doi:10.3969/j.issn.1000-436x.2013.z1.009

基于 X-RDP 阵列码的一种数据分布策略

万武南[1,2]，索望[1]，陈运[2]，王拓[1]
(1. 成都信息工程学院 网络工程学院，四川 成都 610225；2. 成都信息工程学院 应用密码学研究所，四川 成都 610225)

摘 要：对双容错 RDP(row diagonal parity)码进行了扩展，提出了一种基于 X-RDP 阵列码 3 容错的数据分布策略。利用 X-RDP 码的代数定义，从理论上证明了 X-RDP 码具有 MDS 编码特性。并采用不同斜率几何直线图描述编译码过程，易于软硬件实现。与其他数据分布策略进行比较，理论分析结果表明，X-RDP 码的空间利用率、编译码效率、小写性能以及平衡性的综合性能达到最优，具有实用价值。

关键词：编码；纠删码；RDP 码；数据布局；磁盘阵列
中图分类号：TP333 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0067-09

Data distribution strategy based on the X-RDP array codes

WAN Wu-nan[1,2], SUO Wang[1], CHEN Yun[2], WANG Tuo[1]
(1. Network Engineering Department, Chengdu University of Information Technology, Chengdu 610225, China;
2. Institute of Applied Cryptograph, Chengdu University of Information Technology, Chengdu 610225, China)

Abstract: A data distribution strategy based on the X-RDP code was presented for correcting triple storage failures, which is an extension of the double-erasure-correcting RDP code. A theoretical proof that the X-RDP code is an MDS code was given by using algebraic definition. The encoding and decoding procedures were described by geometrical line graphs, which were easily implemented by soft hardware. The theoretical analysis shows that the comprehensive properties of the X-RDP codeis better than other popular MDS codes in encoding and decoding efficiency, small writes and balance performance, thus the X-RDP code is practically meaningful for storage systems.

Key words: coding; erasure-correcting code; RDP code; data placement; RAID

1 引言

目前，分布式存储系统在硬盘级的数据容错技术大多采用基于单容错或双容错的数据分布策略来提高系统可靠性[1,2]。双容错数据布局策略已经有许多研究，文献[3~8]分别提出了 EVENODD 码[3]、X 码[4]、B 码[5]、C 码[6]、RDP 码[7]、H 码[8]，编译码只需要异或运算，并具有 MDS 编码特性，数据冗余率达到了最优。但随着海量存储系统的发展，存储介质急剧增大，设备发生损毁的概率也越来越大，因此单容错和双容错数据分布策略已经无法满足存储系统可靠性的要求，研究 3 容错、多容错的数据分布策略已成为硬盘级数据容错技术的一个重要研究问题。

在 3 容错和多容错数据分布策略研究方面，文献[9~11]提出了 GRID[9]、HoVer 码[10]、WEAVER 码[11]能够纠 4 个以上错误的阵列编码布局，但是这 3 类编码都不具有 MDS 编码特性，空间利用率只有大概 50%。FENG G L 等人在文献[12,13]中提出了 2 种新的能够承受 3 个和多个存储介质同时故障的 2 类阵列编码，分别是由类似于范德蒙矩阵和柯西矩阵来构造的，编译码结构不易软硬件实现。文献[14,15]提出的 Blaum 码[14]和 T 码[15]是低密度奇偶 MDS 码，理论上能够容许多个错误，但是其译码方法不易实现。Tau 在文献[16]中提出了 HDD1 码和 HDD2 码，MDS 编码特性证明不充分，译码过程是基于高斯三

收稿日期：2013-06-21
基金项目：国家自然科学基金资助项目（60873216）；四川省教育厅重点基金资助项目（12ZA223）
Foundation Items: The National Natural Science Foundation of China (60873216); Key Project of Sichuan Provincial Department of Education (12ZA223)

角的矩阵变换，其译码复杂度高。文献[17,18]分别提出了在EVENODD码的基础进行扩展的2类3容错MDS阵列码STAR码[17]和EEOD码[18]，但这2类编码继承了EVENODD码小写分布不平衡特性，容易造成I/O瓶颈。

