文章编号:1671-4598(2026)05-0274-10 DOI:10.16526/j.cnki.11-4762/tp.2026.05.033 中图分类号:TP301 文献标识码:A

具有灵活容错能力的局部修复码构造

喻婷婷,马 妍,杨 琨
(长安大学 信息工程学院,西安 710018)

摘要:局部修复码(LRCs)能有效应对分布式存储系统中多节点故障的修复难题,针对现有局部修复码容错能力不灵活且码率较低的问题,提出一类基于循环置换矩阵构造局部修复码的方法;该方法采用循环置换矩阵构造校验矩阵,并由校验矩阵生成局部修复码,经验证,与现有的局部修复码相比,构造的码实现了最小距离最优和码长最优,同时具有更高的码率和更灵活的可用性参数选择,但其容错能力受可用性参数的限制;进一步,在上述局部修复码构造的基础上,通过对校验矩阵进行克罗内克积运算,提出了另一类局部修复码的构造方法,该类局部修复码实现了最小距离最优,并提高了系统容错能力的灵活性,可通过调整局部容错参数δ的取值实现灵活的容错能力,满足了分布式存储系统在可调容错能力上的应用需求。

关键词:分布式存储系统;局部修复码;循环置换矩阵;最小距离;码率;容错能力

Construction of LRCs with Flexible Fault Tolerance

YU Tingting, MA Yan, YANG Kun
(School of Information Engineering, Chang'an University, Xi'an 710018, China)

Abstract: Locally repairable codes (LRCs) are used to effectively solve the challenge of multi-node failure recovery in distributed storage systems (DSSs). To overcome the limitations of existing LRCs, such as inflexible fault tolerance and low code rates, a method for constructing the LRCs based on cyclic permutation matrices is proposed, which utilizes cyclic permutation matrices to construct a parity-check matrix, achieving the LRCs from the parity-check matrix. Experiments validate that, compared to existing LRCs, the constructed codes achieve optimal minimum distance and optimal code length while offering higher code rates and more flexible availability parameter choices. However, their fault tolerance capability is constrained by the availability parameters. Furthermore, based on the aforementioned construction of the LRCs, a construction method for another class of LRCs is proposed by applying the Kronecker column-wise product operation to the parity-check matrix. This class of LRCs achieves optimal minimum distance while enhancing the flexibility of the system fault tolerance. By adjusting the local fault tolerance parameter δ, the flexible fault tolerance can be achieved, meeting the application requirements of DSSs in terms of adjustable fault tolerance.

Keywords: DSSs; LRCs; circulant permutation matrices; minimum distance; code rate; fault tolerance

0 引言

在当前海量数据急剧增长的背景下,传统的数据存储方式已难以应对大规模数据的存储需求,分布式存储系统(DSSs,distributed storage systems)已逐步成为主要的针对海量数据的存储手段[1]。DSSs通过将数据分散存储在大量节点上,以实现高可靠性和高可用性。然而,节点故障在DSSs中常有发生。为了对抗节点故障导致的数据丢失,DSSs一般通过引入冗余的策略来实现数据的可靠性存储[2],其中最简单的方法是直接复制[3],但这需要保存多份数据副本,造成了较大的存储开销。为了减少存储开销,目前实际系统中常用的是纠删码[4-6],该编码将原始数据文件分割成k个数据块,通过线性编码生成冗余,有效降低了系统的存储开销,但在数据修复时需要访问相当于全部文件大小的数据量,造成了较大的修复带宽开销。针对这些问题,文献[7]将网络编码技术应用于分布式存储系统,提出了再生码策略,该方法让中间节点参与计算,从存活节点下载部分数据并直接再生出丢失数据,无需经历完整的解码再编码过程,再生码虽然平衡了存储成本和修复带宽

收稿日期:2025-09-25; **修回日期**:2025-11-07。
基金项目:国家自然科学基金(62001059);陕西省重点研发计划项目(2021GY-019)。
作者简介:喻婷婷(2001-),女,硕士研究生。
引用格式:喻婷婷,马 妍,杨 琨.具有灵活容错能力的局部修复码构造[J].计算机测量与控制,2026,34(5):274-283.

开销，但在修复过程带来了较高的磁盘 I/O 开销、且其编解码过程中涉及复杂矩阵运算和有限域操作，造成较高的计算延迟和 CPU 消耗。基于此，文献［8］中进一步提出具有修复局部性的局部修复码（LRCs，locally repairable codes），该编码方法仅需访问同一校验组内少量的其他节点即可完成丢失数据的修复，从而显著降低了磁盘 I/O 开销、修复带宽开销以及编解码复杂度。

分布式存储系统中常出现多个节点发生故障的问题，为了在多节点故障的情况下局部修复码仍然能维持其局部修复特性。文献［9］对 LRCs 进一步推广，提出了具有 (r,t)- 局部性的 LRCs（即 (r,t) -LRCs），每个信息符号都可以从其他大小为 r 的 t 个不相交修复组中恢复出来，文中推导并证明了线性或非线性 (r,t) -LRCs 的最小汉明距离的理论上限。文献［10］提出了所有符号具有 (r,t) -局部性的 LRCs 的码率上界和最小距离上界。进一步地，文献［11］在此基础上提出可用性等于 2 时，$(r,t=2)$ -LRCs 的码率理论上界和分块码长理论下界。在上述文献中提出的概念和推导的理论界限基础上，文献［12］基于线性函数族将二元域上的 (r,t) -LRCs 扩展到多元域，在可用性参数固定为 2 条件下，此构造实现了最小距离最优，然而系统容错能力受限于固定的可用性参数，难以灵活调整，且整体码率较低。文献［13］提出一种可顺序恢复的 2-seq LRCs，该码的码率实现最优，但其最小距离取固定值 3，导致系统容错能力受限，此外，有限域规模随着局部性增大而扩展，该特性限制了其在参数较大时的实际适用性。文献［14］基于射影平面 $PG(2,2^a)$ 构造了一类信息符号具有 (r,t) -局部性的 LRCs，又基于仿射平面中的特殊点与线构造了另一类信息符号具有 (r,t) -局部性 LRCs，两类构造方法得到的 LRCs 的码率均为 1/2，然而局部性参数和可用性参数取值相互关联，必须满足条件 $r=t$，受限的可用性参数取值导致系统容错能力缺乏灵活性，文中两类构造的码率均较低且参数限制较大。文献［15］利用校验多项式与有限域上迹函数的关系，构造了一类具有循环特性的 (r,t) -LRCs，此构造码具有高可用性且最小距离达到最优，但其码率因其高可用性带来较多的系统冗余而未达到最优码率界。上述具有多故障节点修复特性的 (r,t) -LRCs，其容忍多故障节点的个数均受到可用性参数 t 的限制。文献［16］提出了具有 (r,δ) -局部性的 LRCs（即 (r,δ) -LRCs），此类 LRCs 能容忍多个故障节点，但由于仅包含单个局部修复组，无法支持多故障节点的并行修复，且系统整体码率较低。文献［17］进一步提出了 (r,N,δ) -LRCs 的概念，并推导其最小距离理论边界，此类码能实现故障节点的并行修复，但存在码率不高和构造难度大的问题。文献［18］基于正则矩阵构造了信息符号具有 (r,δ,t) -局部性的 LRCs，推导并证明出其最小距离界，此类码支持并行修复，但其局部性参数和可用性参数取值相互制约，且存在参数取值不够灵活，整体码率较低的问题。

为了解决上述问题，构造出一类参数取值灵活、整体高码率、且最小距离最优的局部修复码。本文先基于循环置换矩阵提出了一类信息符号具有 (r,t) -局部性的局部修复码的构造方法。与现有 (r,t) -LRCs 相比，本文所构造的码在最小距离和码长达到最优的同时，还具有较高的码率和灵活的参数选择。进一步，在构造的 (r,t) -LRCs 的基础上，通过对校验矩阵进行克罗内克列积运算，构造一类信息符号具有 (r,δ,t) -局部性的 LRCs，构造的 (r,δ,t) -LRCs 的容错能力可随参数 δ,t 的变化而调整。当可用性一定，根据实际场景灵活地调整 δ 取值，在追求高码率的场景中，适当降低 δ 值以提高码率；在容错能力要求较高的场景中，则可适当增加 δ 值以增强容错。

1　基础知识

1.1　局部修复码

定义 1（(r,t)-LRCs）[9]：若一类局部修复码同时满足下列 3 个条件：

1）对于每一个信息（系统）符号 $c_i \in C, i \in [k]$，都存在有 t 个子集 $\varphi_1(i),\varphi_2(i),\cdots\varphi_t(i) \subset [n]/\{i\}$；

