B)$ be an $(n, N, k, k + 1)$-CBC. If there exist two blocks in $B$ with union of size at most $n - k$, then there exist at least $k$ points contained in neither of the two blocks which only can be retrieved from the remaining $k - 1$ blocks. This contradicts the fact that the combinatorial batch codes with $t = 1$ permit at most one point to be retrieved from each block. Therefore the union of any two blocks has length at least $n - k + 1$ in an $(n, N, k, k + 1)$-CBC, which implies that the number of blocks of size less than $\frac{n-k+1}{2}$ is at most 1.

Suppose that the minimum size of blocks in $B$ is $x$. If $x > \frac{n-k+1}{2}$, then
\[ N \geq (k + 1) \left( \frac{n - k + 1}{2} \right) + 1. \]

If $x < \frac{n-k+1}{2}$, then there exists exactly one block in $B$ of size $x$ and the others have size at least $n - k + 1 - x$. It follows that
\[ N \geq x + k(n - k + 1 - x) = k(n - k + 1) - (k - 1)x. \]

If $x = \frac{n-k+1}{2}$, then except for the blocks of size $x$, the others have size at least $n - k + 1 - x = x$, so the inequality (6) also holds. Hence we obtain a lower bound on $N(n, k, k + 1)$ when $x = \left\lfloor \frac{n-k+1}{2} \right\rfloor$.

Next let $B$ have minimum block size $\left\lfloor \frac{n-k+1}{2} \right\rfloor$. If $n - k + 1$ is even, then the blocks of size $\frac{n-k+1}{2}$ are pairwise disjoint, hence the number of those of size $\frac{n-k+1}{2}$ is at most $\left\lfloor \frac{2n}{n-k+1} \right\rfloor$. Notice that the other blocks have length at least $\frac{n-k+1}{2} + 1$, so we have
\[ N(n, k, k + 1) \geq \frac{(n - k + 3)(k + 1)}{2} - \left\lfloor \frac{2n}{n-k+1} \right\rfloor. \]

If $n - k + 1$ is odd and $B$ contains a block $B_0$ of length $\frac{n-k}{2} \geq 2$, then the other blocks have length at least $\frac{n-k+2}{2}$, and each of the blocks of size $\frac{n-k+2}{2}$ is disjoint from $B_0$. Since $k \geq 2$, there exists at least one block intersecting $B_0$ and of size greater than $\frac{n-k+2}{2}$. Otherwise the points of $B_0$ only can be retrieved from the unique block $B_0$. Therefore, we have
\[ N(n, k, k + 1) \geq \frac{n - k}{2} + \frac{(k - 1)(n - k + 2)}{2} + \frac{n - k + 4}{2} = \frac{(n - k + 2)(k + 1)}{2}. \]

Note that some direct calculations show that both the lower bounds in (7) and (8) are not greater than that in (6) when $x < \left\lfloor \frac{n-k+1}{2} \right\rfloor$.

Notice that the bound in Theorem 2.1 is tight for some $n$ and $k$. For example, from Theorem 2.1, we have
\[ N(k + 3, k, k + 1) \geq 3(k + 1) - \left\lfloor \frac{k + 3}{2} \right\rfloor, \]
where the equality holds according to Equation (1). Also the bound for $n = q^2 + q - 1$, $k = q^2 - q - 1$ is tight using Equation (2), where $q \geq 3$ is a prime power.

However for some $n, k$, the bound in Theorem 2.1 is definitely not tight. For example, according to Theorem 2.1, it follows that $N(17, 7, 8) \geq 48$. But there does not exist a $(17, 48, 7, 8)$-CBC. Suppose, to the contrary, that $(X, B)$ is a $(17, 48, 7, 8)$-CBC. Then there are two cases we need to consider:
By Lemma 1.3, Lemma 1.5 and Equation (3), we have

\begin{align*}
\text{Suppose that } & B \text{ the union of the eight blocks in } B \text{ only can be retrieved from at most 2 blocks in } B, \text{ which leads to a contradiction.}
\end{align*}

For (ii), note that the intersection of any two blocks has length at most 1. Hence the union of the eight blocks in $B$ has cardinality at least $6 \times 8 - \binom{5}{2} = 20$, which contradicts the fact that $n = 17$. Therefore $N(17, 7, 8) > 48$.

3. $N(m + 4, 5, m)$

By using some results on monotonicity of optimal values and a simple construction, we easily obtain $N(m + 4, 5, m)$ for $m \geq 8$.