CORBETT P等人提出了一种基于RDP码的双容错数据分布策略，RDP码的编译码效率和小写能力平衡性都要优于EVENODD码的数据布局策略，得到了双容错数据布局的最优[7]。因此在RDP码的基础上，增加1校验列，提出了一种基于X-RDP码的数据分布策略，保留了RDP码具有小写性能均衡和编码特性最优的特性，能够同时容许3个存储设备出错。并理论上证明X-RDP是容3错MDS码。并采用不同斜率几何直线图描述法给出了编译码算法，易于软硬件实现。并与其他3容错数据分布策略相比，X-RDP码的空间利用率、编译码效率、更新率的综合性能达到了最优。

2 X-RDP码的编码方法

2.1 X-RDP码

在RDP码的基础上增加了1列校验列，RDP码二维阵列结构扩展为$(m-1)\times(m+1)$，其中，前$m-1$列为源数据单元，后3列为校验数据单元。前2列校验数据单元的编码规则与RDP码完全一样，增加的最后1列校验列与第2列校验列编码规则类似，3列校验各数据单元的构造公式如式(1)~式(3)所示。

$$c_{u,m-1}=\bigoplus_{t=0}^{m-2}c_{u,t} \tag{1}$$

$$c_{u,m}=\bigoplus_{\substack{t=0\\ t\neq u+1}}^{m-1}c_{\langle u-t\rangle_m,t} \tag{2}$$

$$c_{u,m+1}=\bigoplus_{\substack{t=0\\ t\neq u-1}}^{m-1}c_{\langle u+t\rangle_m,t} \tag{3}$$

其中，m表示大于2的素数，$\langle x\rangle_m=x(\mathrm{mod}\,m)$，$c_{i,j}$表示为第$i$行第$j$列的源数据单元或者校验单元。根据编码的式(1)~式(3)，表1给出了$m=5$时，X-RDP码的编码实例。

2.2 X-RDP码编码过程的几何描述

X-RDP码的二维阵列结构的每个源数据单元可以看作平面坐标系上的点，则根据X-RDP码的编码的式(1)~式(3)，X-RDP码的3列校验数据单元构造公式可分别用几何直线斜率为0、1、−1的直线图描述（如图1所示）。为了描述更直观，增加1行虚拟行(实际并不存在)，该行虚拟单元的数据都假设为0，即$c_{m-1,i}=0\,(0\leqslant i\leqslant m+1)$。图1给出了$m$=5时，X-RDP码的3列校验列的几何结构。

从图1中可以很清楚地看出，第1列水平校验列的校验单元构造的几何特性就是沿着斜率为0的直线所经过的前$m-2$列的数据单元的异或值，第2列斜校验列校验单元则从左下到右上45°的斜率为1的直线经过前$m-1$列的数据单元的异或值，称为“正斜校验列”。第3列斜校验列校验单元从左上到右上45°的斜率为−1的直线经过前$m-1$列的数据单元的异或值，称为“反斜校验列”。正斜校验列与反斜校验列形状如“X”，因此称扩展RDP码为X-RDP码。从图1可以看出最后两斜校验列需要水平校验列的数据单元进行异或，因此在编码过程中，需要首先构造水平校验列，才能构造后两校验列。

2.3 XRDP阵列码编码的代数定义

为了证明X-RDDP码具有MDS编码性质，引入与上述几何直线描述方法等价的代数编码表示方法，给出理论上的证明。预先给出相关矩阵的定义。

定义1 在GF(2)有限域上，定义矩阵集$\{\boldsymbol{I}_m,\boldsymbol{E}_m,\boldsymbol{E}_m^2,\cdots,\boldsymbol{E}_m^{m-1}\}$，$\boldsymbol{E}_m^{\alpha}$是一个$m\times m$矩阵，矩阵$\boldsymbol{E}_m^{\alpha}=(\boldsymbol{e}_{i,j})_{m\times m}$，$e_{i,j}$定义如式(4)所示。

$$e_{i,j}=\begin{cases}1, i=\langle j+\mu\rangle_m\\ 0,\text{其他}\end{cases} \tag{4}$$

