SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

February 2020, Vol. 63 122304:1–122304:15
https://doi.org/10.1007/s11432-019-2649-5

Locally repairable codes from combinatorial designs

Yu ZHANG[1,2,3,4] & Haibin KAN[1,2,3,4*]

[1]*Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai* 200433*, China;*
[2]*Fudan-Zhongan Joint Laboratory of Blockchain and Information Security, Shanghai Engineering Research Center of Blockchain, Shanghai* 200433*, China;*
[3]*Shanghai Institute for Advanced Communication and Data Science, Shanghai* 200433*, China;*
[4]*Shanghai Institute of Intelligent Electronics & Systems, Shanghai* 200433*, China*

Received 23 May 2019/Revised 1 August 2019/Accepted 18 September 2019/Published online 15 January 2020

Abstract Locally repairable codes (LRCs) were proposed to reduce the repair degree in distributed storage systems. In particular, LRCs with availability are highly desirable for distributed storage systems, since this kind of codes provide the mechanism of local repair for code symbols and parallel reading of hot data. In this paper, we propose four types of $(n, k, r, t)_q$ LRCs from combinatorial designs. We introduce several constructions of LRCs with strict availability and some constructions of distance-optimal LRCs with information-symbol locality. Most of our constructions in this paper are over $\mathbb{F}_2$, i.e., they are suitable for implementation.

Keywords locally repairable codes, erasure codes, combinatorial designs, distributed storage systems, codes with availability

Citation Zhang Y, Kan H B. Locally repairable codes from combinatorial designs. Sci China Inf Sci, 2020, 63(2): 122304, https://doi.org/10.1007/s11432-019-2649-5

1 Introduction

Distributed storage systems are widely used for large-scale data warehousing. In distributed storage systems, data integrity is ensured by employing erasure codes. For example, Reed-Solomon codes are widely used in distributed storage systems to ensure data integrity [1]. When node failure occurs, a number of new nodes connect to a subset of the undamaged nodes, and download information required to reconstruct the damaged nodes. This process is called data-repairing [2]. The bandwidth consumed in the recovery process is called repair bandwidth. Repair degree is the number of nodes connected during data-repairing.

Regenerating codes [2,3] and locally repairable codes (LRCs) [4] were proposed to ensure data reliability and efficient node repair. Regenerating codes reduce the repair bandwidth by improving the repair degree and downloading fewer data from each node, while LRCs reduce the repair degree. In recent years, LRCs have attracted the attention of many researchers due to their applications to distributed storage systems [4–7]. $[n, k, d]$ linear codes with (r, δ)-locality were introduced in [7]. In large-scale distributed storage systems, parallel reading of hot data is a desirable property. $[n, k, d]$ linear codes with (r, δ)-locality cannot guarantee parallel reading of hot data. To address the problem, Wang et al. [8] introduced the notation of $(n, k, r, t)_q$ LRCs with (r, t)-availability. In an $(n, k, r, t)_q$ LRC with (r, t)-availability, the data in any given node can be obtained in $t + 1$ different ways in parallel.

* Corresponding author (email: hbkan@fudan.edu.cn)

Definition 1. A code symbol c_i of a codeword c in an $[n,k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ is said to have (r,t)-availability, if we can find t disjoint subsets $\Gamma_1(i),\ldots,\Gamma_t(i)$ of $[n]\backslash i$, in which $|\Gamma_j(i)|\leqslant r,\ j\in[t]$, such that c_i can be represented by symbols indexed by $\Gamma_j(i)$ [8]. $\Gamma_1(i),\ldots,\Gamma_t(i)$ are t recovering sets of c_i, r is the locality of c_i, and t is the availability of c_i. If all information symbols in an $[n,k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ have (r,t)-availability, then the code $\mathcal{C}$ is an $(n,k,r,t)_q$ locally repairable code with information-symbol (IS) locality and (r,t)-availability (IS-LRC with (r,t)-availability for short). If all n code symbols in an $[n,k]$ code $\mathcal{C}$ over $\mathbb{F}_q$ have (r,t)-availability, then the code $\mathcal{C}$ is an $(n,k,r,t)_q$ locally repairable code with all-symbol (AS) locality and (r,t)-availability (AS-LRC with (r,t)-availability for short). Usually when the context is clear, the parameter q can be omitted.

Wang et al. [8] proposed a construction of square codes. $\mathcal{X}=\{X_{i,j}\}_{1\leqslant i,j\leqslant r+1}\subseteq\mathbb{F}_q^k$ is a set of $(r+1)^2$ column vectors s.t.

$$\begin{cases}\sum\limits_{i=1}^{r+1}X_{i,j}=0, & \text{for } 1\leqslant j\leqslant r+1,\\ \sum\limits_{j=1}^{r+1}X_{i,j}=0, & \text{for } 1\leqslant i\leqslant r+1.\end{cases}\tag{1}$$

For an $[n=(r+1)^2,k]_q$ code $\mathcal{C}$, if the generator matrix of $\mathcal{C}$ consists of the $(r+1)^2$ vectors in $\mathcal{X}$, then $\mathcal{C}$ is a square code. An $[n,k]_q$ square code is also an $(n,k,r,t=2)_q$ AS-LRC. Wang et al. [8] also gave an upper bound on minimum distance d of (n,k,r,t) LRCs:

$$d\leqslant n-k-\left\lceil\frac{t(k-1)+1}{t(r-1)+1}\right\rceil+2.\tag{2}$$

When $n=(r+1)^2$, $k\in[r+1,2r-1]$ and $q>\binom{n}{k+1}$, there exist $[n,k]_q$ square codes attaining the bound (2). When $n=(r+1)^2$, $k\in[2r,r^2]$ and $q>\binom{n}{k+1}$, the minimum distance of a square code always outperforms the bound (3) [8]. Rawat et al. [9] proved that for an (n,k,r,t) LRC in which each recovering set contains only one parity symbol, the minimum distance d satisfies:

$$d\leqslant n-k-\left\lceil\frac{kt}{r}\right\rceil+t+1.\tag{3}$$

They also introduced a construction of $(n,k,r,t)_q$ IS-LRCs with (r,t)-availability attaining the bound (3) and a construction of $(n,k,r,t)_q$ AS-LRCs with (r,t)-availability attaining the bound (3) from resolvable balanced incomplete block designs (RBIBDs) when $r|k$. The construction in [9] provided an extension to the construction in [8], improved availability of LRCs from 2 to $t\geqslant 2$. Su et al. [10] proposed constructions of LRCs from resolvable configurations by replacing the membership matrix used in [9].

Notice that compared to codes over $\mathbb{F}_q$ $(q>2)$, codes over $\mathbb{F}_2$ are more suitable for implementation. Hao et al. [11] provided a construction of $(n,k,r,t)_2$ IS-LRCs with (r,t)-availability from low-density parity-check (LDPC) codes. Balaji et al. [12] introduced the notation of locally repairable codes with strict availability (SA-LRCs).

Definition 2. An $(n,k,r,t)_q$ locally repairable code with strict availability ($(n,k,r,t)_q$ SA-LRC for short) [1, 12] is an $(n,k,r,t)_q$ AS-LRC with (r,t)-availability, and in its parity-check matrix H, the weight of each row is $r+1$ and the weight of each column is t.

Balaji et al. [12] also proposed a construction of $(n,k,r,t)_2$ SA-LRCs with code length $(r+1)^g$, in which $g\geqslant 1$. Zhang et al. [13] provided an extension to the construction in [12]. The construction in [13] does not require code length n to be a power of $r+1$. Balaji et al. [14] gave a construction of binary SA-LRCs from transposed incidence matrices of block designs without rigorous proof. The block length of the code in [14] attains the bound (6).

Apart from the bounds on minimum distance of LRCs, there are also bounds on code rate and block length of LRCs. Tamo et al. [15] concluded an upper bound on the code rate $\mathcal{R}$ of (n,k,r,t) LRCs with (r,t)-availability:

$$\mathcal{R}\leqslant\frac{1}{\prod_{j=1}^{t}(1+\frac{1}{jr})}.\tag{4}$$

Prakash et al. [16] provided an upper bound on the code rate of (n, k, r, t) LRCs with sequential repair property when $t = 2$:

$$\frac{k}{n} \leqslant \frac{r}{r+2}. \tag{5}$$

Balaji et al. [14] proposed a lower bound on the minimum code length of (n, k, r, t) SA-LRCs:

$$n \geqslant (r+1)^2 - \frac{(r+1)r}{t}. \tag{6}$$

Equality in (6) holds only when $t|r(r+1)$. An LRC with minimum distance d attaining bound (2) or bound (3) is called a distance-optimal LRC. An LRC with code rate $\mathcal{R}$ attaining bound (4) or bound (5) is called a rate-optimal LRC.

1.1 Contributions

This paper proposes four types of LRCs with availability properties. Moreover, most of our codes are constructed over binary field, which are especially practical for system implementation. Tables A1 and A2 in Appendix A list all the constructions with specific parameters and their optimality in this work. The main contributions of this paper are summarized below.