**Theorem 3.1.** If $m \geq 8$, then $N(m + 4, 5, m) = m + 13$.

**Proof.** By Lemma 1.3, Lemma 1.5 and Equation (3), if $m \geq 7$, then

\begin{align*}
N(m + 4, 5, m) & \geq N(m + 3, 5, m) + 2 = m + 13.
\end{align*}

For $m \geq 8$, from the inequality (5), we have

\begin{align*}
N(m + 4, 5, m) & \leq N(12, 5, 8) + m - 8.
\end{align*}

Now we present a set system $(X_0, B_0)$, where $X_0 = \{1, 2, \ldots, 12\}$, and $B_0 = \{\{1, 4\}, \{2, 5\}, \{3, 6\}, \{4, 7, 8\}, \{5, 9, 10\}, \{6, 11, 12\}, \{7, 9, 11\}, \{8, 10, 12\}\}$. It is easy to show that $(X_0, B_0)$ is a $(12, 21, 5, 8)$-CBC. Therefore, if $m \geq 8$, then

\begin{align*}
N(m + 4, 5, m) & \leq N(12, 5, 8) + m - 8 \leq 21 + m - 8 = m + 13.
\end{align*}

The proof is completed.$\hfill\Box$

Now we present a construction of an optimal $(m+4, m+13, 5, m)$-CBC for $m \geq 8$. Let $X = X_0 \cup X_1$, where $X_1$ is an $(m - 8)$-element set and $X_0 \cap X_1 = \emptyset$. Let $B = B_0 \cup B_1$, where $B_1 = \{\{x\} : x \in X_1\}$. It is obvious that $|X| = m + 4$, $|B| = m$ and $\sum_{B \in B} |B| = m + 13$. It is also easy to see that $(X, B)$ is an $(m+4, m+13, 5, m)$-CBC. Similar constructions can be employed in the following two sections.

In what follows we determine $N(m + 4, 5, m)$ for $m = 6$ and $m = 7$.

**Theorem 3.2.** $N(10, 5, 6) = 21$.

**Proof.** From Theorem 2.1, we have $N(10, 5, 6) \geq 21$. We present a set system $(X, B)$, where $X = \{1, 2, \ldots, 10\}$, and

\begin{align*}
B = \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{1, 4, 7, 10\}, \{2, 5, 8, 10\}, \{3, 6, 9, 10\}\}.
\end{align*}

It is simple to show that $(X, B)$ is a $(10, 21, 5, 6)$-CBC. Therefore $N(10, 5, 6) = 21$. $\hfill\Box$

**Theorem 3.3.** $N(11, 5, 7) = 21$.

**Proof.** By Lemma 1.3, Lemma 1.5 and Equation (3), we have

\begin{align*}
N(11, 5, 7) & \geq N(10, 5, 7) + 2 = 18 + 2 = 20.
\end{align*}

Suppose that $N(11, 5, 7) = 20$. Let $(X, B)$ be an optimal $(11, 20, 5, 7)$-CBC. Because of the optimality, no singleton belongs to $B$. Otherwise $N(10, 5, 6) \leq 20 - 1 = 19$, which contradicts Theorem 3.2. Hence all blocks in $B$ have length at least 2. Since $N = 20$, at least one pair belongs to $B$. 

686 Yuebo Shen, Dongdong Jia and Gengsheng Zhang
We can infer that the union of any three blocks in an $(11, 5, 7)$-CBC has length at least 7 since if there exist three blocks with union of size at most 6, then the remaining at least 5 points will be retrieved from the remaining 4 blocks. Hence at most two pairs belong to $B$.

If $B$ contains exactly one pair, then $B$ consists of one pair and six triplets, say, $B_1 = \{u, v\}$. Since the two points $u, v$ should be retrieved from at least two blocks in $B$, there is another block containing $u$ or $v$, say $B_2$. If $|B_1 \cap B_2| = 2$, then for any other block $B \in B$ we have $|B_1 \cup B_2 \cup B| < 7$. Thus $|B_2 \setminus B_1| = 2$. Likewise, since the three points of $B_2$ should be retrieved from at least three blocks, at least one point of $B_2 \setminus B_1$ belongs to another block $B_3$. Then we have $|B_1 \cup B_2 \cup B_3| < 7$, which leads to a contradiction.

If two pairs belong to $B$, then $B$ consists of two pairs, four triplets and one block of size 4. Let $|B_1| = |B_2| = 2, |B_3| = 4$. Recall that the union of any three blocks has length at least 7, which suggests that $B_1 \cap B_2 = \emptyset$ and each triplet is disjoint from $B_1 \cup B_2$. Hence we can only obtain the 4 points contained in $B_1 \cup B_2$ from the 3 blocks $B_1, B_2$ and $B_4$. This yields a contradiction.