其中，$\boldsymbol{E}_m^m=\boldsymbol{I}_m,\boldsymbol{E}_m^{-1}=\boldsymbol{E}_m^{m-1},\boldsymbol{E}_m^{-\alpha}=\boldsymbol{E}_m^{m-\alpha}$，$\boldsymbol{I}_m$是$m\times m$的单位矩阵，而$\boldsymbol{E}_m$是$m\times m$矩阵，如式(5)所示。

$$\boldsymbol{E}_m=\begin{bmatrix}0&0&\cdots&0&1\\1&0&\cdots&0&0\\0&1&\cdots&0&0\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&0&1&0\end{bmatrix} \tag{5}$$

定义2 $\boldsymbol{Q}_{m\times(m-1)}$分别是$m\times(m-1)$、$(m-1)\times m$矩阵，具体如式(6)、式(7)所示。

$$\widetilde{\boldsymbol{Q}}_{(m-1)\times m}=\begin{bmatrix}\boldsymbol{I}_{m-1} & \overrightarrow{\boldsymbol{0}}_{m-1}^{\mathrm{T}}\end{bmatrix} \tag{6}$$

表 1　　**X-RDP 码的编码实例($m=5$)**

数据源				校验数据		
C_{i0}	C_{i1}	C_{i2}	C_{i3}	C_{i4}	C_{i5}	C_{i6}
C_{00}	c_{01}	c_{02}	c_{03}	$c_{04}=c_{00}\oplus c_{01}\oplus c_{02}\oplus c_{03}$	$c_{05}=c_{14}\oplus c_{23}\oplus c_{32}\oplus c_{00}$	$c_{06}=c_{33}\oplus c_{22}\oplus c_{11}\oplus c_{00}$
c_{10}	c_{11}	c_{12}	c_{13}	$c_{14}=c_{10}\oplus c_{11}\oplus c_{12}\oplus c_{13}$	$c_{15}= c_{24}\oplus c_{33}\oplus c_{01}\oplus c_{10}$	$c_{16}= c_{04}\oplus c_{32}\oplus c_{21}\oplus c_{10}$
c_{20}	c_{21}	c_{22}	c_{23}	$c_{24}=c_{20}\oplus c_{21}\oplus c_{22}\oplus c_{23}$	$c_{25}= c_{34}\oplus c_{02}\oplus c_{11}\oplus c_{20}$	$c_{26}=c_{14}\oplus c_{03}\oplus c_{31}\oplus c_{20}$
c_{30}	c_{31}	c_{32}	c_{33}	$c_{34}=c_{30}\oplus c_{31}\oplus c_{32}\oplus c_{33}$	$c_{35}=c_{03}\oplus c_{12}\oplus c_{21}\oplus c_{30}$	$c_{36}=c_{24}\oplus c_{13}\oplus c_{02}\oplus c_{30}$