(1) We provide several constructions of SA-LRCs based on balanced incomplete block designs (BIBDs). Our first construction of this kind gives $(n, k, r, t)_q$ SA-LRCs based on resolvable designs. Given a $(\hat{v}, \hat{b}, \hat{r}, \hat{k}, \hat{\lambda})$-RBIBD, we can construct $(n = \hat{v}, k, r = \hat{k} - 1, t \leqslant r + 1)_q$ SA-LRCs. If we choose an $((r+1)^s, r+1, 1)$-RBIBD, in which $r+1$ is a prime power, we get $((r+1)^s, k, r, t \leqslant r+1)_q$ SA-LRCs with minimum distance $d \geqslant t+1$ and code rate $\mathcal{R} \geqslant 1 - \frac{t}{r+1} + \frac{t-1}{n}$.

Our second construction of this type gives $(n, k, r, t)_q$ SA-LRCs, in which $r+1 \geqslant 2$ and $(r+1)|n$. This construction does not require n to be a power of $r+1$, while $n = (r+1)^g$ is necessary in the construction from [12].

Our third construction of this kind gives $(n, k, r, t)_q$ SA-LRCs from transposed incidence matrices of BIBDs with rigorous proof. The block length of this construction attains the bound (6).

(2) We give several constructions of distance-optimal IS-LRCs with (r, t)-availability. In constructions of this type, $r|kt$. We propose an $(n = k + \frac{kt}{r}, k, r, t = \frac{k-1}{r-1})_2$ IS-LRC with (r, t)-availability from the incidence matrix of a $(k, r, 1)$-BIBD first. Then, we give $(n = k + \frac{kt}{r}, k, r, 1 \leqslant t \leqslant \frac{k-1}{r-1})_2$ IS-LRCs from the incidence matrix of a $(k, r, 1)$-RBIBD.

Our third construction of this kind gives an $(n = k + \frac{kt}{r}, k, r, t)_2$ IS-LRC based on the transposed incidence matrix of a $(\frac{kt}{r}, k, r, t, 1)$-BIBD. Then, we propose a construction of $(n = k + \frac{kt}{r}, k = \frac{r\hat{v}}{t}, 1 \leqslant r \leqslant \frac{\hat{v}-1}{t-1}, t)_2$ IS-LRCs from the transposed incidence matrix of a $(\hat{v}, t, 1)$-RBIBD.

Although it seems that the four constructions have the same block lengths, the constraints on them are different. The first construction of this type gives a fixed code for fixed k, r. The second construction of this kind gives a series of codes for fixed k, r. The third construction of this type gives a fixed code for fixed $\frac{kt}{r}, t$. The fourth construction of this kind gives a series of codes for fixed $\hat{v}, t$. The minimum distance of all constructions of this kind attains the bound (3), and the code rate of these constructions attains the bound (5) when $t = 2$. Codes of this type do not require $r|k$, while in the constructions in [9], $r|k$ is necessary.

(3) We give a construction of SA-LRCs from s mutually orthogonal Latin squares (MOLS) of order $r+1$. From s MOLS of order $r+1$, we can construct $(n = (r+1)^2, k, r, t \leqslant s+2)_2$ SA-LRCs. This construction will provide SA-LRCs with parameters that are impossible from BIBDs.

(4) We propose a construction of IS-LRCs with (r, t)-availability from MOLS and maximum distance separable (MDS) codes. Given s MOLS of order r and an $(N + t, k = r^2)_q$ MDS code, we can construct $(n = N + \frac{kt}{r} = N + tr, k = r^2, r, t \leqslant s+2)_q$ distance-optimal IS-LRCs.

1.2 Organization

The rest of this paper is organized as follows. In Section 2, we present some notations and background knowledge of combinatorial designs. In Section 3, we introduce constructions of $(n, k, r, t)_q$ SA-LRCs

from BIBDs. Section 4 gives constructions of distance-optimal $(n,k,r,t)_2$ IS-LRCs with (r,t)-availability from BIBDs. We propose a construction of $(n,k,r,t)_2$ SA-LRCs from MOLS in Section 5. Section 6 gives a construction of distance-optimal $(n,k,r,t)_q$ IS-LRCs with (r,t)-availability from MOLS. Section 7 concludes this paper.

2 Preliminaries

In this section we introduce some notations and background knowledge. $[i]$ denotes the set $\{1,\ldots,i\}$, and $[i,j]$ denotes $\{i,i+1,\ldots,j\}$, where $i<j$. $\mathbb{F}_q$ is a finite field of size q, in which q is a prime power. The support of a vector x is represented by supp_x. Assume that $\mathcal{C}$ is an (n,k) code. $\mathcal{C}|_{\mathcal{I}}$ is the restriction of $\mathcal{C}$ to $\mathcal{I}$, where $\mathcal{I}$ is a subset of $[n]$.

2.1 Backgrounds on block designs

$\hat{v}$, $\hat{k}$, $\hat{\lambda}$ are integers, $\hat{v}\geqslant\hat{k}\geqslant 2$ and $\hat{\lambda}\geqslant 1$. X is a finite set of elements. We call X a set of points. $\mathcal{B}$ is a collection of subsets of X. Elements in $\mathcal{B}$ are called blocks. $(X,\mathcal{B})$ is a $(\hat{v},\hat{k},\hat{\lambda})$-BIBD if $|X|=\hat{v}$, $|B|=\hat{k}$ for all $B\in\mathcal{B}$, and every pair of distinct points from X is contained in exactly $\hat{\lambda}$ blocks [17]. In a $(\hat{v},\hat{k},\hat{\lambda})$-BIBD, every point appears exactly $\hat{r}=\frac{\hat{\lambda}(\hat{v}-1)}{\hat{k}-1}$ times, and there are precisely $\hat{b}=\frac{\hat{v}\hat{r}}{\hat{k}}=\frac{\hat{\lambda}(\hat{v}^2-\hat{v})}{\hat{k}^2-\hat{k}}$ blocks. A $(\hat{v},\hat{k},\hat{\lambda})$-BIBD is also called a $(\hat{v},\hat{b},\hat{r},\hat{k},\hat{\lambda})$-BIBD, and $\{\hat{v},\hat{b},\hat{r},\hat{k},\hat{\lambda}\}$ is the set of its parameters. When $\hat{v}>\hat{k}\geqslant 2$, a $(\hat{v},\hat{k},\hat{\lambda})$-BIBD is said to be nondegenerate. A necessary condition for the existence of $(\hat{v},\hat{k},\hat{\lambda})$-BIBD is $\hat{v}$, $\hat{b}$, $\hat{r}$, $\hat{k}$, $\hat{\lambda}$ are all integers. For example, there does not exist a $(16,6,1)$-BIBD.

A $(\hat{v},\hat{k},\hat{\lambda})$-BIBD is called a symmetric BIBD (SBIBD) if $\hat{b}=\hat{v}$. In this case, $\hat{r}=\hat{k}$ and $\hat{\lambda}(\hat{v}-1)=\hat{k}^2-\hat{k}$. Every pair of distinct blocks in a $(\hat{v},\hat{k},\hat{\lambda})$-SBIBD intersects at $\hat{\lambda}$ points [17]. Given a positive integer n, a finite projective plane of order n is an $(n^2+n+1,n+1,1)$-SBIBD. When q is a prime power, there exists a finite projective plane of order q. If there exists a projective plane of order n, then n is the sum of two squares of integers.

A BIBD can also be represented by its incidence matrix. $(X,\mathcal{B})$ is a $(\hat{v},\hat{b},\hat{r},\hat{k},\hat{\lambda})$-BIBD, in which $|X|=\hat{v}$ and $|\mathcal{B}|=\hat{b}$. M is a $\hat{b}\times\hat{v}$ matrix. The rows of M are indexed by the blocks $B_1,\ldots,B_{\hat{b}}$, in which $B_i\in\mathcal{B}$ for all $i\in[\hat{b}]$, the columns of M are indexed by the points $p_1,\ldots,p_{\hat{v}}$, where $p_i\in X$ for all $i\in[\hat{v}]$. The entries m_{ij} in M are defined as follows:

$$m_{ij}=\begin{cases}1, & \text{if } p_j\in B_i,\\ 0, & \text{otherwise.}\end{cases} \tag{7}$$

Then M is the incidence matrix of a $(\hat{v},\hat{b},\hat{r},\hat{k},\hat{\lambda})$-BIBD [18]. The weight of each row in M is $\hat{k}$ and the weight of each column in M is $\hat{r}$. If M is an incidence matrix of a $(\hat{v},\hat{b},\hat{r},\hat{k},\hat{\lambda})$-SBIBD, then M^{T} is also an incidence matrix of a $(\hat{v},\hat{b},\hat{r},\hat{k},\hat{\lambda})$-SBIBD.