2）$|\varphi_j(i)| \leqslant r, i \in [k], j \in [t]$；

3）$\varphi_j(i) \cap \varphi_l(i) = \varphi, i \in [k], j \neq l \in [t]$。

式中，$\varphi_j(i)(j \in [t])$ 为码字符号 c_i 的修复集。我们称此类码为 (n,k,r,t) -LRCs。

具体来说，对于每个码字符号 $c_i \in C, i \in [k]$，存在 t 个修复集；每个修复集的大小至多为 r，修复时最多需要读取其他 r 个符号，保证修复局部性，只需要少量数据便可完成修复，具有较低的修复开销；任意两个不同的修复集 $\varphi_j(i)$ 和 $\varphi_l(i)$ 不相交，从而给故障的码字符号提供多种修复方式，如果一个修复集中某些校验符号发生故障不可用，仍能通过其他修复集来恢复故障的码字符号。

定理 1[19]：若一类 LRCs 具有 (r,t) -局部性，则其最小距离需满足下面公式：

$$d \geqslant t+1 \tag{1}$$

定理 2[9]：若码 C 是一类线性或非线性的 (n,k,r,t) -LRCs，码 C 中每个信息符号的局部修复组仅包含一个奇偶校验位，则此类码的最小距离界为：

$$d_{\min}(C) \leqslant n-k-\left\lceil \frac{kt}{r} \right\rceil + t + 1 \tag{2}$$

最小距离越大，码的纠错能力和抗干扰能力越强。公式（2）给出了 (r,t) -LRCs 的最小距离上界，如果一类局部修复码的最小距离达到了这个上界，则此类局

部修复码是最小距离最优的 LRCs。

定理 3[10]：若码 C 是一类具有 t 个大小为 r 不相交修复集的 (n,k,r,t) -LRCs，则此码的码率满足：

$$R \leqslant \prod_{i=1}^{t} \frac{1}{1+\frac{1}{ir}} \tag{3}$$

码率越高，表示系统存储的冗余越少、信息传输的效率越高。公式（3）给出了 (r,t) -局部性的 LRCs 的码率上界，若一类局部修复码的码率大小达到了此上界，说明此码是码率最优的局部修复码。

定理 4[11]：特别地，当 $t=2$ 时，$(n,k,r,t=2)$ -LRCs 的码率上界和分块码长下界分别为：

$$R \leqslant \frac{r}{r+2} \tag{4}$$

$$n \geqslant k+\left\lceil \frac{2k}{r} \right\rceil \tag{5}$$

码长 n 是编码后的总符号数，包含信息符号和校验符号两部分。公式（4）和公式（5）给出了 $(r,t=2)$ 情况下 LRCs 的码率上界和码长下界，若一类局部修复码的码率和码长均达到了上述边界，则称其为码率最优、码长最优的码。

定义 2（(r,δ,t) -LRCs）[18]：若线性码 C 是信息符号具有 (r,δ,t) -局部性的 q 元 LRCs，信息符号 $i(1 \leqslant i \leqslant k)$ 的 t 个修复集为 $\Phi_1,\Phi_2,\cdots,\Phi_t \subset [n]$，需要满足以下条件：

1）$i \in \Phi_j, \forall j \in [t]$；

2）$|\Phi_j| \leqslant r+\delta-1$，子码 C_{Φ_j} 的最小距离为 $\delta, j \in [t]$；

3）$\Phi_j \cap \Phi_s = \{i\}, j \neq s \in [t]$；

4）$|\Phi_j \cap \{k+1,k+2,\cdots,n\}| = \delta-1, \forall j \in [t]$。

简单来说，若一类 LRCs 的信息符号具有 (r,δ,t) -局部性，则其第 $i(1 \leqslant i \leqslant k)$ 个信息符号包含于 t 个局部修复组；由局部修复组构成的子码，子码长度不超过 $r+\delta-1$，最小距离为 δ；这 t 个局部修复组的支撑集仅相交于第 i 个位置；且每个局部修复组中都具有的校验符号个数为 $\delta-1$。

定理 5[18]：信息符号具有 (r,δ,t) -局部性的 q 元 (n,k,d) -LRCs 的最小距离界为：

$$d \leqslant n-k-(\delta-1)\left\lceil \frac{kt}{r} \right\rceil + t(\delta-1)+1 \tag{6}$$

若一类信息符号具有 (r,δ,t) -局部性的局部修复码的最小距离达到了公式（6）的上界，则称此类局部修复码为最小距离最优的 (r,δ,t) -LRCs。

1.2 循环置换矩阵

定义 3（克罗内克列积）：矩阵 $\boldsymbol{A} \in \mathbb{F}^{Z \times W}$ 每行具有 ε 个非零元素，设 $\boldsymbol{A}=[a_{i,j}]$，其中 $a_{i,j}$ 为矩阵 $\boldsymbol{A}$ 中第 $i \in Z$ 行、第 $j \in W$ 列的元素；矩阵 $\boldsymbol{B} \in \mathbb{F}^{\mu \times \varepsilon}$ 不含全零列，其第 θ（$1 \leqslant \theta \leqslant \varepsilon$）列记为 $\boldsymbol{B}_\theta \in \mathbb{F}^{\mu \times 1}$。则矩阵 $\boldsymbol{A}$ 和矩阵 $\boldsymbol{B}$ 克罗内克列积运算后得到矩阵 $\boldsymbol{C}$。矩阵 $\boldsymbol{C}$ 是一个 $Z\mu \times W$ 的分块矩阵，其第（i，j）个分块 $\boldsymbol{C}_{i,j}$ 为：

$$\boldsymbol{C}_{i,j} = \begin{cases} a_{i,j} \times \boldsymbol{B}_\theta, & a_{i,j} \neq 0 \\ 0_{\mu \times 1}, & a_{i,j} = 0 \end{cases}$$

定义 4（循环置换矩阵）：设 $\boldsymbol{P}^0$ 代表单位矩阵 $\boldsymbol{I}_{p \times p}$，定义循环置换矩阵 $\boldsymbol{P}^1$ 为如下 $p \times p$ 矩阵：

$$\boldsymbol{P}^1 = \begin{bmatrix} 0 & \cdots & 0 & 1 \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{bmatrix}_{p \times p}$$

$\boldsymbol{P}^1$ 即 $\boldsymbol{P}^0 \times \boldsymbol{P}^1$，表示单位矩阵循环左移一位，$\boldsymbol{P}^2$ 即 $\boldsymbol{P}^0 \times \boldsymbol{P}^2$，表示单位矩阵循环左移两位，$\boldsymbol{P}^0$ 与 j 个 $\boldsymbol{P}^1$ 相乘得到 $\boldsymbol{P}^j$，$\boldsymbol{P}^j$ 代表矩阵 $\boldsymbol{P}^0$ 向左循环移位 j 次。

2 基于循环置换矩阵构造 LRCs

基于循环置换矩阵可以构造行重为素数、列重小于等于行重的矩阵。进一步地，根据得到的矩阵级联单位矩阵得到校验矩阵，由该校验矩阵可以构造出一类信息符号具有 (r,t) -局部性的 LRCs，此类 LRCs 的局部性 r 为素数，可用性为 $t \leqslant r$ 的任意整数。在此构造的基础上，对 (r,t) -LRCs 进行扩展，通过对矩阵采用克罗内克列积的数学运算方式，进一步构造了另一类信息符号具有 (r,δ,t) -局部性的 LRCs。

2.1 具有 (r,t) -局部性的 LRCs 的构造

步骤一：定义一类集合 $\boldsymbol{X}=\{1,2,\cdots,cp\}$，其中 c 和 p 为满足 $1 \leqslant c \leqslant p$ 的整数，且 p 是素数。基于集合 $\boldsymbol{X}$ 构造一个大小为 $c \times p$ 的矩阵 $\boldsymbol{A}_1$，集合 $\boldsymbol{X}$ 中的元素按照行优先的顺序依次填充，具体形式如下：

$$\boldsymbol{A}_1 = \begin{bmatrix} 1 & 2 & \cdots & p \\ p+1 & p+2 & \cdots & 2p \\ \vdots & \ddots & \vdots & \vdots \\ (c-1)p+1 & (c-1)p+2 & \cdots & cp \end{bmatrix}_{c \times p}$$