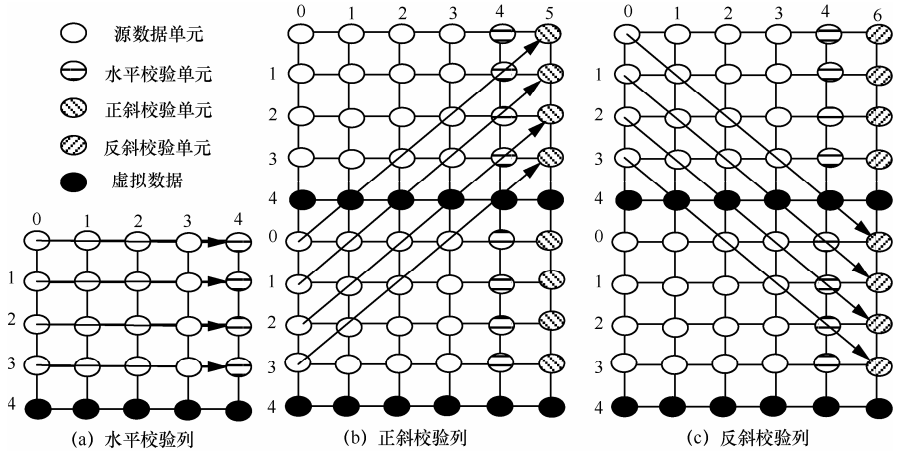

图 1　X-RDP 编码几何结构

$$\boldsymbol{Q}_{m\times(m-1)}=\begin{bmatrix}\boldsymbol{I}_{m-1}\\ \vec{\boldsymbol{0}}_{m-1}\end{bmatrix}\overrightarrow{\boldsymbol{c}_{m-1}}\ (m-1)\times(m-1)\qquad(7)$$

其中，$\boldsymbol{I}_{m-1}$ 是单位矩阵，$\vec{\boldsymbol{0}}_{m-1}$ 是 $1\times(m-1)$ 的零向量，$\vec{\boldsymbol{0}}_{m-1}^{\mathrm{T}}$ 是 $(m-1)\times1$ 全 0 的向量。

为了描述方便，矩阵 E_m^{α}、$\widetilde{\boldsymbol{Q}}_{(m-1)\times m}$、$\boldsymbol{Q}_{m\times(m-1)}$ 下标省略，简写为 $\boldsymbol{E}^{\alpha}$、$\widetilde{\boldsymbol{Q}}$、$\boldsymbol{Q}$。

X-RDP 码的二维阵列矩阵中每列数据单元可以分别记为 $\vec{\boldsymbol{c}}_0,\vec{\boldsymbol{c}}_1,\cdots,\overrightarrow{\boldsymbol{c}_{m-1}},\vec{\boldsymbol{c}}_m,\overrightarrow{\boldsymbol{c}_{m+1}}$，而 $\vec{\boldsymbol{c}}_0,\vec{\boldsymbol{c}}_1,\cdots,\overrightarrow{\boldsymbol{c}_{m-2}}$ 为 $m-1$ 列源数据列，$\overrightarrow{\boldsymbol{c}_{m-1}}$、$\vec{\boldsymbol{c}}_m$、$\overrightarrow{\boldsymbol{c}_{m+1}}$ 为 3 列校验列。其中，每列数据单元可记为 $\vec{\boldsymbol{c}}_i=[\boldsymbol{c}_{0,i},\boldsymbol{c}_{1,i},\cdots,\boldsymbol{c}_{m-1,i}]^{\mathrm{T}}$，$0\leqslant i\leqslant m+1$。根据 2.1 节中 X-RDP 码的编码规则，X-RDP 码的编码规则代数定义如式(8)所示。

$$\begin{bmatrix}\overrightarrow{\boldsymbol{c}_{m-1}}\\ \vec{\boldsymbol{c}}_m\\ \overrightarrow{\boldsymbol{c}_{m+1}}\end{bmatrix}=\boldsymbol{G}\times\begin{bmatrix}\vec{\boldsymbol{c}}_0\\ \vec{\boldsymbol{c}}_1\\ \vdots\\ \overrightarrow{\boldsymbol{c}_{m-2}}\end{bmatrix}\qquad(8)$$