In a $(\hat{v},\hat{k},\hat{\lambda})$-BIBD $(X,\mathcal{B})$, a parallel class is a subset of disjoint blocks from $\mathcal{B}$ s.t. the union of these disjoint blocks is X. A resolution is a partition of $\mathcal{B}$ into several parallel classes. If $\mathcal{B}$ has a resolution, then $(X,\mathcal{B})$ is resolvable [18]. We denote a resolvable $(\hat{v},\hat{k},\hat{\lambda})$-BIBD by $(\hat{v},\hat{k},\hat{\lambda})$-RBIBD. In a $(\hat{v},\hat{k},\hat{\lambda})$-BIBD, if $(X,\mathcal{B})$ has a parallel class, then $\hat{k}|\hat{v}$, and the parallel class contains $\hat{v}/\hat{k}$ blocks. If $(X,\mathcal{B})$ is resolvable, then $\mathcal{B}$ is partitioned into $\hat{b}/(\hat{v}/\hat{k})=\hat{r}$ parallel classes. For each prime power q and positive integer n, we can construct a $(q^n,q,1)$-RBIBD [17]. If a nondegenerate $(\hat{v},\hat{b},\hat{r},\hat{k},\hat{\lambda})$-BIBD exists, then $\hat{b}\geqslant\hat{v}+\hat{r}-1$ and $\hat{r}\geqslant\hat{k}+\hat{\lambda}$ [18]. A finite affine plane of order n is an $(n^2,n,1)$-RBIBD [18]. When q is a prime power, there exists a finite affine plane of order q.

2.2 Orthogonal Latin squares

X is a finite set of size n. A Latin square [17] L of order n defined on X is an $n\times n$ array, in which every row (column) of L is a permutation of X. A Latin square L of order n defined on X can also be called a Latin square of order n with entries from X. Assume that the columns and rows are indexed by $i,j\in[n]$. We denote the element in L at the intersection of ith row and jth column as $L(i,j)$.

Assume that L_1 and L_2 are Latin squares of order n with entries from X and Y, in which $|X| = |Y| = n$. If for all $x \in X$ and $y \in Y$, there exists a unique pair (i, j), where $1 \leqslant i, j \leqslant n$, such that $L_1(i, j) = x$ and $L_2(i, j) = y$, then L_1 and L_2 are said to be orthogonal. A group of t Latin squares $L_1, \ldots, L_t$ of order n are said to be mutually orthogonal, provided that for any pair of distinct Latin squares L_i, L_j in this group, where $1 \leqslant i < j \leqslant t$, L_i and L_j are orthogonal. We denote the maximum number of MOLS of order n by $N(n)$. $N(n) \leqslant n - 1$ for all $n > 1$. And $N(n) = n - 1$ if and only if there exists an affine plane of order n. If there exist s MOLS of order n_1 and s MOLS of order n_2, then there exist s MOLS of order $n_1 n_2$ [18].

3 SA-LRCs from BIBD

Our first construction in this section is based on the incidence matrix M of a $(\hat{v}, \hat{k}, 1)$-RBIBD. We will show that for each $(\hat{v}, \hat{k}, 1)$-RBIBD, we can give a construction of $(n = \hat{v}, k, r = \hat{k}-1, t \leqslant r+1)_q$ SA-LRCs.

Theorem 1. For each $(\hat{v}, \hat{b}, \hat{r}, \hat{k}, 1)$-RBIBD, we can construct $(n = \hat{v}, k, r = \hat{k} - 1, t \leqslant r + 1)_q$ SA-LRCs, in which $q \geqslant 2$ is a prime power. Let d be the minimum distance of our code and $\mathcal{R}$ be the code rate of our code. Then $d \geqslant t + 1$ and $\mathcal{R} \geqslant 1 - \frac{t}{r+1} + \frac{t-1}{n}$.

Proof. We consider the incidence matrix M of a $(\hat{v}, \hat{b}, \hat{r}, \hat{k}, 1)$-RBIBD. We know that in an RBIBD, the blocks can be partitioned into $\hat{r}$ parallel classes. Therefore, the incidence matrix M of a $(\hat{v}, \hat{b}, \hat{r}, \hat{k}, 1)$-RBIBD can also be partitioned into $\hat{r}$ sub-matrices $\{M_1, \ldots, M_{\hat{r}}\}$:

$$M = \begin{pmatrix} M_1 \\ \vdots \\ M_{\hat{r}} \end{pmatrix}. \tag{8}$$

Each sub-matrix M_i denotes a parallel class in the RBIBD. From the definition of RBIBD, we can conclude that the weight of each row in M_i is $\hat{k}$, the weight of each column in M_i is 1. We choose $t \leqslant r+1$ matrices $M'_1, \ldots, M'_t$ from $\{M_1, \ldots, M_{\hat{r}}\}$, then construct a new matrix

$$H = \begin{pmatrix} M'_1 \\ \vdots \\ M'_t \end{pmatrix}. \tag{9}$$

In a $(\hat{v}, \hat{b}, \hat{r}, \hat{k}, 1)$-RBIBD, $\hat{r} \geqslant \hat{k} + 1$. Therefore, we can choose any $t \leqslant \hat{k} = r + 1$ parallel classes from M. In a $(\hat{v}, \hat{b}, \hat{r}, \hat{k}, 1)$-RBIBD, every pair of distinct points is contained in exactly $\hat{\lambda} = 1$ blocks, and each point appears $\hat{r}$ times in M, once in each M_i. The supports of t rows containing the same coordinate i in H only intersect at i. Assume that two rows in H containing i intersect in at least two coordinates. Then, at least two points represented by these coordinates are contained in two blocks. This contradicts with the fact that every pair of distinct points is contained in exactly $\hat{\lambda} = 1$ blocks.

If we take H as the parity-check matrix of an LRC, then each code symbol has t disjoint recovering sets of size $\hat{k} - 1$. There is one recovering set for this code symbol in each M'_i from $\{M'_1, \ldots, M'_t\}$. Note that the weight of each column in H is t, the weight of each row in H is $\hat{k}$. We get a parity-check matrix H of an $(n = \hat{v}, k, r = \hat{k} - 1, t \leqslant r + 1)_q$ SA-LRC.

Next, we will deduce the minimum distance and code rate of our construction. Let c be a codeword from our code with minimum distance d. Since each code symbol has (r, t)-availability, any code symbol from c could be recovered in case of at most t erasures at any position of c. Then, the minimum distance d of our code is lower bounded by $t + 1$.

There are t parallel classes from a $(\hat{v}, \hat{b}, \hat{r}, \hat{k}, 1)$-RBIBD in our parity-check matrix H, so there are totally $t \cdot \frac{\hat{v}}{\hat{k}}$ rows in H. For each choice of two sub-matrices M'_i, M'_j composed of two parallel classes in H, there exists one redundant row. Each parallel class is a partition of $\hat{v}$ elements into subsets of size $\hat{k}$. Assume

that the values of all the parity-check equations associated with M_i' are determined, and the values of all the parity-check equations associated with M_j' are determined except one parity-check equation in M_j'. Since M_i' and M_j' give two partitions of the same $\hat{v}$ elements, the value of the undetermined parity-check equation can be deduced from the value of other equations from M_i', M_j', which means this row in H associated with the undetermined parity-check equation can be represented by the other rows in M_i', M_j'. If we fix one parallel class in H, then for each remaining parallel class in H, we can get one redundant row. Therefore, there are at least $t-1$ redundant rows in H. The row rank of H is at most $t\cdot\frac{\hat{v}}{\hat{k}}-(t-1)$. $\mathcal{R}$ is the code rate:

$$\mathcal{R}=1-\frac{\mathrm{rank}(H)}{n}\geqslant 1-\frac{t\cdot\frac{\hat{v}}{\hat{k}}-(t-1)}{\hat{v}}=1-\frac{t}{\hat{k}}+\frac{t-1}{\hat{v}}=1-\frac{t}{r+1}+\frac{t-1}{n}. \tag{10}$$

This completes the proof.

For each $(\hat{v},\hat{b},\hat{r},\hat{k},1)$-RBIBD, we can construct $(n=\hat{v},k,r=\hat{k}-1,t\leqslant r+1)_q$ SA-LRCs. Therefore, from a finite affine plane of order $r+1$, we can construct $((r+1)^2,k,r,t\leqslant r+1)_q$ SA-LRCs, and from an $((r+1)^n,r+1,1)$-RBIBD, we can get $((r+1)^n,k,r,t\leqslant r+1)_q$ SA-LRCs. However, these codes require that $r+1$ is a prime power. We will give a construction of LRCs from the existing RBIBDs. With the following theorem, we can give a construction of SA-LRCs for arbitrary r.

Theorem 2. For any integer $r+1\geqslant 2$, we can factorize $r+1$ to the product of prime powers, i.e., $r+1=\prod_{i=1}^{l}q_i$. We factorize n to the product of prime powers, i.e., $n=\prod_{i=1}^{l}q_i^{m_i}$. We can construct $(n,k,r,t)_q$ SA-LRCs when $t\leqslant\min_{i\in[l]}\frac{q_i^{m_i}-1}{q_i-1}$ and q is a prime power.