步骤二：将矩阵 $\boldsymbol{A}_1$ 与一个大小为 $cp \times p$ 的二进制矩阵 $\boldsymbol{Q}_1$ 建立对应关系。$\boldsymbol{Q}_1$ 构造方式如下，矩阵 $\boldsymbol{A}_1$ 的每一列包含的 c 个元素在 $\boldsymbol{Q}_1$ 中对应的列位置设为非零元素“1”，其余位置为“0”。$\boldsymbol{Q}_1$ 可表示为分块矩阵的形式：

$$\boldsymbol{Q}_1 = [\boldsymbol{I}^1_{p \times p}, \boldsymbol{I}^2_{p \times p}, \cdots, \boldsymbol{I}^j_{p \times p}, \cdots, \boldsymbol{I}^c_{p \times p}]^T$$

其中：$\boldsymbol{I}^j_{p \times p}(1 \leqslant j \leqslant c)$ 表示第 j 个 $p \times p$ 单位矩阵，整体构成一个 $cp \times p$ 的矩阵，其每一列有 c 个“1”，这些“1”的位置与矩阵 $\boldsymbol{A}_1$ 中相应列的元素索引保持一致。

通过对上述矩阵 $\boldsymbol{A}_1$ 施加循环移位操作，可生成 $p-1$ 个不同的矩阵，与矩阵 $\boldsymbol{A}_1$ 共同构成一个包含 p 个元素的矩阵集合 $\boldsymbol{A}=\{\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_l,\cdots,\boldsymbol{A}_p\}$，其中 $1 \leqslant l \leqslant p$。该集合中的每一个矩阵 $\boldsymbol{A}_l$ 的维度大小均为

$c\times p$。具体地，对于 $l=2$，3，…，p，矩阵 $\boldsymbol{A}_l$ 的第 i $(2\leqslant i\leqslant c)$ 行由矩阵 $\boldsymbol{A}_1$ 的第 i 行向左循环移位 $s_{i,l}$ 位得到，移位的个数 $s_{i,l}$ 通过以下公式计算：

$$s_{i,l}=(i-1)(l-1)\bmod p \tag{7}$$

步骤三：矩阵集合 $\boldsymbol{A}=\{\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_l,\cdots,\boldsymbol{A}_p\}$，$(1\leqslant l\leqslant p)$ 中的每个子矩阵 $\boldsymbol{A}_l$ 都与一个对应的二进制矩阵 $\boldsymbol{Q}_l$ 相关联，从而得到一个二进制矩阵集合 $\boldsymbol{Q}=\{\boldsymbol{Q}_1,\boldsymbol{Q}_2,\cdots,\boldsymbol{Q}_l,\cdots,\boldsymbol{Q}_p\}$，其中 $1\leqslant l\leqslant p$。矩阵 $\boldsymbol{Q}_l$ 中的 $\boldsymbol{P}^{(i-1)(l-1)\bmod p}$ 是由矩阵 $\boldsymbol{Q}_1$ 中的单位矩阵 $\boldsymbol{I}^i$ 向左循环移 $(i-1)(l-1)\bmod p$ 位得到，其它部位循环移位方式同矩阵 $\boldsymbol{Q}_l$ 保持一致。基于集合 $\boldsymbol{Q}$ 可以得到一个关联矩阵 $\boldsymbol{U}$，其结构如下所示：

$$\boldsymbol{U}=\begin{bmatrix}\overbrace{\boldsymbol{I}^0}^{Q_1} & \overbrace{\boldsymbol{P}^0}^{Q_2} & \cdots & \overbrace{\boldsymbol{P}^0}^{Q_l} & \cdots & \overbrace{\boldsymbol{P}^0}^{Q_p}\\ \boldsymbol{I}^2 & \boldsymbol{P}^1 & \cdots & \boldsymbol{P}^{l-1} & \cdots & \boldsymbol{P}^{p-1}\\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots\\ \boldsymbol{I}^i & \boldsymbol{P}^{i-1} & \cdots & \boldsymbol{P}^{(i-1)(l-1)\bmod p} & \cdots & \boldsymbol{P}^{(i-1)(p-1)\bmod p}\\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots\\ \boldsymbol{I}^c & \boldsymbol{P}^{c-1} & \cdots & \boldsymbol{P}^{(c-1)(l-1)\bmod p} & \cdots & \boldsymbol{P}^{(c-1)(p-1)\bmod p}\end{bmatrix}$$

该关联矩阵 $\boldsymbol{U}$ 是一个分块矩阵，其维度为 $cp\times p^2$。通过分析其结构特性可知，关联矩阵 $\boldsymbol{U}$ 的每行行重为 p；每列列重为 c。关联矩阵 $\boldsymbol{U}$ 是大小为 $cp\times p^2$ 的二元稀疏 (x,y)-正则矩阵，其中 $x=p$，$y=c$。该关联矩阵的稀疏性和正则性是构造局部修复码的基础。

构造 1：关联矩阵 $\boldsymbol{U}$ 通过级联一个大小为 $cp\times cp$ 的单位矩阵，得到校验矩阵 $\boldsymbol{H}_1=[U\mid I]$，由该校验矩阵生成一类线性码记为码 C_1，则码 C_1 是信息符号具有 (r,t)-局部性的 LRCs，其满足参数条件 $(n=p^2+cp,k=p^2,r=p,t=c)$。其中，n 为码长，k 为信息符号数量，r 为局部修复集的最大取值参数，t 为每个信息符号的不相交修复集的个数。

证明：由校验矩阵 $\boldsymbol{H}_1=[U\mid I]$ 的列数和行数可直接得出码 $\boldsymbol{C}_1$ 的码长、维数；从校验矩阵的行重可得出局部性。最后证明可用性，即证明对于任意信息符号 c_i $(i\in[p^2])$，在其对偶码中存在 t 个码字，满足每个码字的汉明重量不超过 r，且这个码字中任意两个不同码字的非零元素相交个数为 1。对于信息符号 c_i $\{i\in[1,p^2]\}$，在校验矩阵 $\boldsymbol{H}_1$ 的前 k 列中，每一列非零元素所在的 t 行对应的码字均满足上述两个条件。因此，得证码 $\boldsymbol{C}_1$ 的信息符号具有可用性 $t=c$。

推论 1：由校验矩阵 $\boldsymbol{H}_1$ 可以生成一类局部修复码，此类码的信息符号具有 (r,t)-局部性。其中各参数满足条件 $(n=p^2+cp,k=p^2,r=p,t=c)$。特别地，当可用性 $t=2$ 时，此类码的码长达到了文献 [11] 提出的最优码长下界，因此，构造 1 中基于循环置换矩阵构造的 LRCs 是码长最优的 (r,t)-LRCs。

证明：由校验矩阵可计算该码的码长、维数、局部性分别为 $n=p^2+cp$，$k=p^2$，$r=p$，将这些参数代入定理 4 中的码长下界，即：

$$n\geqslant k+\left\lceil\frac{2k}{r}\right\rceil=p^2+\left\lceil\frac{2p^2}{p}\right\rceil=p^2+2p \tag{8}$$

可以看出，当可用性 $t=2$ 时，有码长 $n=p^2+2p$，恰好达到码长下界。这表明在该参数下，构造 1 的码长是最优的，证毕。

例 1：以参数 $c=3,p=5$ 为例进行构造说明。首先定义集合 $\boldsymbol{X}=\{1,2,\cdots,15\}$，基于该集合 $\boldsymbol{X}$ 中的元素构造一个大小为 $c\times p=3\times5$ 的矩阵 $\boldsymbol{A}_1$，矩阵 $\boldsymbol{A}_1$ 表示如下：

$$\boldsymbol{A}_1=\begin{bmatrix}1&2&3&4&5\\6&7&8&9&10\\11&12&13&14&15\end{bmatrix}_{3\times5}$$

构造一个与矩阵 $\boldsymbol{A}_1$ 对应的二进制矩阵 $\boldsymbol{Q}_1$。对于矩阵 $\boldsymbol{A}_1$ 的每一列，其包含的 c 个元素在矩阵 $\boldsymbol{Q}_1$ 中对应的列位置设为非零元素“1”，其余位置为“0”。构造的矩阵 $\boldsymbol{Q}_1$ 由三个 5×5 的单位矩阵纵向叠加组成：

$$\boldsymbol{Q}_1=\begin{bmatrix}I^1_{5\times5}\\I^2_{5\times5}\\I^3_{5\times5}\end{bmatrix}_{15\times5}$$