其中，$\boldsymbol{G}$ 为 X-RDP 码的生成矩阵，如式(9)所示。

$$\boldsymbol{G}=\begin{bmatrix}\boldsymbol{I}_{m-1} & \boldsymbol{I}_{m-1} & \boldsymbol{I}_{m-1} & \cdots & \boldsymbol{I}_{m-1}\\ \boldsymbol{I}_{m-1}+\boldsymbol{E}^{-1} & \widetilde{\boldsymbol{Q}}(\boldsymbol{E}+\boldsymbol{E}^{-1})\boldsymbol{Q} & \widetilde{\boldsymbol{Q}}(\boldsymbol{E}^{2}+\boldsymbol{E}^{-1}) & \cdots & \widetilde{\boldsymbol{Q}}\widetilde{\boldsymbol{Q}}(\boldsymbol{E}^{m-2}+\boldsymbol{E}^{-1})\boldsymbol{Q}\\ \boldsymbol{I}_{m-1}+\boldsymbol{E} & \widetilde{\boldsymbol{Q}}(\boldsymbol{E}^{-1}+\boldsymbol{E})\boldsymbol{Q} & \widetilde{\boldsymbol{Q}}(\boldsymbol{E}^{-2}+\boldsymbol{E}) & \cdots & \widetilde{\boldsymbol{Q}}\widetilde{\boldsymbol{Q}}(\boldsymbol{E}^{2-m}+\boldsymbol{E})\boldsymbol{Q}\end{bmatrix}\qquad(9)$$

2.4　X-RDP 码 MDS 性质

根据 2.3 节 X-RDP 码的代数描述，下面从数学理论上给出 X-RDP 码的 MDS 性质证明。

定理 1　当且仅当 m 为素数时，X-RDP 码的最小汉明列距离为 4，即 $d_{\min}=4$。

证明　X-RDP 码是一类线性码，根据编码理论，码的最小列重量等于码的最小列距离。要证明 X-RDP 码的最小距离 $d_{\min}=4$，即只要证明 X-RDP 码的最小列重量为 4 即可。

1) X-RDP 码是在 RDP 码基础上进行扩展，而 RDP 码是容双错阵列码，并具有 MDS 性质,即 RDP 码的最小列重量为 3，即最小汉明距离为 3，因此 X-RDP 码的最小列距 $d_{\min}\geqslant3$。

2) X-RDP 码的最小列距离不可能等于 3，即 $d_{\min}\neq3$。

采用反证法。假设 X-RDP 码的最小列距离等于 3 成立。即假设 X-RDP 码任意非零有效码字至少有 3 列非零数据列成立。现假设 X-RDP 码码字中非零列列号 $0\leqslant u_1<u_2<u_3\leqslant m+2$，其余列全为零数据列。根据 2.3 节码的生成公式，有如下 3 种情况。

①假设 3 列非零列向量 $0\leqslant u_1<u_2<u_3\leqslant m-1$，即全部是源数据单元列，那么校验单元列全部为零列向量。则根据编码规则可知式(10)成立。

$$\boldsymbol{AX}=\begin{bmatrix}\tilde{\boldsymbol{Q}}\boldsymbol{Q} & \tilde{\boldsymbol{Q}}\boldsymbol{Q} & \tilde{\boldsymbol{Q}}\boldsymbol{Q}\\ \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q} & \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{u_2}+\boldsymbol{E}^{-1})\boldsymbol{Q} & \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{u_3}+\boldsymbol{E}^{-1})\boldsymbol{Q}\\ \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{-u_1}+\boldsymbol{E})\boldsymbol{Q} & \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{-u_2}+\boldsymbol{E})\boldsymbol{Q} & \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{-u_3}+\boldsymbol{E})\boldsymbol{Q}\end{bmatrix}\times\begin{bmatrix}\overrightarrow{\boldsymbol{c}_{u_1}}\\ \overrightarrow{\boldsymbol{c}_{u_2}}\\ \overrightarrow{\boldsymbol{c}_{u_3}}\end{bmatrix}=\begin{bmatrix}\overrightarrow{\boldsymbol{c}_{m-1}}\\ \overrightarrow{\boldsymbol{c}_{m}}\\ \overrightarrow{\boldsymbol{c}_{m+1}}\end{bmatrix}=\begin{bmatrix}\overrightarrow{\boldsymbol{0}_{m-1}}\\ \overrightarrow{\boldsymbol{0}_{m-1}}\\ \overrightarrow{\boldsymbol{0}_{m-1}}\end{bmatrix}\tag{10}$$