Proof. For each factor q_i of $r+1$, we construct a $(q_i^{m_i},q_i,1)$-RBIBD $\mathcal{A}_i$. We give a construction of parity-check matrix H of our $(n,k,r,t)_q$ SA-LRC. We choose t parallel classes from each $\mathcal{A}_i$. In this case, $t\leqslant\min_{i\in[l]}\frac{q_i^{m_i}-1}{q_i-1}$. When m_i is large, t could be as large as $r+1$. M_i is the incidence matrix of t chosen parallel classes in $\mathcal{A}_i$. Notice that M_i is a $tq_i^{m_i-1}\times q_i^{m_i}$ matrix. The columns of H are indexed by $x=(x_1,\ldots,x_l)\in\prod_{i=1}^{l}\mathbb{F}_{q_i^{m_i}}$, the rows of H are indexed by $(y,z)=((y_1,\ldots,y_l),z)\in(\prod_{i=1}^{l}\mathbb{F}_{q_i^{m_i-1}})\times[t]$, in which $z\in[t]$ denotes the zth parallel class. The rows of M_i are indexed by $(y_i,z)\in\mathbb{F}_{q_i^{m_i-1}}\times[t]$, the columns of M_i are indexed by $x_i\in\mathbb{F}_{q_i^{m_i}}$, where $z\in[t]$ denotes the zth parallel class. The entries in M_i are denoted by $m_i((y_i,z),x_i)$. The entries $h_{(y,z),x}$ in H are defined as follows:

$$h_{(y,z),x}=\begin{cases}1, & \text{for all } i\in[1,l],\ m_i((y_i,z),x_i)=1,\\ 0, & \text{otherwise.}\end{cases} \tag{11}$$

The weight of each row in H is $\prod_{i=1}^{l}q_i=r+1$. Since we chose t parallel classes from each $\mathcal{A}_i$, the weight of each column in H is t. Fix a coordinate x. We will show that the t recovering sets of x are disjoint. Assume that x' appears in two recovering sets of x. Then, the four entries $h_{(y,z),x}$, $h_{(y,z),x'}$, $h_{(y',z'),x}$, $h_{(y',z'),x'}$ in H are all 1. Note that from our construction of H, $h_{(y,z),x}=1$ only when $\forall i\in[1,l],\ m_i((y_i,z),x_i)=1$. Assume that x and x' are different at the ith coordinate. Then, the four entries $m_i((y_i,z),x_i)$, $m_i((y_i,z),x_i')$, $m_i((y_i',z'),x_i)$, $m_i((y_i',z'),x_i')$ in M_i are all 1. This contradicts with the fact that M_i is composed of t parallel classes from $\mathcal{A}_i$. So for each coordinate x, the t recovering sets are disjoint.

The minimum distance d of our construction comes from the availability t, $d\geqslant t+1$. There are t parallel classes in our parity-check matrix H. For each choice of two sub-matrices H_i, H_j composed of two parallel classes from H, we can get one redundant row. Each parallel class is a partition of n elements into subsets of size $r+1$. If the values of all the parity-check equations associated with H_i, H_j are determined except one parity-check equation, then the value of the undetermined parity-check equation can be deduced from the other equations related to H_i, H_j, which means this row in H associated with the undetermined parity-check equation can be represented by the other rows in H_i, H_j. If we fix one parallel class in H, then for each remaining parallel class in H, we can get one redundant row. Therefore, there are at least $t-1$ redundant rows in H. The row rank of H is at most $t\cdot\prod_{i=1}^{l}q_i^{m_i-1}-(t-1)$. $\mathcal{R}$

is the code rate:

$$\mathcal{R} = 1 - \frac{\mathrm{rank}(H)}{n} \geqslant 1 - \frac{t \cdot \prod_{i=1}^{l} q_i^{m_i - 1} - (t-1)}{n} = 1 - \frac{t \cdot \prod_{i=1}^{l} q_i^{m_i - 1}}{\prod_{i=1}^{l} q_i^{m_i}} + \frac{t-1}{n} = 1 - \frac{t}{r+1} + \frac{t-1}{n}. \quad (12)$$

This completes the proof.

Remark 1. The codes in [13] are contained in our construction. Notice that the square code in [8] is a subcode of our code when $t \geqslant 2$ and $n = (r+1)^2$. In this case, the minimum distance of our construction attains the bound (2) when $n = (r+1)^2$, $t = 2$, $k \in [r+1, 2r-1]$ and $q > \binom{n}{k+1}$ [13]. The minimum distance of our construction outperforms the bound (3) when $n = (r+1)^2$, $t = 2$, $k \in [2r, r^2]$ and $q > \binom{n}{k+1}$. For the general case when $n = (r+1)^2$, $q > \binom{n}{k+e+1}$ and $t \in [2, r]$, the minimum distance of our construction is at least $n - k - e$ when $k \in [r+1-e, 2r-1-e]$, in which $e = (r+1)(t-2)$, and when $n = (r+1)^2$, $q > \binom{n}{k+e+1}$, $t \in [2, r]$ and $k \in [2r-e, r^2-e]$, the minimum distance of our construction is at least $n - k - e - \lceil \frac{2(k+e)}{r} \rceil + 3$ [13].

Theorem 3. For each $(\hat{v}, \hat{b}, \hat{r}, \hat{k}, 1)$-BIBD, we can construct an $(n = \hat{b}, k, r = \hat{r} - 1, t = \hat{k})_q$ SA-LRC, in which $q \geqslant 2$ is a prime power. Let d be the minimum distance of our code and $\mathcal{R}$ be the code rate of our code. Then $d \geqslant t + 1$ and $\mathcal{R} \geqslant 1 - \frac{t}{r+1}$. Moreover, code length n of this construction attains the bound (6).

Proof. Assume that M is the incidence matrix of a $(\hat{v}, \hat{b}, \hat{r}, \hat{k}, 1)$-BIBD $(X, \mathcal{B})$. We give a construction based on M^{T}. In $H = M^{\mathrm{T}}$, the rows are indexed by points, and the columns are indexed by blocks. The row weight of each row in H is $\hat{r}$, the column weight of each column in H is $\hat{k}$. Since every pair of distinct points appears in one block, the supports of rows in H containing the same coordinate i intersect only at i. If the supports of rows in H containing the same coordinate i intersect more than once, then there exist two points in X, such that these two points appear in two blocks. This contradicts with the properties of $(\hat{v}, \hat{b}, \hat{r}, \hat{k}, 1)$-BIBD.

If we take H as the parity-check matrix of an LRC, then each code symbol has $t = \hat{k}$ disjoint recovering sets of size $r = \hat{r} - 1$. Therefore, given a $(\hat{v}, \hat{b}, \hat{r}, \hat{k}, 1)$-BIBD, we can construct an $(n = \hat{b}, k, r = \hat{r} - 1, t = \hat{k})_q$ SA-LRC, denoted by $\mathcal{C}$. The minimum distance $d \geqslant t + 1$ comes from the availability t. $\mathcal{R}$ is the code rate:

$$\mathcal{R} = 1 - \frac{\mathrm{rank}(H)}{n} \geqslant 1 - \frac{\hat{v}}{\hat{b}} = 1 - \frac{\hat{k}}{\hat{r}} = 1 - \frac{t}{r+1}. \quad (13)$$

This construction contains the code constructed in [14]. Minimum block length of (n, k, r, t) SA-LRCs is $(r+1)^2 - \frac{(r+1)r}{t}$. In this construction, $n = \hat{b}$ and

$$(r+1)^2 - \frac{(r+1)r}{t} = \hat{r}^2 - \frac{\hat{r}(\hat{r}-1)}{\hat{k}} = \frac{\hat{k}\hat{r}^2 - \hat{r}(\hat{r}-1)}{\hat{k}} = \frac{\hat{r}}{\hat{k}} \cdot (\hat{k}\hat{r} - \hat{r} + 1) \quad (14)$$

$$= \frac{\hat{r}}{\hat{k}} \cdot \left(\hat{k} \frac{\hat{v}-1}{\hat{k}-1} - \frac{\hat{v}-1}{\hat{k}-1} + 1 \right) = \frac{\hat{r}\hat{v}}{\hat{k}} = \hat{b}. \quad (15)$$

So the block length of $\mathcal{C}$ attains the bound (6). This completes the proof.

Remark 2. Notice that although there are some constraints on the second construction, it provides some parameters that are impossible from the first construction. For example, we want to construct $(36, k, 5, t \leqslant 3)_q$ SA-LRCs. Since there is no $(36, 6, 1)$-BIBD [18], we cannot construct $(36, k, 5, t \leqslant 3)_q$ SA-LRCs from the first construction. Meanwhile, from the second construction, we can get $(36, k, 5, t \leqslant 3)_q$ SA-LRCs. Given an RBIBD, we can give several codes from the other two constructions in this section. For instance, given a $(9, 3, 1)$-RBIBD, we can get $(9, k, 2, t \leqslant 3)_q$ SA-LRCs from the first construction and a $(12, k, 3, 3)_q$ SA-LRC from the third construction.