接下来，对矩阵 $\boldsymbol{A}_1$ 按照步骤二所述的循环移位规则进行操作，可以得到如下所示的 4 个不同的新矩阵，分别表示为 $\boldsymbol{A}_2$、$\boldsymbol{A}_3$、$\boldsymbol{A}_4$、$\boldsymbol{A}_5$，与矩阵 $\boldsymbol{A}_1$ 共同构成集合 $\boldsymbol{A}=\{\boldsymbol{A}_1,\boldsymbol{A}_2,\boldsymbol{A}_3,\boldsymbol{A}_4,\boldsymbol{A}_5\}$。移位位数由公式 $s_{i,l}=(i-1)(l-1)\bmod5$ 得到，其中 i 为行号，l 为矩阵编号。生成的具体矩阵如下：

$$\boldsymbol{A}_2=\begin{bmatrix}1&2&3&4&5\\7&8&9&10&6\\13&14&15&11&12\end{bmatrix},$$

$$\boldsymbol{A}_3=\begin{bmatrix}1&2&3&4&5\\8&9&10&6&7\\15&11&12&13&14\end{bmatrix}$$

$$\boldsymbol{A}_4=\begin{bmatrix}1&2&3&4&5\\9&10&6&7&8\\12&13&14&15&11\end{bmatrix},$$

$$\boldsymbol{A}_5=\begin{bmatrix}1&2&3&4&5\\10&6&7&8&9\\14&15&11&12&13\end{bmatrix}$$

随后，将集合 $\boldsymbol{A}=\{\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_5\}$ 中的每个矩阵 $\boldsymbol{A}_l$ 都与一个对应的二进制矩阵 $\boldsymbol{Q}_l$ 相关联，得到矩阵集合 $\boldsymbol{Q}=\{\boldsymbol{Q}_1,\boldsymbol{Q}_2,\cdots,\boldsymbol{Q}_5\}$。集合中矩阵 $\boldsymbol{Q}_l$ 中的 $\boldsymbol{P}^{(i-1)(l-1)\bmod5}$ 是由矩阵 $\boldsymbol{Q}_1$ 中的单位矩阵 $\boldsymbol{I}^i$ 向左循环移 $(i-1)(l-1)\bmod5$ 位得到。若规定 $\boldsymbol{P}^0$ 表示单位矩阵 $\boldsymbol{I}_{5\times5}$，$\boldsymbol{P}^1$ 表示 $\boldsymbol{P}^0\times\boldsymbol{P}$，即单位矩阵左移 1 位，$\boldsymbol{P}^2$ 表示 $\boldsymbol{P}^0\times\boldsymbol{P}^2$，

即单位矩阵左移 2 位，以此类推，$\boldsymbol{P}^j$ 表示对单位矩阵进行循环左移 j 位，循环置换矩阵 $\boldsymbol{P}^1$ 的表示形式为：

$$\boldsymbol{P}^1=\begin{bmatrix}0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\end{bmatrix}_{5\times5}$$

由集合 $\boldsymbol{Q}$ 构造关联矩阵 $\boldsymbol{U}$，其结构表示如下：

$$\boldsymbol{U}=\begin{bmatrix}\overset{Q_1}{\widehat{\boldsymbol{I}^1}}&\overset{Q_2}{\widehat{\boldsymbol{P}^0}}&\cdots&\overset{Q_j}{\widehat{\boldsymbol{P}^0}}&\cdots&\overset{Q_p}{\widehat{\boldsymbol{P}^0}}\\\boldsymbol{I}^2&\boldsymbol{P}^1&\cdots&\boldsymbol{P}^{l-1}&\cdots&\boldsymbol{P}^{p-1}\\\vdots&\vdots&\ddots&\vdots&\ddots&\vdots\\\boldsymbol{I}^i&\boldsymbol{P}^{i-1}&\cdots&\boldsymbol{P}^{(i-1)(l-1)\bmod p}&\cdots&\boldsymbol{P}^{(i-1)(p-1)\bmod p}\\\vdots&\vdots&\ddots&\vdots&\ddots&\vdots\\\boldsymbol{I}^c&\boldsymbol{P}^{c-1}&\cdots&\boldsymbol{P}^{(c-1)(l-1)\bmod p}&\cdots&\boldsymbol{P}^{(c-1)(p-1)\bmod p}\end{bmatrix}=\begin{bmatrix}\boldsymbol{I}^1_{5\times5}&\boldsymbol{P}^0&\boldsymbol{P}^0&\boldsymbol{P}^0&\boldsymbol{P}^0\\\boldsymbol{I}^2_{5\times5}&\boldsymbol{P}^1&\boldsymbol{P}^2&\boldsymbol{P}^3&\boldsymbol{P}^4\\\boldsymbol{I}^3_{5\times5}&\boldsymbol{P}^2&\boldsymbol{P}^4&\boldsymbol{P}^1&\boldsymbol{P}^3\end{bmatrix}$$

该关联矩阵 $\boldsymbol{U}$ 是一个大小为 15×25 的二进制矩阵，其具体表达形式如下：

$$\boldsymbol{U}=\left[\begin{array}{ccccc|ccccc|ccccc|ccccc|ccccc}
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0\\
0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0\\
0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
\hline
1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0\\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&0&1\\
0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&0\\
\hline
1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&1&0&0&1&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&0&0&1&0&0&0&1\\
0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&1&0&0&0\\
0&0&0&1&0&0&1&0&0&0&0&1&0&0&0&0&0&1&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&1&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
\hline
1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&0&0&1&0&0&0&1\\
0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&1&0&0&0\\
0&0&0&1&0&0&1&0&0&0&0&1&0&0&0&0&0&1&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&1&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0
\end{array}\right]$$

通过对关联矩阵 $\boldsymbol{U}$ 级联一个大小为 15×15 的单位矩阵，得到校验矩阵 $\boldsymbol{H}_1=[\boldsymbol{U}_{15\times25}\mid\boldsymbol{I}_{15\times15}]$。由该校验矩阵 $\boldsymbol{H}_1$ 构造的码是具有 $(r=5,t=3)$-局部性的 $(n=40,k=25,d=4)$-LRCs，最多可以纠正 3 个故障。以信息符号 c_1 为例，若该符号发生故障，根据校验矩阵 $\boldsymbol{H}_1$ 的结构可知，信息符号 c_1 可通过以下 3 种修复方式 $c_1=c_{26}-c_6-c_{11}-c_{16}-c_{21}$，$c_1=c_{31}-c_{10}-c_{14}-c_{18}-c_{22}$，$c_1=c_{36}-c_9-c_{12}-c_{20}-c_{23}$修复，对应的修复集分别表示为 $\varphi(1)=\{6,11,16,21,26\}$,$\varphi(2)=\{10,14,18,22,31\}$,$\varphi(3)=\{9,12,20,23,36\}$，这些修复集两两不相交，且每个修复集的大小均为 $r=5$。在此构造码中，每个信息符号的修复集大小均为 r、修复集的个数均为 t，且各个修复集相交为零。任一信息符号发生故障，均可通过 t 种不同修复集完成修复。因为每个修复集中包含的校验符号个数均为 1，所以此码是单校验局部修复码，可有效降低故障修复过程中的修复开销。

2.2 具有 (r,δ,t)-局部性的 LRCs 的构造

为了进一步提升容错能力，本小节在构造 1 的基础上进行扩展，构造了一类具有 (r,δ,t)-局部性的 LRCs，其中 δ 表示局部修复组的最小距离，用于处理多个符号同时发生故障的情况。具体构造过程如下。

在构造 1 的步骤三中得到的关联矩阵 $\boldsymbol{U}$ 是一个行重为 p、列重为 t、大小为 $cp\times p^2$ 阶的二元稀疏矩阵，且满足 $(x=p,y=c)$-正则性。进一步，设 $\hat{\boldsymbol{M}}=[\boldsymbol{M}\mid\boldsymbol{I}]$ 为一类最大距离可分（MDS）码的校验矩阵，其中 $\boldsymbol{M}$ 是大小为 $(\delta-1)\times p$ 的矩阵，且其所有元素均非零。接下来，定义一种矩阵运算方式“$*$”，用于对关联矩阵 $\boldsymbol{U}$ 进行变换。具体运算规则如下，$\boldsymbol{U}*\boldsymbol{M}$ 表示将矩阵 $\boldsymbol{U}$ 的每一行向量中的第 $e(1\leqslant e\leqslant p)$ 个“1”分别与矩阵 $\boldsymbol{M}$ 的第 e 列进行克罗内克列积运算；同理，将矩阵 $\boldsymbol{U}$ 的所有“0”与大小为 $(\delta-1)$ 的全零列向量进行克罗内克列积运算。通过该运算，可以得到一个新的矩阵 $\boldsymbol{U}'$，可表示为 $\boldsymbol{U}'=[\boldsymbol{U}*\boldsymbol{M}]_{cp(\delta-1)\times p^2}$。在关联矩阵 $\boldsymbol{U}'$ 右侧级联一个大小为 $cp(\delta-1)\times cp(\delta-1)$ 单位矩阵 $\boldsymbol{I}$，构造新的校验矩阵 $\boldsymbol{H}_2=[\boldsymbol{U}'\mid\boldsymbol{I}_{cp(\delta-1)\times cp(\delta-1)}]$。