式(10)可以看作是 $\boldsymbol{AX}=0$ 矩阵方程形式，而又因为根据引理 2(见附录)可知，生成矩阵 $\boldsymbol{G}$ 可逆，根据矩阵的性质可知，若 $\boldsymbol{A}$ 可逆，$\boldsymbol{AX}=0$ 没有非零解，即 $\boldsymbol{X}$ 必须为零列向量。但这与假设三列源数据单元列 $\left[\overrightarrow{\boldsymbol{c}_{u_1}},\overrightarrow{\boldsymbol{c}_{u_2}},\overrightarrow{\boldsymbol{c}_{u_3}}\right]^{\mathrm{T}}$ 构成非零列向量相矛盾，所以假设不成立。

②假设 3 列非零列有 1 列是源数据列，2 列校验列，其余列为零列向量。设源数据列为 u_1 列，则根据编码规则可知式(11)成立。

$$\begin{bmatrix}\overrightarrow{\boldsymbol{c}_{m-1}}\\ \overrightarrow{\boldsymbol{c}_{m}}\\ \overrightarrow{\boldsymbol{c}_{m+1}}\end{bmatrix}=\begin{bmatrix}\tilde{\boldsymbol{Q}}\boldsymbol{Q}\\ \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q}\\ \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{-u_1}+\boldsymbol{E})\boldsymbol{Q}\end{bmatrix}\times\left[\overrightarrow{\boldsymbol{c}_{u_1}}\right]=\begin{bmatrix}\tilde{\boldsymbol{Q}}\boldsymbol{Q}\overrightarrow{\boldsymbol{c}_{u_1}}\\ \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q}\overrightarrow{\boldsymbol{c}_{u_1}}\\ \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{-u_1}+\boldsymbol{E})\boldsymbol{Q}\overrightarrow{\boldsymbol{c}_{u_1}}\end{bmatrix}\tag{11}$$

根据假设条件可知 $\tilde{\boldsymbol{Q}}\boldsymbol{Q}\overrightarrow{\boldsymbol{c}_{u_1}}$、$\tilde{\boldsymbol{Q}}\boldsymbol{E}^{u_1}\boldsymbol{Q}\overrightarrow{\boldsymbol{c}_{u_1}}$、$\tilde{\boldsymbol{Q}}\boldsymbol{E}^{2u_1}\boldsymbol{Q}\overrightarrow{\boldsymbol{c}_{u_1}}$ 3 个式子中，至少有 2 个式子满足 $\boldsymbol{AX}=0$ 矩阵方程形式，而任意矩阵 $\tilde{\boldsymbol{Q}}\boldsymbol{Q}$、$\tilde{\boldsymbol{Q}}\boldsymbol{E}^{u_1}\boldsymbol{Q}$、$\tilde{\boldsymbol{Q}}\boldsymbol{E}^{2u_1}\boldsymbol{Q}$ 的秩都是 $m-1$，即都为可逆矩阵，因此 $\boldsymbol{X}$ 必须为零列向量，即 $\overrightarrow{\boldsymbol{c}_{u_1}}$ 为零列向量，但是这与假设相矛盾，所以假设不成立.

③假设 3 列非零列有 2 列是源数据单元列，1 列校验单元列，其余列为零列向量。设非零列信息列为 u_1,u_2 列，则根据编码规则可知式(12)成立。

$$\begin{bmatrix}\overrightarrow{\boldsymbol{c}_{m-1}}\\ \overrightarrow{\boldsymbol{c}_{m}}\\ \overrightarrow{\boldsymbol{c}_{m+1}}\end{bmatrix}=\begin{bmatrix}\tilde{\boldsymbol{Q}}\boldsymbol{Q} & \tilde{\boldsymbol{Q}}\boldsymbol{Q}\\ \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q} & \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{u_2}+\boldsymbol{E}^{-1})\boldsymbol{Q}\\ \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{-u_1}+\boldsymbol{E})\boldsymbol{Q} & \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{-u_2}+\boldsymbol{E})\boldsymbol{Q}\end{bmatrix}\begin{bmatrix}\overrightarrow{\boldsymbol{c}_{u_1}}\\ \overrightarrow{\boldsymbol{c}_{u_2}}\end{bmatrix}\tag{12}$$