Example 1. H_1^{T} is the incident matrix of a $(4, 2, 1)$-RBIBD. H_1 is a parity-check matrix of a $(6, 3, 2, 2)_q$ SA-LRC. Assume that M is the incidence matrix of a $(9, 3, 1)$-RBIBD. H_2 comes from M by deleting the last 3 rows in M. H_2 is a parity-check matrix of a $(9, k, 2, 3)_q$ SA-LRC $\mathcal{C}$. However, H_2 is not full rank. $c = \{c_0, \ldots, c_8\}$ denotes a codeword in $\mathcal{C}$. Each row in H_2 is related to a parity-check equation.

For example, the second row in H_2 denotes the equation $c_2 + c_6 + c_8 = 0$. If we fix the first three rows (the first parallel class) in H_2, then from the rest parallel classes, we can get 2 redundant rows in H_2. In another word, for each pair of parallel classes in H_2, there exists a redundant row, which can be represented by all the other rows in these two parallel classes. H_3 comes from H_2 by deleting the forth and seventh rows. We denote the vector representing the ith row in H_2 as R_i. $R_4 = (\sum_{i=1}^{3} R_i) - R_5 - R_6$, $R_7 = (\sum_{i=1}^{3} R_i) - R_8 - R_9$. Note that H_3 is also a parity-check matrix of $\mathcal{C}$.

$$H_1 = \begin{pmatrix} 1&1&1&0&0&0 \\ 1&0&0&1&1&0 \\ 0&1&0&1&0&1 \\ 0&0&1&0&1&1 \end{pmatrix}, \quad H_2 = \begin{pmatrix} 1&1&0&0&0&1&0&0&0 \\ 0&0&1&0&0&0&1&1&0 \\ 0&0&0&1&1&0&0&0&1 \\ 1&0&1&0&1&0&0&0&0 \\ 0&1&0&0&0&0&1&0&1 \\ 0&0&0&1&0&1&0&1&0 \\ 1&0&0&1&0&0&1&0&0 \\ 0&1&0&0&1&0&0&1&0 \\ 0&0&1&0&0&1&0&0&1 \end{pmatrix}, \quad H_3 = \begin{pmatrix} 1&1&0&0&0&1&0&0&0 \\ 0&0&1&0&0&0&1&1&0 \\ 0&0&0&1&1&0&0&0&1 \\ 0&1&0&0&0&0&1&0&1 \\ 0&0&0&1&0&1&0&1&0 \\ 0&1&0&0&1&0&0&1&0 \\ 0&0&1&0&0&1&0&0&1 \end{pmatrix}. \tag{16}$$

4 Distance-optimal LRCs with information-symbol locality from BIBD

First, we introduce the notation of the membership matrix [9,10]. A membership matrix R is an $m \times k$ matrix over $\mathbb{F}_2$, in which m is the number of different local groups $\Gamma_j(i) \cup \{i\}$. R denotes the information symbols in these distinct local groups. The entries r_{ij} in R are defined as follows:

$$r_{ij} = \begin{cases} 1, & \text{the } j\text{-th symbol participates in the } i\text{-th local group,} \\ 0, & \text{otherwise.} \end{cases} \tag{17}$$

In [9], the author provided a construction of distance-optimal $(n, k, r, t)_q$ LRCs with information-symbol locality from RBIBD. This code was constructed from a membership matrix R and an $(N+t, k)_q$ MDS code. However, the construction in [9] requires $r|k$. In this section, we will give a construction of $(n, k, r, t)_2$ IS-LRCs with (r, t)-availability whether $r|k$ or $r \nmid k$. The construction in [9] requires that R is a $\frac{kt}{r} \times k$ matrix, each row in R has weight r, each column in R has weight t, and the supports of rows in R gives t partitions of k.

In our construction, we only require that R is an incidence matrix of a $(k, \frac{kt}{r}, t, r, 1)$-BIBD, in which $r|kt$. R is our $\frac{kt}{r} \times k$ membership matrix, in which the weight of each row is r and the weight of each column is t. Our construction is based on a generator matrix G:

$$G = \left(I_{k\times k} \,|\, R^{\mathrm{T}}\right). \tag{18}$$

We will show that the LRC with G as its generator matrix is an IS-LRC with (r, t)-availability, its distance attains the bound (3), its code rate attains the bound (5) when $t = 2$.

Theorem 4. The code with generator matrix G is an $(n = k + \frac{kt}{r}, k, r, t)_2$ IS-LRC with (r, t)-availability, and its minimum distance attains the bound (3). The code rate of our code is $\frac{k}{n} = \frac{r}{r+t}$. When $t = 2$, the code rate of our construction attains the bound (5).

Proof. Since R is an incidence matrix of a $(k, \frac{kt}{r}, t, r, 1)$-BIBD, any two rows in R intersect at most once. Since the weight of each row in R is r and the weight of each column in R is t, each information symbol in our code is protected by t disjoint recovering sets of size r. Therefore, our code with generator matrix G is an $(n, k, r, t)_2$ IS-LRC with (r, t)-availability.

Next, we will show that the minimum distance of our code attains the bound (3). Consider the parity-check matrix H of our code:

$$H = \left(-R \,\middle|\, I_{\frac{kt}{r}\times\frac{kt}{r}}\right) = \left(R \,\middle|\, I_{\frac{kt}{r}\times\frac{kt}{r}}\right). \tag{19}$$

This is because our code is constructed over $\mathbb{F}_2$.

Let c be a codeword from our code with minimum distance d. Let c_i be the ith non-zero code symbol in c. First, assume that c_i is in the last $\frac{kt}{r}$ coordinates of c. In this case, there exists a nonzero c_j in the first k coordinates of c. Since R is an incidence matrix of a $(k, \frac{kt}{r}, t, r, 1)$-BIBD, c_j participates in t parity-check equations. For each of these t equations, there will be another non-zero c_h. Notice that these t equations are disjoint in H. Thus, there are at least $t+1$ non-zero coordinates in c.

Then, we assume that c_i is in the first k coordinates of c. Similarly, c_i participates in t parity-check equations. For each of these t equations, there will be another non-zero c_j. Note that these t equations are disjoint in H. Thus, there are at least $t+1$ non-zero coordinates in c. Therefore, the minimum distance d of our code is lower bounded by $t+1$.

Next we will show that our construction is distance-optimal. We know that in an LRC, when each recovering set contains only one parity symbol:

$$d \leqslant n - k - \left\lceil \frac{kt}{r} \right\rceil + t + 1. \tag{20}$$

In our code, each recovering set contains only one parity symbol. So the minimum distance d of our construction satisfies:

$$d \leqslant n - k - \left\lceil \frac{kt}{r} \right\rceil + t + 1 = k + \frac{kt}{r} - k - \left\lceil \frac{kt}{r} \right\rceil + t + 1 = t + 1. \tag{21}$$

In this case, our construction is distance-optimal. The code rate of our construction is $\frac{k}{k+\frac{kt}{r}} = \frac{r}{r+t}$. Since IS-LRC with (r,t)-availability is a special case of LRC with sequential repair property, the bound (5) can be applied to our code. When $t=2$, the code rate of our code attains the bound (5), so our construction is rate-optimal when $t=2$. This completes the proof.

Remark 3. We can also choose t parallel classes from a $(k, r, 1)$-RBIBD, and then construct a membership matrix R containing t parallel classes from this RBIBD. In this case, R is also a $\frac{kt}{r} \times k$ matrix, in which $r|kt$. However, in this case, we can choose any $1 \leqslant t \leqslant \frac{k-1}{r-1}$. We get a construction of $(n = k + \frac{kt}{r}, k, r, 1 \leqslant t \leqslant \frac{k-1}{r-1})_2$ IS-LRCs with (r,t)-availability from a $(k, r, 1)$-RBIBD.

Remark 4. Assume that M is the incidence matrix of a BIBD. We can also choose $R = M^{\mathrm{T}}$. Similar to the above proof, given a $(\frac{kt}{r}, k, r, t, 1)$-BIBD, in which $r|kt$, we can give a construction of $(n = k + \frac{kt}{r}, k, r, t)_2$ IS-LRC with (r,t)-availability. In this case, R is also a parity-check matrix of an $(n' = k, k', r' = r-1, t' = t)_2$ SA-LRC.

$$(r'+1)^2 - \frac{(r'+1)r'}{t'} = r^2 - \frac{r(r-1)}{t} = \frac{r^2 t - r(r-1)}{t} = \frac{r}{t}(rt - r + 1) \tag{22}$$

$$= \frac{r}{t}\left(t\frac{\frac{kt}{r}-1}{t-1} - \frac{\frac{kt}{r}-1}{t-1} + 1 \right) = k = n'. \tag{23}$$

The block length of the $(n' = k, k', r' = r-1, t' = t)_2$ SA-LRC attains the bound (6). Then, for a pair of fixed r and t, our $(k + \frac{kt}{r}, k, r, t)_2$ IS-LRC with (r,t)-availability has the minimum possible k. In other words, this construction could give larger t for a given pair k and r compared to other constructions.