构造 2：基于以上校验矩阵 $\boldsymbol{H}_2=[\boldsymbol{U}'\mid\boldsymbol{I}_{cp(\delta-1)\times cp(\delta-1)}]$ 构造的线性码 $\boldsymbol{C}_2$ 是一类信息符号具有 (r,δ,t)-局部性的 LRCs，其中参数分别满足条件 $n=p^2+cp(\delta-1),k=p^2,r=p,\delta=\delta,t=c$。此构造引入了 MDS 码和克罗内克列积运算，增强了局部修复码的容错能力，使其能够处理局部修复组内多个符号同时故障的情况，同时保持高效修复特性。

证明：由校验矩阵 $\boldsymbol{H}_2=[\boldsymbol{U}'\mid\boldsymbol{I}_{cp(\delta-1)\times cp(\delta-1)}]$ 的列数和行数可直接得出码 $\boldsymbol{C}_2$ 的码长、维数。接下来证明此类 LRCs 具有 (r,δ,t)-局部性。码 $\boldsymbol{C}_2$ 的任意第 $i(1\leqslant i\leqslant k)$ 个信息符号都包含在 t 个局部修复组中；每个局部修复组生成的子码长度不超过 $r+\delta-1$，且最小距离至少为 δ；校验矩阵 $\boldsymbol{H}_2$ 中的 t 个局部修复组的支撑集仅相交于第 i 个位置，满足修复集不相交条件；不同的局部修复组中的校验符号个数均为 $\delta-1$，用于提供系统的局部容错能力。故通过上述步骤构造的码 $\boldsymbol{C}_2$ 为信息符号具有 (r,δ,t)-局部性的 LRCs。

例 2：以例 1 中参数 $c=3,p=5$ 为例，构造信息符号具有 (r,δ,t)-局部性的 LRCs。设局部最小距离参数 $\delta=3$，并选择一个最大距离可分（MDS）码的校验矩阵 $\hat{\boldsymbol{M}}=[\boldsymbol{M}\mid\boldsymbol{I}]$，其中矩阵 $\boldsymbol{M}$ 大小为 $(\delta-1)\times p=2\times$

5，采用有限域 F_q，$(q \geqslant 5)$ 上的范德蒙结构，设 α 为域中的本原元，则矩阵 $\boldsymbol{M}$ 的结构如下所示：

$$\boldsymbol{M}=\begin{bmatrix}1 & 1 & 1 & 1 & 1\\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4\end{bmatrix}$$

将矩阵 $\boldsymbol{M}$ 与例 1 中得到的关联矩阵 $\boldsymbol{U}$ 进行定义的 $*$ 运算，即 $\boldsymbol{U}*\boldsymbol{M}$。通过该运算，得到一个新的矩阵 $\boldsymbol{U}'_{cp(\delta-1)\times p^2}$，其维度为 $cp(\delta-1)\times p^2=30\times 25$，如下所示：

$$\boldsymbol{U}'=\left[\begin{array}{ccccc|ccccc|ccccc|ccccc|ccccc}
1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0\\
1&0&0&0&0&\alpha&0&0&0&0&\alpha^2&0&0&0&0&\alpha^3&0&0&0&0&\alpha^4&0&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0\\
0&1&0&0&0&0&\alpha&0&0&0&0&\alpha^2&0&0&0&0&\alpha^3&0&0&0&0&\alpha^4&0&0&0\\
0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&\alpha&0&0&0&0&\alpha^2&0&0&0&0&\alpha^3&0&0&0&0&\alpha^4&0&0\\
0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0\\
0&0&0&1&0&0&0&0&\alpha&0&0&0&0&\alpha^2&0&0&0&0&\alpha^3&0&0&0&0&\alpha^4&0\\
0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1\\
0&0&0&0&1&0&0&0&0&\alpha&0&0&0&0&\alpha^2&0&0&0&0&\alpha^3&0&0&0&0&\alpha^4\\
\hline
1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0\\
1&0&0&0&0&0&0&0&0&\alpha&0&0&0&\alpha^2&0&0&0&\alpha^3&0&0&0&\alpha^4&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&1&0&0&0&\alpha&0&0&0&0&0&0&0&0&\alpha^2&0&0&0&\alpha^3&0&0&0&\alpha^4&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0\\
0&0&1&0&0&0&\alpha&0&0&0&\alpha^2&0&0&0&0&0&0&0&0&\alpha^3&0&0&0&\alpha^4&0\\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&\alpha&0&0&0&\alpha^2&0&0&0&0&\alpha^3&0&0&0&0&0&0&0&\alpha^4\\
0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&\alpha&0&0&0&\alpha^2&0&0&0&\alpha^3&0&0&0&\alpha^4&0&0&0&0\\
\hline
1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0\\
1&0&0&0&0&0&0&0&\alpha&0&0&\alpha^2&0&0&0&0&0&0&0&\alpha^3&0&0&\alpha^4&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&1&0\\
0&1&0&0&0&0&0&0&0&\alpha&0&0&\alpha^2&0&0&\alpha^3&0&0&0&0&0&0&0&\alpha^4&0\\
0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&1\\
0&0&1&0&0&\alpha&0&0&0&0&0&0&0&\alpha^2&0&0&\alpha^3&0&0&0&0&0&0&0&\alpha^4\\
0&0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&1&0&0&0&0\\
0&0&0&1&0&0&\alpha&0&0&0&0&0&0&0&\alpha^2&0&0&\alpha^3&0&0&\alpha^4&0&0&0&0\\
0&0&0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&1&0&0&0\\
0&0&0&0&1&0&0&\alpha&0&0&\alpha^2&0&0&0&0&0&0&0&\alpha^3&0&0&\alpha^4&0&0&0
\end{array}\right]$$

在关联矩阵 $\boldsymbol{U}'$ 右侧级联一个大小为 30×30 的单位矩阵 $\boldsymbol{I}$，可以得到新的校验矩阵 $\boldsymbol{H}_2=[\boldsymbol{U}'\mid \boldsymbol{I}_{30\times 30}]$。由校验矩阵 $\boldsymbol{H}_2$ 生成的码 $(n=55,k=25,d=7)$-LRCs 的信息符号具有 $(r=5,\delta=3,t=3)$-局部性。以信息符号 c_1 为例，若其发生故障，可通过以下 3 个互不相交的修复集 $\varphi(1)=\{6,11,16,21,26,27\}$，$\varphi(2)=\{10,14,18,22,36,37\}$，$\varphi(3)=\{9,12,20,23,46,47\}$ 进行恢复，其它信息符号的修复方式与此类似。每一个信息符号均具备 $t=3$ 个互不相交的修复集，且每个局部修复组内可容忍至多 $\delta-1=2$ 个符号同时故障，整个系统能容忍任意一个信息符号和最多 $t(\delta-1)-1$ 个校验符号同时发生故障。此外，系统的容错能力可通过参数 δ 值灵活调节。

本文提出的编码构造方法在结构与参数设置上具有显著优势，具体体现在以下两个方面。

在结构设计上，采用循环置换矩阵构造校验矩阵，循环置换矩阵具有较强的规则性，使编码后的码字在空间分布上更加均匀，从而在相同码长下，实现最小距离最优。同时，这种结构也使校验符号数可控制，以较少冗余实现目标容错能力，进而提高了码率。进一步，我们引入克罗内克列积运算对上述校验矩阵进行扩展，在每个局部修复组中实现局部容错能力 δ 可调，当局部容错能力增强时，克罗内克列积运算保留了局部修复块的局部性，单节点故障的修复仍然在原始的局部组内进行，修复局部度大小并未随 δ 增大而变化，从而实现了容错能力与修复局部度之间相互独立。