那么 $\overrightarrow{\boldsymbol{c}_{m}}$、$\overrightarrow{\boldsymbol{c}_{m+1}}$、$\overrightarrow{\boldsymbol{c}_{m+2}}$ 3 列校验列有 2 列为零列向量，则式(13)~式(15)中的某一式成立。

$$\begin{bmatrix}\overrightarrow{\boldsymbol{c}_{m-1}}\\ \overrightarrow{\boldsymbol{c}_{m}}\end{bmatrix}=\begin{bmatrix}\tilde{\boldsymbol{Q}}\boldsymbol{Q} & \tilde{\boldsymbol{Q}}\boldsymbol{Q}\\ \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q} & \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{u_2}+\boldsymbol{E}^{-1})\boldsymbol{Q}\end{bmatrix}\begin{bmatrix}\overrightarrow{\boldsymbol{c}_{u_1}}\\ \overrightarrow{\boldsymbol{c}_{u_2}}\end{bmatrix}=\begin{bmatrix}\overrightarrow{\boldsymbol{0}_{m-1}}\\ \overrightarrow{\boldsymbol{0}_{m-1}}\end{bmatrix}\tag{13}$$

$$\begin{bmatrix}\overrightarrow{\boldsymbol{c}_{m-1}}\\ \overrightarrow{\boldsymbol{c}_{m+1}}\end{bmatrix}=\begin{bmatrix}\tilde{\boldsymbol{Q}}\boldsymbol{Q} & \tilde{\boldsymbol{Q}}\boldsymbol{Q}\\ \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{-u_1}+\boldsymbol{E})\boldsymbol{Q} & \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{-u_2}+\boldsymbol{E})\boldsymbol{Q}\end{bmatrix}\begin{bmatrix}\overrightarrow{\boldsymbol{c}_{u_1}}\\ \overrightarrow{\boldsymbol{c}_{u_2}}\end{bmatrix}=\begin{bmatrix}\overrightarrow{\boldsymbol{0}_{m-1}}\\ \overrightarrow{\boldsymbol{0}_{m-1}}\end{bmatrix}\tag{14}$$

$$\begin{bmatrix}\overrightarrow{\boldsymbol{c}_{m}}\\ \overrightarrow{\boldsymbol{c}_{m+1}}\end{bmatrix}=\begin{bmatrix}\tilde{\boldsymbol{Q}}(\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q} & \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{u_2}+\boldsymbol{E}^{-1})\boldsymbol{Q}\\ \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{-u_1}+\boldsymbol{E})\boldsymbol{Q} & \tilde{\boldsymbol{Q}}(\boldsymbol{E}^{-u_2}+\boldsymbol{E})\boldsymbol{Q}\end{bmatrix}\begin{bmatrix}\overrightarrow{\boldsymbol{c}_{u_1}}\\ \overrightarrow{\boldsymbol{c}_{u_2}}\end{bmatrix}=\begin{bmatrix}\overrightarrow{\boldsymbol{0}_{m-1}}\\ \overrightarrow{\boldsymbol{0}_{m-1}}\end{bmatrix}\tag{15}$$

同理根据矩阵的性质可知，$\boldsymbol{AX}$ =0 时，若 $\boldsymbol{A}$ 可逆，方程没有非零解，即 $\boldsymbol{X}$ 肯定等于 0。又因为根据引理 2(见附录)可知，X-RDP 码任意子矩阵都是可逆矩阵,即 $\left[\overrightarrow{\boldsymbol{c}_{u_1}},\overrightarrow{\boldsymbol{c}_{u_2}}\right]^{\mathrm{T}}$ 为零列向量，但这与假设矛盾。

因此根据①、②、③可知，X-RDP 码不可能出现码的最小列重量为 3 有效码字的情况，即最小列距离不可能等于 3，即 $d_{\min}\neq 3$。

因此根据 1)、2)，很容易可得：X-RDP 码的最小列距离 $d_{\min}=4$。证毕。

3 X-RDP 码译码算法

在存储系统，哪个存储节点出错是预先知道的，也就是在 X-RDP 码的二维阵列中，事先知道出错列的位置。X-RDP 码的译码过程主要可分为 2 种情况，第 1 种失效源数据单元为 2 列，此时 X-RDP 可以采用类似 RDP 容双错译码算法，在此不再详述。第 2 种情况失效 3 列都是源数据列，校验列没有数据失效，译码过程如下。