Remark 5. Given an incidence matrix M of a $(\hat{v}, t, 1)$-RBIBD, we can also choose r parallel classes from M^{T} to form R. Then, we get a construction of $(n = k + \frac{kt}{r} = k + \hat{v}, k = r\frac{\hat{v}}{t}, 1 \leqslant r \leqslant \frac{\hat{v}-1}{t-1}, t)_2$ IS-LRCs with (r,t)-availability, in which $r|kt$.

Remark 6. Notice that when the chosen BIBD is symmetric, the first and third constructions are the same. For example, if we choose a $(q^2+q+1, q+1, 1)$-SBIBD, in which q is a prime power, we can get a $(2k, k = q^2+q+1, r = q+1, t = r)_2$ IS-LRC with (r,t)-availability. If in the second construction of this kind we choose a $(q^2, q, 1)$-RBIBD, we can get $(q^2 + sq, q^2, q, s \leqslant q)_2$ IS-LRCs with (q,s)-availability. These constructions contain codes proposed in [11]. Note that all the constructions in this section are distance-optimal. When $t=2$, all the codes constructed in this section are rate-optimal. If we choose

a $(k, r, 1)$-BIBD in which $r \nmid k$ in our first construction of this type, we can get an IS-LRC with (r, t)-availability when $r \nmid k$, while in the constructions in [9], $r|k$ is necessary. Moreover, all the codes constructed in this section are over binary field, which are especially practical for system implementation compared with the codes in [9].

Remark 7. An $m \times n$ matrix M is a (τ, ρ)-regular matrix with girth > 4 (no cycle of length $\leqslant 4$), if the weight of each column in M is τ, the weight of each row in M is ρ and the supports of any two rows of M intersect at most once. Notice that any parity-check matrix of (n', k', r', t') SA-LRC is a $(t', r'+1)$-regular matrix with girth > 4. Similar to the proof process in Theorem 4, we can also prove that any (τ, ρ)-regular $m \times n$ matrix M with girth > 4 can substitute the membership matrix R to obtain a distance-optimal $(n' = k' + \frac{k't'}{r'}, k' = n, r' = \rho, t' = \tau)$ LRC with information-symbol locality and $d = t' + 1$.

For a given BIBD, we could give several constructions of distance-optimal LRCs with information-symbol locality and some constructions of SA-LRCs. Therefore, our constructions have a large range of parameters. Thus, depending on the circumstances, we could choose different BIBDs in our constructions to meet the different requirements of the parameters. Notice that most of the codes constructed in this paper (all codes in Sections 3–5) are over binary field, which are especially practical for system implementation. We give several examples to illustrate that the parameters of codes obtained in this paper are better than other codes.

For a given pair of r and t, our constructions in this section have relatively smaller k. For example, the block length of the code proposed by Wang, Zhang and Liu (WZL code for short) in [19] is $\binom{r'+t'}{t'}$ for a pair of given r' and t'. We denote the distance-optimal LRC with information-symbol locality from WZL code as WZL-ISLRC. The dimension k of WZL-ISLRC is $\binom{r'+t'}{t'} = \binom{r+t-1}{t}$. At the same time, in our first construction in this section, $k = t(r-1)+1$. Especially, in our third construction in this section, $k = r^2 - \frac{r(r-1)}{t}$, which is the minimum possible k for a pair of given r, t. Compared to WZL-ISLRC, our code has smaller dimension k for a pair of given r and t. In other words, our construction should have larger t for a given pair k and r, which means the codes constructed in this section have higher reliability and better availability compared to WZL-ISLRC. Moreover, compared to WZL-ISLRC, our codes in this section are more suitable for small-scale distributed storage systems and hot data warehousing.

Our constructions in this section are more flexible compared to some distance-optimal LRCs with information-locality from SA-LRCs with short block lengths. For example, the block length of $(n' = 2^{2m} - 1, k' = 2^{2m} - 3^m, r' = 2^m - 1, t' = 2^m)$ SA-LRC from Euclidean geometries in [20] is shorter than the block length of the WZL code for a given pair r' and t'. The block lengths of the $(n' = Q^2 + Q + 1$, $k' = Q^2 + Q - 3^s$, $r' = Q$, $t' = Q + 1)$ SA-LRC and $(n' = Q^2 + Q$, $k' = Q^2 + Q - 3^s$, $r' = Q$, $t' = Q)$ SA-LRC in [14] attain the bound (6), in which $Q = 2^s$, $s \geqslant 2$. If we substitute R with the parity-check matrices of the above SA-LRCs, then in the LRCs with information-symbol locality, $r - 1 = t$ or $r = t$. At the same time, in our second construction in this section, t could be any integer less than or equal to $\frac{k-1}{r-1}$, and in the forth construction in this section, r could be any integer less than or equal to $\frac{\hat{v}-1}{t-1}$. Our constructions could give more choices of parameters compared to the above codes, which means our codes in this section are more flexible and more widely applicable.

For a given pair r and t, the block lengths of our constructions in Section 3 could be shorter than the WZL code in [19], which means that our codes in Section 3 are more suitable for small-scale distributed storage systems and hot data warehousing. The $(n' = 2^{2m} - 1$, $k' = 2^{2m} - 3^m$, $r' = 2^m - 1$, $t' = 2^m)$ SA-LRC from Euclidean geometries in [20], the $(n' = Q^2 + Q + 1$, $k' = Q^2 + Q - 3^s$, $r' = Q$, $t' = Q + 1)$ SA-LRC and $(n' = Q^2 + Q$, $k' = Q^2 + Q - 3^s$, $r' = Q$, $t' = Q)$ SA-LRC in [14] have shorter block lengths compared to the WZL code in [19]. Notice that in these SA-LRCs $r = t$ or $r + 1 = t$. Our codes in Sections 3 and 5 could give more choices of parameters compared to the above codes, which means our codes in Sections 3 and 5 are more flexible and more widely applicable.

Example 2. Although it seems that the four constructions in this section have the same block lengths, the constraints on them are different. The first construction gives a fixed code for given k, r. The second construction gives a series of codes for fixed k, r. The third construction gives a fixed code for

given $\frac{kt}{r}$, t. The fourth construction gives a series of codes for fixed $\hat{v}$, t. For example, given a $(4,2,1)$-BIBD, the first construction gives a $(10,4,2,3)_2$ IS-LRC with $(2,3)$-availability, the second construction gives $(4+2t,4,2,1\leqslant t\leqslant 3)_2$ IS-LRCs with $(2,t)$-availability, the third construction gives a $(10,6,3,2)_2$ IS-LRC with $(3,2)$-availability, the forth construction gives $(4+2r,2r,1\leqslant r\leqslant 3,2)_2$ IS-LRCs with $(r,2)$-availability. G_1 is the generator matrix of a $(10,4,2,3)_2$ IS-LRC with $(2,3)$-availability. G_2 is the generator matrix of an $(8,4,2,2)_2$ IS-LRC with $(2,2)$-availability. G_3 is the generator matrix of a $(10,6,3,2)_2$ IS-LRC with $(3,2)$-availability. G_4 is the generator matrix of an $(8,4,2,2)_2$ IS-LRC with $(2,2)$-availability.

$$G_1=\begin{pmatrix}1&0&0&0&1&1&1&0&0&0\\0&1&0&0&1&0&0&1&1&0\\0&0&1&0&0&1&0&1&0&1\\0&0&0&1&0&0&1&0&1&1\end{pmatrix},\quad G_2=\begin{pmatrix}1&0&0&0&1&1&0&0\\0&1&0&0&1&0&1&0\\0&0&1&0&0&1&0&1\\0&0&0&1&0&0&1&1\end{pmatrix},\tag{24}$$

$$G_3=\begin{pmatrix}1&0&0&0&0&0&1&1&0&0\\0&1&0&0&0&0&1&0&1&0\\0&0&1&0&0&0&1&0&0&1\\0&0&0&1&0&0&0&1&1&0\\0&0&0&0&1&0&0&1&0&1\\0&0&0&0&0&1&0&0&1&1\end{pmatrix},\quad G_4=\begin{pmatrix}1&0&0&0&1&0&1&0\\0&1&0&0&1&0&0&1\\0&0&1&0&0&1&1&0\\0&0&0&1&0&1&0&1\end{pmatrix}.\tag{25}$$

5 SA-LRCs from MOLS

In this section, we provide a construction of SA-LRCs from MOLS. Our code is based on s MOLS of order $(r+1)$. $\Omega=\{1,\ldots,(r+1)^2\}$ is a set of $(r+1)^2$ elements (points). If we arrange the elements of Ω in an $(r+1)\times(r+1)$ array A, then s MOLS $\{L_1,\ldots,L_s\}$ of order $r+1$ give $s+2$ partitions of Ω into $r+1$ blocks of size $r+1$, i.e., $s+2$ parallel classes. These parallel classes are partition of rows P^{row}, partition of columns P^{col}, and partitions of numbers from L_i ($i\in[s]$), i.e., the entries numbered $1,\ldots,r+1$ in L_i, denoted as P^{L_i}. Every pair of distinct blocks from different parallel classes in $\{P^{\text{row}},P^{\text{col}},P^{L_1},\ldots,P^{L_s}\}$ intersects exactly once [21].