Therefore $N(11, 5, 7) \geq 21$. Let $(X, B)$ be a set system where $X = \{1, 2, \ldots, 11\}$ and $B = \{\{1, 2\}, \{2, 3, 4, 5\}, \{6, 7, 8\}, \{9, 10, 11\}, \{3, 6, 9\}, \{4, 7, 10\}, \{5, 8, 11\}\}$. By a simple verification, $(X, B)$ is an $(11, 21, 5, 7)$-CBC. Hence $N(11, 5, 7) = 21$. \hfill $\square$

4. $N(m + 4, 6, m)$

If the conclusion in Lemma 1.4 is an equality, that is, $N(n + 1, k, m + 1) = N(n, k, m) + 1$, then according to $N(n, k, m)$ and the construction of an $(n, N(n, k, m), k, m)$-CBC, we can easily obtain an optimal $(n + 1, N(n, k, m) + 1, k, m + 1)$-CBC, optimal $(n + 2, N(n, k, m) + 2, k, m + 2)$-CBC, \ldots. That is to say, we can obtain a series of optimal CBCs from one optimal CBC. Obviously, the following conclusions can be seen from (3), (4) and Theorem 3.1.

For $m \geq 7$, $N(m + 4, 5, m + 1) = N(m + 3, 5, m) + 1$.
For $m \geq 8$, $N(m + 4, 6, m + 1) = N(m + 3, 6, m) + 1$.
For $m \geq 8$, $N(m + 5, 5, m + 1) = N(m + 4, 5, m) + 1$.

Hence we can obtain an optimal $(m + 3, m + 11, 5, m)$-CBC $(m \geq 7)$, an optimal $(m + 3, m + 13, 6, m)$-CBC $(m \geq 8)$ and an optimal $(m + 4, m + 13, 5, m)$-CBC $(m \geq 8)$ from a $(10, 18, 5, 7)$-CBC, an $(11, 21, 6, 8)$-CBC and a $(12, 21, 5, 8)$-CBC, respectively.

In this section, we concentrate on the case of $n = m + 4, k = 6$. Here we study the condition for which the conclusion in Lemma 1.4 is an equality, from which we can easily obtain $N(m + 4, 6, m)$. We begin with two special cases.

**Theorem 4.1.** $N(11, 6, 7) = 25$.

**Proof.** Theorem 2.1 implies that $N(11, 6, 7) \geq 25$. Let $X = \{1, 2, \ldots, 11\}$ and $B = \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{1, 4, 7, 10\}, \{2, 5, 8, 10\}, \{3, 6, 9, 11\}, \{1, 5, 7, 11\}\}$. It is easy to check that the set system $(X, B)$ is an $(11, 25, 6)$-CBC. Hence $N(11, 6, 7) = 25$. \hfill $\square$

**Theorem 4.2.** $N(12, 6, 8) = 24$. 
Proof. According to Lemma 1.3, Lemma 1.5 and Equation (4), it follows that
\[ N(12,6,8) = N(11,6,8) + 2 = 21 + 2 = 23. \]

Suppose that \( N(12,6,8) = 23 \). Let \((X, \mathcal{B})\) be an optimal \((12,23,6,8)\)-CBC. There is no singleton contained in \( \mathcal{B} \), or \( N(11,6,7) \leq N(12,6,8) - 1 = 22 \), which contradicts Theorem 4.1. Notice that the union of any three blocks of \( \mathcal{B} \) has length at least 7, which suggests that \( \mathcal{B} \) contains at most two pairs. Furthermore, it follows from \( N = 23 \) that at least one pair belongs to \( \mathcal{B} \).

An argument similar to the one used in Theorem 3.3 shows that \( N(12,6,8) \geq 24 \). Let 
\[ X = \{1,2,\ldots,12\} \]
and \( \mathcal{B} = \{\{1,8,9\}, \{1,2,11\}, \{2,3,12\}, \{3,4,9\}, \{4,5,10\}, \{5,6,12\}, \{6,7,11\}, \{7,8,10\}\} \).