在参数设置方面，循环移位运算使校验冗余分布更均匀和可控，克罗内克列积运算使局部容错能力灵活可调，且每个校验符号能够同时保护多个信息符号，提升了冗余信息的利用率，这也是实现高码率的关键之一。将循环置换运算与克罗内克列积运算相结合，实现参数的灵活调整，从而广泛适用于不同的分布式存储应用场景，在高码率需求环境中，适当减小 δ 值以提高码率；在高容错需求环境中，适当增加 δ 值以增强容错。

3　性能分析

3.1　最小距离分析

本小节对所构造的局部修复码的最小距离进行详细的证明，验证了两种局部修复码的最小距离均达最优。

推论 2：本文基于循环置换矩阵构造的具有 (r,t)-局部性的 LRCs 的最小距离为 $d=t+1$，该最小距离达到最优。

证明：由构造 1 中的校验矩阵 $\boldsymbol{H}_1=[\boldsymbol{U}\mid \boldsymbol{I}_{cp\times cp}]$ 的结构可知，关联矩阵 $\boldsymbol{U}$ 每列列重均为 t，矩阵 $\boldsymbol{U}$ 的每个列向量都可由右侧级联的单位矩阵的 t 列线性组合，则 $\boldsymbol{H}_1$ 中存在 $t+1$ 列线性相关。即构造 1 的最小距离 $d\leqslant t+1$。若想证明 $d=t+1$，还需证明 $d\geqslant t+1$。由构造 1 可知，关联矩阵 $\boldsymbol{U}$ 的行重为 $r=p$、列重为 $t=c$，且 t 行中任意不同两行的 r 个非零元素相交个数均为 1，即构造 1 中的码是信息符号具有 (r,t)-局部性的 LRCs，由定理 1 可知此码的最小距离需 $d\geqslant t+1$。综上所述，可以得到构造 1 的最小距离 $d=t+1$。

又因为构造 1 中信息符号具有 (r,t)-局部性的

LRCs 的参数满足 $n=p^2+cp$，$k=p^2$，$r=p$，$t=c$，将这些码长、维数、局部性和可用性的参数值代入公式（2）中可得：

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

$$p^2+cp-p^2-\left\lceil \frac{p^2 c}{p} \right\rceil + c + 1 = c + 1 = t + 1 \quad (9)$$

所以 (r,t) -LRCs 的最小距离 $d=t+1$，达到了最小距离边界。由此得证构造 1 的最小距离最优。

推论 3：本文基于循环置换矩阵构造的具有 (r,δ,t) -局部性的 LRCs 的最小距离为 $d=t(\delta-1)+1$，该最小距离达到最优。

证明：与推论 2 同理，可得校验矩阵 $\boldsymbol{H}_2$ 中存在 $t(\delta-1)$ 列线性相关，即构造 2 的最小距离 $d \leqslant t(\delta-1)+1$。此外，若想证明 $d=t(\delta-1)+1$，还需证明 $d \geqslant t(\delta-1)+1$。若矩阵 $\boldsymbol{H}_2$ 中任意选择 $t(\delta-1)$ 列，考虑以下两种情况，1）若这 $t(\delta-1)$ 列均选自后 $cp(\delta-1)$ 列的单位矩阵，显然这 $t(\delta-1)$ 列是线性无关的；2）若这 $t(\delta-1)$ 列中至少有一列 ξ 来自矩阵 $\boldsymbol{U}'$，列 ξ 的汉明重量为 $t(\delta-1)$，将其按照支撑集的位置划分成 t 个权重为 $\delta-1$ 的子向量，分别包含在 t 个局部校验矩阵中，由于每个局部校验矩阵来自 MDS 码的扩展，其中的任意 $\delta-1$ 列都是线性无关的，因此，要消除子向量中的 $\delta-1$ 个非零元素，至少需要 $\delta-1$ 个其他列。又因包含列 ξ 坐标的 t 个局部校验矩阵仅在该坐标上相交，所以至少需要 $t(\delta-1)$ 个其他列来消除这 t 个子向量，即 $d \geqslant t(\delta-1)+1$。综上所述，可以得到由校验矩阵 $\boldsymbol{H}_2$ 生成的信息符号具有 (r,δ,t) -局部性的 LRCs 的最小距离 $d=t(\delta-1)+1$。

又因为构造 2 中信息符号具有 (r,δ,t) -局部性的 LRCs 的满足参数条件 $n=p^2+cp(\delta-1)$，$k=p^2$，$r=p$，$\delta=\delta$，$t=c$，将这些参数代入公式（6）的最小距离边界可得：

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

$$p^2+cp(\delta-1)-p^2-(\delta-1)\left\lceil \frac{p^2 c}{p} \right\rceil + c(\delta-1)+1 \leqslant$$

$$c(\delta-1)+1 = t(\delta-1)+1 \quad (10)$$

所以 (r,δ,t) -LRCs 的最小距离 $d=t(\delta-1)+1$，达到了最小距离边界。由此得证构造 2 的最小距离最优。

3.2 码率和容错能力分析

本小节主要通过理论参数以及数值仿真曲线对构造的局部修复码的两个性能进行分析，即码率和容错能力。

由表 1 的对比结果可知，基于 $PG(2,2^a)$ 构造方案和基于迹函数构造方案得到的 (r,t) -LRCs，二者的局部性参数与可用性参数之间存在较强的关联性，当局部性 r 取某一固定值时，可用性 t 也被限制为某一特定值，因此，这两种构造方案的参数灵活性较低，在一定程度上限制了系统的应用范围。相比之下，基于阵列 LDPC 码的构造方案和本文基于循环置换矩阵的构造方案中，局部性与可用性之间不存在此类约束关系。进一步对比发现，基于阵列 LDPC 码的 t 仅取偶数，而本文构造 1 方案的可用性可在 $t \in \{1,2,\cdots,p\}$ 范围内灵活选取任意整数。在局部性参数和可用性参数的取值均相等的条件下，从码率参数分析可以得到本文构造 1 方案的码率高于基于阵列 LDPC 码构造方案的码率；此外，构造 1 方案的码率始终大于 1/2，而 $PG(2,2^a)$ 构造方案的码率始终等于 1/2、基于迹函数构造方案的码率小于 1/2，可得构造 1 方案的码率始终高于 $PG(2,2^a)$ 构造方案和基于迹函数构造方案的码率。此外，本文所提出的构造 2 中的 (r,δ,t) -LRCs，具有灵活的可用性参数取值和可调节的局部容错能力参数取值。

图 1 给出了文献［11］提出的理论码率上界以及基于阵列 LDPC 码、基于迹函数和构造 1 三种方案的码率随局部性 r 的变化图。由图 1 可知，在可用性参数固定为 2 时，随局部性 r 的增大，系统的不同修复集中包含的符号数增加，冗余所占比重减小，存储效率提升，故

表 1 参数比较分析

构造类型	构造方法	n	k	r	t	R
(r,t) -LRCs	基于阵列 LDPC 码 LRCs[20]	q^2+qs+1	q^2	q 是素数	s 是偶数	$\frac{r^2}{r^2+rt+1}$
	基于 $PG(2,2^a)$ LRCs[14]	$2(4^a+2^a+1)$	4^a+2^a+1	2^a+1a 是正整数	2^a+1	$\frac{1}{2}$
	基于迹函数 LRCs[15]	2^m-1	$2^{m-1}-1$	$m-1$	m	$\frac{2^r-1}{2^{r+1}-1}$
	基于循环置换阵 LRCs(构造 1)	p^2+cp	p^2	p 是素数	$t,t \in \{1,2\cdots p\}$	$\frac{r}{r+t}$
(r,δ,t) -LRCs	基于循环置换阵 LRCs(构造 2)	$p^2+cp(\delta-1)$	p^2	p 是素数	$t,t \in \{1,2\cdots p\}$	$\frac{r}{r+t(\delta-1)}$

所有方案的码率均呈增大的趋势；在给定 r 和 $t=2$ 下，构造 1 的码率与文献［11］提出的最优码率重合，实现了码率最优；阵列 LDPC 码方案比构造 1 方案的码率低；基于 $PG(2,2^a)$ 构造方案的码率等于 1/2、基于迹函数构造方案的码率小于 1/2、二者的码率均低于构造 1 方案的码率。