Each block from P^{row} and each block from P^{col} intersect at one point. Next, we consider a pair of distinct blocks from P^{L_a} and P^{L_b}, in which $a,b\in[s]$. Since these two blocks are from a pair of orthogonal Latin squares, they intersect once. Assume that these two blocks are from number i and j. If these two blocks intersect at least twice, then the (i,j) pair appears at least twice. This contradicts with the fact that these two Latin squares are orthogonal. Next, we consider a block from P^{row} and a block from P^i. Since L_i is a Latin square, these two blocks intersect at one point. Assume that these two blocks intersect more than once. Then, there will be at least two same elements in L_i in the same row. This contradicts with the fact that L_i is a Latin square. Therefore, a block from P^{row} and a block from any P^{L_i} intersect exactly once. Similarly, a block from P^{col} and a block from any P^{L_i} intersect exactly once.

We construct a matrix H from these $s+2$ parallel classes. H is a $t(r+1)\times(r+1)^2$ matrix, in which $1\leqslant t\leqslant s+2$. We choose t parallel classes $P'_1,\ldots,P'_t$ from $\{P^{\text{row}},P^{\text{col}},P^{L_1},\ldots,P^{L_s}\}$. $B_1,\ldots,B_{t(r+1)}$ denotes the blocks in these t parallel classes. The columns of H are indexed by the $(r+1)^2$ points, the rows of H are indexed by the blocks. The entries h_{ij} in H are defined as follows:

$$h_{ij}=\begin{cases}1, & \text{point } j \text{ is contained in } B_i,\\ 0, & \text{otherwise.}\end{cases}\tag{26}$$

We will prove that H is the parity-check matrix of an $(n=(r+1)^2,k,r,t\leqslant s+2)_2$ SA-LRC.

Theorem 5. *H is the parity-check matrix of an $(n=(r+1)^2,k,r,t\leqslant s+2)_2$ SA-LRC. The minimum distance of this code is at least $t+1$ and the code rate of this code is at least $1-\frac{t}{r+1}+\frac{t-1}{n}$.*

Proof. From the above construction, we can conclude that the weight of each row in H is $r+1$, the weight of each column in H is t. Therefore, each code symbol has t recovering sets of size r. Since each pair of blocks from different parallel classes intersects at one point, these t recovering sets are disjoint. Therefore, the code with the parity-check matrix H is an $(n=(r+1)^2, k, r, t \leqslant s+2)_2$ SA-LRC. The minimum distance $d \geqslant t+1$ comes from the availability t.

For each choice of two sub-matrices H_i, H_j composed of two parallel classes from H, we can get one redundant row. Each parallel class is a partition of n elements into subsets of size $r+1$. If the values of all the parity-check equations associated with H_i, H_j are determined except one parity-check equation, then the value of the undetermined parity-check equation can be deduced from the other equations related to H_i, H_j, which means this row in H associated with the undetermined parity-check equation can be represented by the other rows in H_i, H_j. If we fix one parallel class in H, then for each remaining parallel class we can get one redundant row. Therefore, the rank of H is at most $t(r+1)-(t-1)$. $\mathcal{R}$ denotes the code rate:

$$\mathcal{R}=1-\frac{\mathrm{rank}(H)}{n}\geqslant\frac{n-(t(r+1)-(t-1))}{n}=1-\frac{t(r+1)}{(r+1)^2}+\frac{t-1}{n}=1-\frac{t}{r+1}+\frac{t-1}{n}. \tag{27}$$

This completes the proof.

Remark 8. This construction could give some SA-LRCs with parameters that are impossible from BIBDs. For instance, there is no finite affine plane of order 6 [18]. Therefore, there is no $(36,6,1)$-BIBD. However, we can construct a $(36,k,5,1\leqslant t\leqslant 3)_2$ SA-LRC from a Latin square of order 6. Notice that we can replace the membership matrix R in Section 4 by H. Then, we can get a distance-optimal $(n=k+\frac{kt}{r}, k=r^2, r, t\leqslant s+2)_2$ IS-LRC with (r,t)-availability from s MOLS of order r, and when $t=2$ this construction is also rate-optimal.

Example 3. H_L is a parity-check matrix of a $(9,k,2,3)_2$ SA-LRC from a Latin square of order 3. We denote the vector representing the ith row from H_L as R_i. $R_4=(\sum_{i=1}^{3}R_i)-R_5-R_6$ and $R_7=(\sum_{i=1}^{3}R_i)-R_8-R_9$. Therefore, $\mathrm{rank}(H_L)\leqslant 9-2=7$.

$$H_L=\begin{pmatrix}1&1&1&0&0&0&0&0&0\\0&0&0&1&1&1&0&0&0\\0&0&0&0&0&0&1&1&1\\1&0&0&1&0&0&1&0&0\\0&1&0&0&1&0&0&1&0\\0&0&1&0&0&1&0&0&1\\1&0&0&0&0&1&0&1&0\\0&1&0&1&0&0&0&0&1\\0&0&1&0&1&0&1&0&0\end{pmatrix}. \tag{28}$$

6 Optimal LRCs with information-symbol locality from MOLS

In this section, we provide a construction of distance-optimal $(n,k,r,t)_q$ LRCs with information-symbol locality from MOLS. $\Omega=\{1,\ldots,r^2\}$ is a set of r^2 points. We arrange the elements of Ω in an $r\times r$ array B. $\{L_1,\ldots,L_s\}$ is a set of s MOLS of order r. Then $\{L_1,\ldots,L_s\}$ give $s+2$ partitions of Ω into r blocks of size r, i.e., $s+2$ parallel classes. These parallel classes are partition of rows P^{row}, partition of columns P^{col}, and partitions of numbers from L_i $(i\in[s])$, i.e., the entries numbered $1,\ldots,r$ in L_i, denoted as P^{L_i}. Every pair of distinct blocks from different parallel classes in $\{P^{\mathrm{row}},P^{\mathrm{col}},P^{L_1},\ldots,P^{L_s}\}$ intersects exactly once. Then, we construct a membership matrix R from these $s+2$ parallel classes. R is a $\frac{kt}{r}\times k=tr\times r^2$ matrix, where $1\leqslant t\leqslant s+2$ and $k=r^2$. We choose t parallel classes $P'_1,\ldots,P'_t$ from $\{P^{\mathrm{row}},P^{\mathrm{col}},P^{L_1},\ldots,P^{L_s}\}$. $B_1,\ldots,B_{tr}$ denotes the blocks in the t parallel classes. The columns of

R are indexed by the r^2 points, the rows of R are indexed by the blocks. The entries r_{ij} in R are defined as follows:

$$r_{ij} = \begin{cases} 1, & \text{point } j \text{ is contained in } B_i, \\ 0, & \text{otherwise.} \end{cases} \tag{29}$$

Then, we get a membership matrix R. The weight of each row in R is r, the weight of each column in R is t. Our construction is based on a generator matrix $\hat{G}$ of an $(N+t, k=r^2)_q$ MDS code $\hat{\mathcal{C}}$ and the membership matrix R.

$$\hat{G} = \big(I_{k\times k} \,|\, p_1 \ \ldots \ p_{N-k} \,|\, p_{N-k+1} \ \ldots \ p_{N-k+t}\big). \tag{30}$$

The rows of R give t partitions of $k=r^2$ points into blocks of size r. The first N columns in the generator matrix G of our construction are the same as $\hat{G}$. We partition the last t columns in $\hat{G}$ according to the parallel classes $P'_1, \ldots, P'_t$. Each parallel class is associated with $\frac{k}{r} = r$ columns in G. These columns are local parities for information symbols. Then, we get a $k \times (N + \frac{kt}{r})$ matrix G. Next we will show that G is the generator matrix of an $(n = N + \frac{kt}{r} = N + tr, k = r^2, r, t \leqslant s+2)_q$ IS-LRC with (r,t)-availability.

Theorem 6. *G is the generator matrix of an $(n = N + \frac{kt}{r} = N + tr, k = r^2, r, t \leqslant s+2)_q$ LRC $\mathcal{C}$ with information-symbol locality and (r,t)-availability. The minimum distance of $\mathcal{C}$ attains the bound (3).*

Proof. Notice that in R, any two rows intersect at most once, and the weight of each row in R is r, the weight of each column in R is t. Therefore, each information symbol in $\mathcal{C}$ is protected by t disjoint recovering sets of size r. So our code $\mathcal{C}$ with generator matrix G is an $(n,k,r,t)_q$ IS-LRC with (r,t)-availability. In our code, any local repair group contains only one parity symbol. We will show that our code can correct any $n-k-\lceil\frac{kt}{r}\rceil+t = N-k+t$ erasures. In this case, the minimum distance of $\mathcal{C}$ attains the bound (3).