It can easily be shown that the set system \((X, \mathcal{B})\) is a \((12,24,6,8)\)-CBC. Therefore 
\[ N(12,6,8) = 24. \]

**Lemma 4.3.** If \( m \geq 8 \), then \( N(m + 5,6,m + 1) = N(m + 4,6,m) + 1 \).

Proof. If \( m \geq 8 \), then
\[ N(m + 4,6,m) \geq N(m + 3,6,m) + 2 = m + 13 + 2 = m + 15. \]

From (5) and Theorem 4.2, if \( m \geq 8 \), then
\[ N(m + 4,6,m) \leq N(12,6,8) + m - 8 = 24 + m - 8 = m + 16. \]

It follows that for \( m \geq 8 \),
\[ m + 15 \leq N(m + 4,6,m) \leq m + 16. \]

Assume there is some \( m \geq 8 \) such that \( N(m + 5,6,m + 1) < N(m + 4,6,m) + 1 \), then
\[ N(m + 5,6,m + 1) = N(m + 4,6,m) = m + 16. \]

Let \((X, \mathcal{B})\) be an optimal \((m + 5,m + 16,6,m + 1)\)-CBC. There is no singleton contained in \( \mathcal{B} \), since otherwise \( N(m + 4,6,m) \leq m + 16 = 1 + m + 15 \), which yields a contradiction. Therefore all blocks have length at least 2. Hence \( m + 16 \geq 2(m + 1) \), which implies that \( m \leq 14 \). Observe that \( 2(m + 1) \leq m + 16 < 3(m + 1) \) holds for \( 8 \leq m \leq 14 \), which suggests that \( \mathcal{B} \) contains at least \( 2m - 13 \) pairs.

Because of Lemma 1.5, if there exists a point of degree at least 3 in \( X \), then \( N(m + 4,6,m + 1) \leq m + 16 - 3 = m + 13 \), which is contrary to (4). Therefore, all points in \( X \) have degree either one or two. Since \( |X| = m + 5 \) and \( N = m + 16 \), it follows that the number of points of degree one is \( m - 6 \).

Since the two points of a pair should be retrieved from two blocks, at least one point in a pair has degree two. Suppose that both the points in a pair \( B_1 \in \mathcal{B} \) have degree two. Let \( B_1 = \{x,y\} \). If both \( x \) and \( y \) belong to another block \( B_2 \), then \( B_1 \neq B_2 \) (i.e. \( |B_2| \neq 2 \)) since otherwise \( \mathcal{B} \) remains an \((m + 5,m + 1)\)-CBC when \( B_2 \) is replaced with \( \{y\} \), contradicting minimality. Next we apply some local modifications to \((X, \mathcal{B})\). If \( x, y \in B_2 \) and \( |B_2| > 2 \), then we delete \( x \) from \( X \), and replace \( B_1 \) and \( B_2 \) with \( B'_1 = \{y\} \) and \( B'_2 = B_2 \setminus \{x,y\} \), respectively. If \( x \in B_2 \) and \( y \in B_3 \), then \( B_2 \neq B_3 \) since both \( x \) and \( y \) have degree 2. We delete \( x \) from \( X \) and replace \( B_1, B_2 \) and \( B_3 \) with \( B'_1 = \{y\} \), \( B'_2 = B_2 \setminus \{x\} \) and \( B'_3 = B_3 \setminus \{y\} \), respectively. Recall that \( \mathcal{B} \) contains no singleton, which implies that neither \( B'_2 \) nor \( B'_3 \) is empty.

Let \( Y = X \setminus \{x\} \). We can claim that the set system \((Y, \mathcal{B}')\) derived by applying the modifications above satisfies the definition of CBC with \( k = 6 \). In fact, for any 6-element subset \( X' \) of \( Y \), if \( X' \) does not contain \( y \), then it can be retrieved by the
Theorem 4.4. If $X'$ contains $y$, then the point $y$ can be obtained from $B'_1$, and the remaining points in $X'$ can be retrieved in the same way as shown in the original CBC. Therefore $(Y', B')$ is an $(m+4, m+16-3, 6, m+1)$-CBC, which contradicts the fact that $N(m+4, 6, m+1) = m + 14$.

Thus only one point has degree two in each pair of $(X, B)$, and the other has degree one. Recall that the number of pairs is at least $2m - 13$, so is the number of points of degree one. It follows that $m - 6 \geq 2m - 13$, which implies that $m \leq 7$. Therefore if $m \geq 8$, then $N(m+5, 6, m+1) = N(m+4, 6, m) + 1$.

The following theorem is a direct consequence of Theorem 4.2 and Lemma 4.3.

Theorem 4.4. If $m \geq 8$, then $N(m+4, 6, m) = m + 16$.

5. $N(m+3, 7, m)$

In this section, the goal is to determine $N(m+3, 7, m)$ for $m \geq 8$. We begin with the special case of $m = 8$.

Theorem 5.1. $N(11, 7, 8) = 24$.

Proof. According to Theorem 2.1, it follows that $N(11, 7, 8) \geq 24$. Now we construct an $(11, 24, 7, 8)$-CBC with the point set $X = \{1, 2, \ldots, 11\}$ and the block set

$B = \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\}, \{2, 6, 10\}, \{11, 4, 9\}\}$.