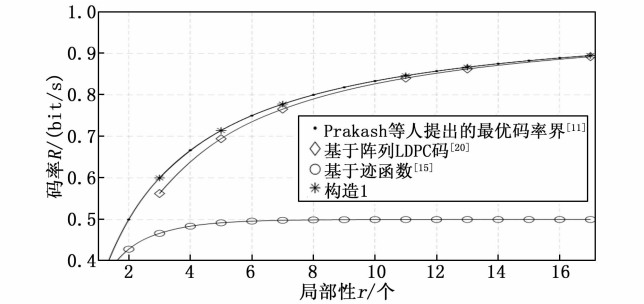

图 1　可用性 $t=2$ 时，码率随局部性 r 的变化

图 2 给出了局部性 $r=17$ 条件下，文献［10］提出的理论码率上界、阵列 LDPC 码方案以及构造 1 方案的码率随 t 的变化图。由图 2 可以看出，当局部性取 17 时，随着可用性 t 的增大，系统中的校验冗余增多，存储效率增大，导致码率呈逐步下降趋势；在相同的可用性 t 取值下，阵列 LDPC 码方案始终比构造 1 方案的码率低，这表明本文提出的构造 1 方案在利用冗余方面更具高效性。此外，构造 1 方案的可用性参数取值更灵活，范围更广。

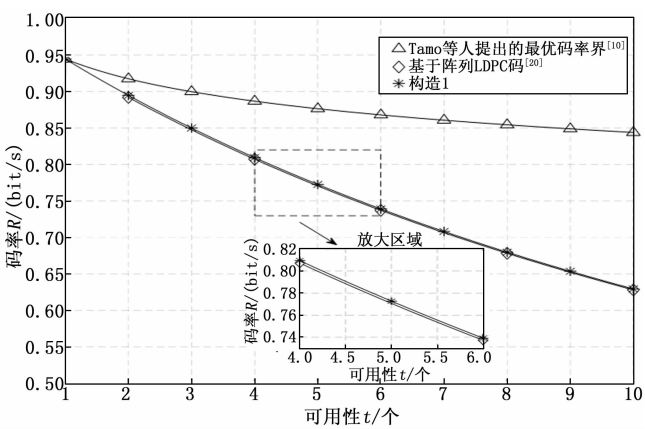

图 2　局部性 $r=17$ 时，码率随局部性 t 的变化

图 3 给出了本文提出的构造 2 方案与构造 1 方案在可用性取值相同时码率随着局部性 r 的变化图，由图可知，构造 2 方案在 $\delta=2$ 时，码率变化趋势与构造 1 方案完全重合，即两者均达到了最优码率上界。但随着 δ 的增大，每个修复集内引入的用来抵抗多个节点故障的局部校验符号增多，总的冗余开销增加，构造 2 的码率呈现下降趋势。图 4 给出了当局部性 r 取固定值 17 时，构造 2 方案和构造 1 方案的容错能力随可用性的变化图。由图可知，随着可用性 t 和局部容错能力 δ 的增大，最小距离随之变大，从而系统整体容错能力呈逐渐上升趋势。由此得到结论，当 r、t 固定，随着 δ 的增大，码率呈下降趋势，而容错能力呈增大的趋势。利用这一特点，可以根据现实场景灵活地调整 δ 取值，在高码率需求环境中，适当减小 δ 值以提高码率，保证较高的存储效率；在高容错需求环境中，适当增加 δ 值以增强容错。这种灵活可调节的特点使本文所提出的构造 2 方案能够适用于各种分布式存储场景。

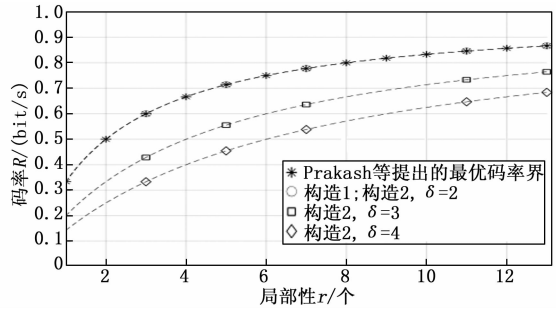

图 3　可用性 $t=2$ 时，构造 2 和构造 1 的码率对比

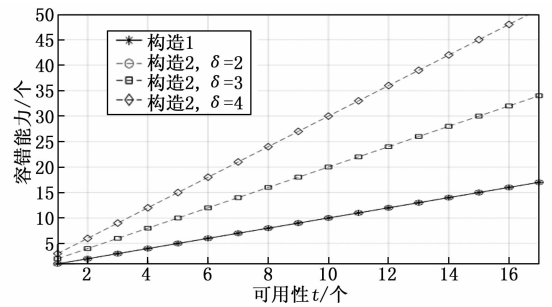

图 4　局部性 $r=17$ 时，构造 2 和构造 1 的容错能力随可用性的变化

3.3　编解码复杂度分析

为评估不同编码方案在实际系统中的可用性，现对本文提出的 (r,t) -LRCs 和 (r,δ,t) -LRCs 构造方法的计算复杂度进行分析，主要关注整体编码复杂度与信息符号平均修复复杂度两个性能指标。在有限域 F_q 中，任何运算的复杂度至少为 $O(\log_2 q)$，设 $e=\lfloor \log_2 q \rfloor$。一次加法或减法运算的复杂度为 $O(e)$，一次乘法运算的复杂度为 $O(e^2)$。对于 (r,t) -LRCs，生成单个校验符号或修复单个故障信息符号平均需要进行 $r-1$ 次有限域加法，计算复杂度为 $O((r-1)e)$，设 $J=n-k$ 为校验符号总数，则其整体编码复杂度为 $O[J(r-1)e]$；对于 (r,δ,t) -LRCs，由于其校验结构更为复杂，生成单个校验符号或修复单个故障信息符号的复杂度增至 $O[re^2+(r-1)e]$，其整体编码复杂度相应为 $O\{J[re^2+(r-1)e]\}$。

将表 1 中不同编码方案的参数代入上述编解码复杂度公式，得到如表 2 所示的计算结果。由表 2 可知，基于射影几何 $PG(2,2^a)$ 构造方案的编解码复杂度随参数

a 呈指数级增长。类似地，基于迹函数构造方案也表现相同的趋势。而本文提出的基于循环置换阵的构造 1 具有显著优势，该方案的编码复杂度 $O[cp(p-1)e]$ 在渐近趋势上远低于上述两种指数级增长方案。即便与编码复杂度较低的基于阵列 LDPC 码的方案相比，在相同局部性参数和可用性参数条件下，而本文提出的基于循环置换阵的构造 1 的编码复杂度略低。相比于构造 1，本文构造 2 中的 (r,δ,t) -LRCs 通过引入额外的克罗内克列积运算来获得可灵活调节的容错能力 $\delta \geqslant 2$，这不可避免的带来了更高的计算复杂度 $O\{cp(\delta-1)[pe^2+(p-1)e]\}$，此方案以可控地增加编解码复杂度为代价，换取系统应对不同故障场景的灵活性，其在复杂多变的实际分布式存储系统中也具有广泛的应用前景。

表 2 不同构造方法编解码复杂度的对比分析

构造类型	构造方法	编码复杂度	信息符号平均修复复杂度
(r,t) -LRCs	基于阵列 LDPC 码 LRCs[20]	$O[(qs+1)(q-1)e]$	$O[(q-1)e]$
	基于 $PG(2,2^a)$ LRCs[14]	$O[(4^a+2^a+1)(2^a)e]$	$O(2^a e)$
	基于迹函数 LRCs[15]	$O[(2^m-2^{m-1})(m-2)e]$	$O[(m-2)e]$
	基于循环置换阵 LRCs(构造 1)	$O[cp(p-1)e]$	$O(p-1)e)$
(r,δ,t) -LRCs	基于循环置换阵 LRCs(构造 2)	$O\{cp(\delta-1)[pe^2+(p-1)e]\}$	$O[pe^2+(p-1)e]$

3.4 局部性、可用性和局部容错能力参数分析

本文提出的基于循环置换矩阵的两种局部修复码构造，构造 1 与构造 2 在关键性能参数上相较于现有构造展现出显著的灵活性与优越性，具体体现在以下方面。

表 3 给出了具体的参数取值比较分析，由表 3 可知，对于 (r,t) -LRCs，局部性 r 与可用性 t 的参数取值相互关联，一旦局部性 r 确定，可用性 t 的值也随之固定，缺乏根据实际系统需求进行调整的灵活性；相比之下，本文构造的 (r,t) -LRCs 的局部性和可用性没有上述固定的约束关系，局部性 r 由素数 p 决定，而可用性 t 可以在集合 $\{1,2\cdots p\}$ 中灵活地选择。这意味着，在保持局部性不变的前提下，可以根据对并行修复能力的需求，灵活的设置 t 的值，从而更好地平衡存储效率与修复性能。对于 (r,δ) -LRCs，现有的 (r,δ) -LRCs 中局部性 r 取值范围较小，不相交修复集的个数为 1，不支持故障节点的并行读取和修复。相比之下，本文构造的 (r,δ,t) -LRCs 的局部性突破了常固定为 3、2 或者其他特定的数字限制，允许局部容错能力 δ 取任意值，同时引入了可用性参数 t，保障了至少存在 t 个不相交的修复集，可以满足故障节点的并行修复。综上所述，本文的构造方案在局部性、可用性和局部容错能力这 3 个参数上实现了更优的灵活性，克服了现有方案中参数的局限性，适用于不同的存储应用场景。