We order the elements of codeword in $\mathcal{C}$ from 1 to n. $\mathcal{I}$ denotes the coordinates of the information symbols. $\mathcal{P}^{\text{gbl}}$ denotes the coordinates of the global parities, i.e., the indices of $\{p_1, \ldots, p_{N-k}\}$. $\mathcal{P}^i$ denotes the coordinates of the local parities constructed from p_{N-k+i}. $\mathcal{P}^l = \cup_{i=1}^t \mathcal{P}^i$ denotes the indices of local parities in G.

First, assume that there are at most $N-k$ erasures in the set of code symbols indexed by $\mathcal{I} \cup \mathcal{P}^{\text{gbl}}$. Note that $\mathcal{C}|_{\mathcal{I}\cup\mathcal{P}^{\text{gbl}}}$ is an $(N,k)_q$ MDS code. Then, these $N-k$ erasures can be repaired. The remaining erasures can be recovered from $\mathcal{C}|_{\mathcal{I}}$.

Next, assume that among these $N-k+t$ erasures, $N-k+x$ erasures are in the coordinates indexed by $\mathcal{I}\cup\mathcal{P}^{\text{gbl}}$, in which $0 < x \leqslant t$. Then, there are $t-x$ erasures in the coordinates indexed by $\mathcal{P}^l$. Assume that the worst case happens, these $t-x$ erasures appear in $t-x$ local parity groups in $\mathcal{P}^l$. We denote the undamaged parallel classes by $\{\mathcal{P}'^1, \ldots, \mathcal{P}'^x\}$. We can combine the local parities indexed by $\{\mathcal{P}'^1, \ldots, \mathcal{P}'^x\}$ together to get x parities in the code $\hat{\mathcal{C}}$ with generator matrix $\hat{G}$. Now we get $N-(N-k+x)+x = k$ symbols in a codeword from $\hat{\mathcal{C}}$. Notice that $\hat{\mathcal{C}}$ is an $(N+t,k)_q$ MDS code. Then all the $N-k+t$ erasures can be recovered. Minimum distance of our code is $N-k+t+1$, attains the bound (3). This completes the proof.

Remark 9. Assume that M is an incidence matrix of a $(7,3,1)$-SBIBD. In this construction, we can also choose $R = M$. Then, we get an $(N+7, 7, 3, 3)_q$ IS-LRC with $(3,3)$-availability. The minimum distance of the code is $N+4$, which means that this code is distance-optimal. We get an $(n,k,r,t)_q$ IS-LRC with (r,t)-availability when $r \nmid k$. The first construction in [9] gives $(N+\frac{kt}{r}, k, r, 1 \leqslant t \leqslant \frac{k-1}{r-1})_q$ IS-LRCs from a $(k,r,1)$-RBIBD and an $(N+t,k)_q$ MDS code. Notice that there is no $(36,6,1)$-BIBD. Therefore, we cannot get an $(n,36,6,t)_q$ IS-LRC from the first construction in [9]. Meanwhile, given a Latin square of order 6, we can give $(N+6t, 36, 6, t \leqslant 3)_q$ IS-LRCs with (r,t)-availability from the construction in this section.

Example 4. We choose a Latin square of order 2 and an $[8,4,5]_{11}$ Reed-Solomon code with generator matrix $\hat{G}$. The matrix R comes from a Latin square of order 2. Then, we partition the last 3 columns of $\hat{G}$ according to the rows of R to form the generator matrix G of an $(11,4,2,3)_{11}$ LRC with information-

symbol locality and $(2,3)$-availability.

$$\hat{G}=\begin{pmatrix}1&0&0&0&10&7&1&2\\0&1&0&0&4&4&3&4\\0&0&1&0&5&2&10&4\\0&0&0&1&4&10&9&2\end{pmatrix},\quad R=\begin{pmatrix}1&1&0&0\\0&0&1&1\\1&0&1&0\\0&1&0&1\\1&0&0&1\\0&1&1&0\end{pmatrix},\quad G=\begin{pmatrix}1&0&0&0&10&7&0&1&0&2&0\\0&1&0&0&4&4&0&0&3&0&4\\0&0&1&0&5&0&2&10&0&0&4\\0&0&0&1&4&0&10&0&9&2&0\end{pmatrix}. \tag{31}$$

7 Conclusion

In this paper, we proposed several constructions of LRCs. In Section 3, we provided three constructions of $(n,k,r,t)_q$ SA-LRCs from BIBDs. Then, we proposed four constructions of distance-optimal $(n,k,r,t)_2$ IS-LRCs with (r,t)-availability from BIBDs in Section 4. When the parameters of block designs are chosen properly, our codes do not require $r|k$, while in the first code in [9], $r|k$ is necessary. When $t=2$, the codes in Section 4 are rate-optimal. We proposed a construction of $(n,k,r,t)_2$ SA-LRCs from MOLS and a construction of distance-optimal $(n,k,r,t)_q$ IS-LRCs with (r,t)-availability from MOLS in Sections 5 and 6. From these two constructions, we can obtain some LRCs with parameters that are impossible from block designs.

In the future, we would work on the unsolved problems in this paper: (1) improving the code rate and minimum distance in our construction of SA-LRC; (2) improving the code rate of LRCs with (r,t)-availability and information-symbol locality in this paper; (3) constructing a rate-optimal LRC with (r,t)-availability and all-symbol locality.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61672166), Plan of Shanghai Excellent Academic Leaders (Grant No. 16XD1400200), Innovation Plan of Shanghai Science and Technology (Grant No. 16JC1402700) and Shanghai Leading Talent Programmes.

Supporting information Appendix A. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Balaji S B, Krishnan M N, Vajha M, et al. Erasure coding for distributed storage: an overview. Sci China Inf Sci, 2018, 61: 100301
2 Dimakis A G, Godfrey P B, Wu Y, et al. Network coding for distributed storage systems. IEEE Trans Inform Theory, 2010, 56: 4539–4551
3 Liang S T, Liang W J, Kan H B. Construction of one special minimum storage regenerating code when $\alpha=2$. Sci China Inf Sci, 2015, 58: 062308
4 Gopalan P, Huang C, Simitci H, et al. On the locality of codeword symbols. IEEE Trans Inform Theory, 2012, 58: 6925–6934
5 Jin L F, Ma L M, Xing C P. Construction of optimal locally repairable codes via automorphism groups of rational function fields. 2017. ArXiv:1710.09638
6 Jin L F. Explicit construction of optimal locally recoverable codes of distance 5 and 6 via binary constant weight codes. IEEE Trans Inform Theory, 2019, 65: 4658–4663
7 Prakash N, Kamath G M, Lalitha V, et al. Optimal linear codes with a local-error-correction property. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), Cambridge, 2012. 2776–2780
8 Wang A Y, Zhang Z F. Repair locality with multiple erasure tolerance. IEEE Trans Inform Theory, 2014, 60: 6979–6987
9 Rawat A S, Papailiopoulos D S, Dimakis A G, et al. Locality and availability in distributed storage. IEEE Trans Inform Theory, 2016, 62: 4481–4493
10 Su Y S. Design of membership matrices for (r,t)-availability in distributed storage. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), Barcelona, 2016. 998–1002
11 Hao J, Xia S T. Constructions of optimal binary locally repairable codes with multiple repair groups. IEEE Commun Lett, 2016, 20: 1060–1063

12 Balaji S B, Kumar P V. Bounds on the rate and minimum distance of codes with availability. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), Aachen, 2017. 3155–3159
13 Zhang Y, Kan H B. Locally repairable codes with strict availability from linear functions. Sci China Inf Sci, 2018, 61: 109304
14 Balaji S B, Prasanth K P, Kumar P V. Binary codes with locality for multiple erasures having short block length. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), Barcelona, 2016. 655–659
15 Tamo I, Barg A, Frolov A. Bounds on the parameters of locally recoverable codes. IEEE Trans Inform Theory, 2016, 62: 3070–3083
16 Prakash N, Lalitha V, Kumar P V. Codes with locality for two erasures. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), Honolulu, 2014. 1962–1966
17 Colbourn C J, Dinitz J H. Handbook of Combinatorial Designs. 2nd ed. Boca Raton: CRC Press, 2006
18 Wan Z X. Design Theory. Beijing: Higher Education Press, 2009
19 Wang A, Zhang Z, Liu M. Achieving arbitrary locality and availability in binary codes. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), Hong Kong, 2015. 1866–1870
20 Huang P, Yaakobi E, Uchikawa H, et al. Linear locally repairable codes with availability. In: Proceedings of IEEE International Symposium on Information Theory (ISIT), Hong Kong, 2015. 1871–1875
21 Olmez O, Ramamoorthy A. Repairable replication-based storage systems using resolvable designs. In: Proceedings of the 50th Annual Allerton Conference on Communication, Control, and Computing, Monticello, 2012. 1174–1181