Hence we have $N(11, 7, 8) = 24$.

Theorem 5.2. $N(m+3, 7, m) = m + 14$, for $m \geq 9$.

Proof. To begin with, we present a set system $(X, B)$, where $X = \{1, 2, \ldots, 12\}$ and $B = \{\{1, 2\}, \{3, 4\}, \{5, 6\}, \{7, 8\}, \{2, 9, 10\}, \{4, 11, 12\}, \{5, 9, 11\}, \{8, 10, 11\}, \{6, 10, 12\}\}.

It is easy to show that $(X, B)$ is a $(12, 23, 7, 9)$-CBC. Inequality (5) suggests that if $m \geq 9$, then

$N(m+3, 7, m) \leq N(12, 7, 9) + m - 9 \leq m + 14$.

Because of Lemma 1.6 and Equation (4), it follows that for $m \geq 8$,

$N(m+3, 7, m) \geq N(m+3, 6, m) = m + 13$.

Hence for $m \geq 9$, we have

$m + 13 \leq N(m+3, 7, m) \leq m + 14$.

If there is a point of degree greater than or equal to 3 in an optimal $(m+3, N, 7, m)$-CBC, then according to Lemma 1.5,

$N(m+3, 7, m) \geq N(m+2, 7, m) + 3 = m + 11 + 3 = m + 14$.

Assume that $N(m+3, 7, m) = m + 13$. Then all points in the optimal $(m+3, N, 7, m)$-CBC have degree at most 2. Let $(X_1, B_1)$ be an optimal $(m+3, m+13, 7, m)$-CBC. It is obvious that the number of points of degree one in $X_1$ is $m-7$. If each of the points of degree one belongs to a singleton, then omitting these points and the singletons containing them, we can get a $(10, 20, 7, 7)$-CBC. This contradicts the fact that $N(10, 7, 7) = 28$. Hence at least one point of degree one belongs to a block of size greater than one. From Theorem 1.7, we have

$N(m+3, 6, m) \leq N(m+3, 7, m) - 1 = m + 12$,

but $N(m+3, 6, m) = m + 13$. This leads to a contradiction. Hence for $m \geq 9$, $N(m+3, 7, m) = m + 14$. 

□
ACKNOWLEDGMENTS

The authors would like to thank the referees and editors for their valuable suggestions which have helped improve this paper.

REFERENCES

[1] S. Bhattacharya, S. Ruj and B. Roy, Combinatorial batch codes: A lower bound and optimal constructions, Adv. Math. Commun., 6 (2012), 165–174.
[2] R. A. Bru Aldi, K. P. K iernan, S. A. M eyer and M. W. Sch roeder, Combinatorial batch codes and transversal matroids, Adv. Math. Commun., 4 (2010), 419–431.
[3] R. A. Bru Aldi, K. P. K iernan, S. A. M eyer, and M. W. Sch roeder, Erratum to “combinatorial batch codes and transversal matroids”, Adv. Math. Commun., 4 (2010), 597.
[4] C. Bujtás and Z. Tuza, Optimal batch codes: Many items or low retrieval requirement, Adv. Math. Commun., 5 (2011), 529–541.
[5] C. Bujtás and Z. Tuza, Optimal combinatorial batch codes derived from dual systems, Miskolc Math. Notes, 12 (2011), 11–23.
[6] J. Chen, S. Zhang and G. Zhang, Optimal combinatorial batch code: Monotonicity, lower and upper bounds, Sci. Sin. Math., 45 (2015), 311–320 (in Chinese).
[7] Y. Ishai, E. Kushilevitz, R. Ostrovsky and A. Sahai, Batch codes and their applications, in Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing STOC'04, New York, USA, 36 (2004), 262–271.
[8] D. Jia, G. Zhang and L. Yuan, A class of optimal combinatorial batch code, Acta Math. Sinica (Chin. Ser.), 59 (2016), 267–278. (in Chinese)
[9] M. B. Paterson, D. R. Stinson and R. Wei, Combinatorial batch codes, Adv. Math. Commun., 3 (2009), 13–27.
[10] S. Ruj and B. Roy, More on combinatorial batch codes, preprint arXiv:0809.3357v1.
[11] N. Silberstein and A. Gál, Optimal combinatorial batch codes based on block designs, Des. Codes Cryptogr., 78 (2016), 409–424.

Received May 2017; revised March 2018.

E-mail address: shen-y-b@163.com
E-mail address: hbsdjdd@163.com
E-mail address: gshzhang@hebtu.edu.cn