表 3 参数比较分析

构造类型	构造方法	n	k	r	δ	t
(r,t) -LRCs	基于二元常重码的 (r,t) -LRCs[21]	$2q^2-2$	q^2-1	q	$\delta=2$	q
	基于部分几何码的 (r,t) -LRCs[22]	$2^{4h-1}-1$	$(2^{2h-1}+1)(2^{2h}-1)$	$2^{2h-1}+1$	$\delta=2$	2^{2h-1}
(r,δ) -LRCs	基于 $PG(3,q)$ 的 (r,δ) -LRCs[23]	q^2+1	4	3	$q-1$	1
	基于扩展 L -空间的 (r,δ) -LRCs[24]	$\frac{q^u-1}{q-1}$	$\frac{2n}{\delta-1}-u$	2	δ	1
本文构造	构造 1	p^2+cp	p^2	p 是素数	$\delta=2$	$t,t\in\{1,2\cdots p\}$
	构造 2	$p^2+cp(\delta-1)$	p^2	p 是素数	δ 为任意值	$t,t\in\{1,2\cdots p\}$

4 结束语

本文首先基于循环置换矩阵提出一类信息符号具有 (r,t) -局部性的 LRCs 的构造方法。与现有的 (r,t) -LRCs 相比，本文构造的 (r,t) -LRCs 在最小距离和码长达到最优的同时，还具有较高的码率和灵活的参数取值。进一步地，在构造的 (r,t) -LRCs 基础上，通过对校验矩阵进行克罗内克列积运算，构造一类信息符号具有 (r,δ,t) -局部性的 LRCs，构造的 (r,δ,t) -LRCs 的容错能力随着参数 δ,t 的调整而变化。当可用性一定时，根据实际场景需求灵活地调整 δ 取值，在高码率需求环境中，适当减小 δ 值以提高码率；在高容错需求环境中，适当增加 δ 值以增强容错，从而广泛适用于不同的分布式存储应用场景。本文的研究主要针对的是同构分布式存储系统中的局部修复码构造。下一步，我们将致力于把本文的编码方法推广到异构分布式存储系统中，以构造出能更好地适应节点间性能与可靠性差异的局部修复码。

参考文献：

[1] FANG W J, CHEN B, XIA S T, et al. Singleton-optimal LRCs and perfect LRCs via cyclic codes [C] //2021 IEEE International Symposium on Information Theory (ISIT), Melbourne, Australia, 2021, 3261-3266.

[2] QI Y C, FENG D, HOU B B. Towards building reliable and cost-efficient distributed storage systems [J]. IEEE Access, 2020, 8: 157862-157877.

[3] BSOUL M, ABDALLAH A E, ALMAKADMEH K, et al. A round-based data replication strategy [J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27 (1): 31-39.

[4] LIN H Y, TZENG W G. A secure erasure code-based cloud storage system with secure data forwarding [J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23 (6): 995 - 1003.

[5] LI J, LI B C. Erasure coding for cloud storage systems: a survey [J]. Tsinghua Science and Technology, 2013, 18 (3): 259 - 272.

[6] DIMAKIS A G, PRABHAKARAN V, RAMCHANDRAN K. Decentralized erasure codes for distributed networked storage [J]. IEEE Transactions on Information Theory, 2006, 52 (6): 2809 - 2816.

[7] DIMAKIS A G, GODFREY P B, WU Y N, et al. Network coding for distributed storage systems [J]. IEEE Transactions on Information Theory, 2010, 56 (9): 4539 - 4551.

[8] GOPALAN P, HUANG C, SIMITCI H, et al. On the locality of codeword symbols [J]. IEEE Transactions on Information Theory, 2012, 58 (11): 6925 - 6934.

[9] RAWAT A S, PAPAILIOPOULOS D S, DIMAKIS A G, et al. Locality and availability in distributed storage [J]. IEEE Transactions on Information Theory, 2016, 62 (8): 4481 - 4493.

[10] TAMO I, BARG A. Bounds on locally recoverable codes with multiple recovering sets [C] // 2014 IEEE International Symposium on Information Theory (ISIT), Honolulu, HI, USA, 2014, 691 - 695.

[11] PRAKASH N, LALITHA V, BALAJI S B, et al. Codes with locality for two erasures [J]. IEEE Transactions on Information Theory, 2019, 65 (12): 7771 - 7789.

[12] ZHANG Y, KAN H B. Locally repairable codes with strict availability from linear functions [J]. Sci. China Inf. Sci. 2018, 61: 109304.

[13] JING Z, SONG H Y. A construction of 2-sequential-recovery locally repairable codes [C] // 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, 2021, 1431 - 1433.

[14] HAO J, XIA S T. Constructions of optimal binary locally repairable codes with multiple repair groups [J]. IEEE Communications Letters, 2016, 20 (6): 1060 - 1063.

[15] WANG A, ZHANG Z, LIN D. Two classes of (r, t) -locally repairable codes [C] // 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona, Spain, 2016, 445 - 449.

[16] PRAKASH N, KAMATH G M, LALITHA V, et al. Optimal linear codes with a local-error-correction property [C] // 2012 IEEE International Symposium on Information Theory Proceedings (ISIT), Cambridge, MA, USA, 2012, 2776 - 2780.

[17] CAI H, MIAO Y, SCHWARTZ M, et al. On optimal locally repairable codes with multiple disjoint repair sets [J]. IEEE Transactions on Information Theory, 2020, 66 (4): 2402 - 2416.

[18] HAO J, SHUM K W, XIA S T, et al. Optimal locally repairable codes for parallel reading [J]. IEEE Access, 2020, 8: 80447 - 80453.

[19] TAN P, ZHOU Z C, SIDORENKO V, et al. Two classes of optimal LRCs with information (r, t) -locality [J]. Designs, Codes and Cryptography, 2020, 88 (9): 1741 - 1757.

[20] HAO J, XIA S T, and CHEN B. On the single-parity locally repairable codes with availability [C] //2016 IEEE/CIC International Conference on Communications in China (ICCC), Chengdu, China, 2016, 1 - 4.

[21] 汪雅馨. 多错误局部修复码的构造 [D]. 上海：华东师范大学，2023.

[22] TAN P, ZHOU Z, SIDORENKO V, et al. Two classes of optimal LRCs with information (r, t) -locality [J]. Designs, Codes and Cryptography, 2020, 88 (9): 1741 - 1757.

[23] FU Q, LI R, YANG S. Optimal (r, δ) -locally repairable codes from simplex code and cap code [J]. IEEE Access, 2020, 8: 215414 - 215418.

[24] JIN H F, TIAN Y, FU F W. Some constructions of perfect and k-optimal (r, δ) -LRCs [C] //2023 IEEE International Symposium on Information Theory (ISIT). IEEE, 2023: 1758 - 1763.

(上接第 264 页)

[28] 童　菲，李吉宗. MBSE 在汽车电子架构领域的应用研究 [J]. 机电一体化，2018，24 (2)：25 - 30.

[29] 刘自凯，庞仁勇，徐　伟，等. 基于 MBSE 的电子电气架构开发与应用研究 [J]. 汽车电器，2025 (3)：94 - 97.

[30] 陈竹梅，雷　川，龚光红，等. 效能主导的复杂电子信息系统跨域协同设计关键问题与方法论 [J]. 中国电子科学研究院学报，2020，15 (5)：403 - 414.

[31] 温志文，王　中，谢　彬，等. 基于 MBSE 的鱼雷武器装备数字化研制方法 [J]. 水下无人系统学报，2024，32 (2)：295 - 303.

[32] 秦　政，叶东明，彭祺擘. 基于模型的载人航天任务数字化协同设计 [C] //第六届体系工程学术会议论文集-体系工程与高质量发展，昆明，云南，20240802.

[33] 刘伟伟，于俊慧，穆　强，等. 一种开放式模块化星载综合电子系统的设计与实现 [J]. 遥测遥控，2023，44 (3)：53 - 60.