假设失效源数据列分为 i、j、k 3 列($0\leqslant i<j<k\leqslant m-2$)。

Step1 利用数据未失效的 3 列校验列的校验单元，根据编码式(1)~式(3)计算出每个校验单元的校验算子，校验算子分别记为：$S^{(0)}=(S_0^{(0)},S_1^{(0)},\cdots,S_{m-1}^{(0)})$，$S^{(1)}=(S_0^{(1)},S_1^{(1)},\cdots,S_{m-1}^{(1)})$，$S^{(2)}=(S_0^{(2)},S_1^{(2)},\cdots,S_{m-1}^{(2)})$，校验算子计算公式如式(16)~式(18)所示。

$$S_u^{(0)}=c_{u,m-1}\oplus\bigoplus_{\substack{t=0\\ t\neq i,j,k}}^{m-2}c_{u,t}\tag{16}$$

$$S_u^{(1)}=c_{u,m}\oplus\left(\bigoplus_{\substack{t=0\\ t\neq i,j,k}}^{m-1}c_{\langle t-u\rangle_m,u}\right)\tag{17}$$

$$S_u^{(2)}=c_{u,m+1}\oplus\left(\bigoplus_{\substack{t=0\\ t\neq i,j,k}}^{m-1}c_{\langle t+u\rangle_m,u}\right)\tag{18}$$

其中，$0 \leqslant u \leqslant m-2$。并且 $S_{m-1}^{(1)} = \left(\bigoplus_{t=0}^{m-2} c_{t,m} \right) \oplus c_{0,m-1}$ 和 $S_{m-1}^{(2)} = \left(\bigoplus_{t=0}^{m-2} c_{t,m+1} \right) \oplus c_{m-2,m-1}$。

根据 X-RDP 码的校验列编码的几何结构，校验算子计算式(16)~式(18)可以用几何直线图来描述。图 2 给出了 $m=5$，失效源数据列 $i=0$、j=1、k=3 时，3 组校验算子几何直线构造图。图中每条直线对应着式(12)~式(14)的校验算子。从图中可以直观地看出每条直线至多只含 3 个失效数据单元，并且只含每列失效数据列 1 个失效数据单元。

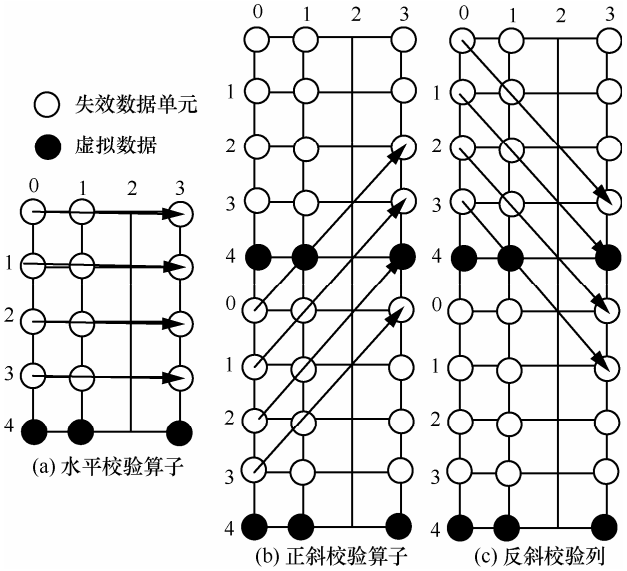

图 2　校验算子几何结构

Step2　式(12)~式(14)校验算子可以看作方程组，方程的变量为失效的数据单元。则可以通过式(19)或式(20)变换，得到只含有失效中间列 j 列的变换式子，并且每个变换方程至多只有 2 个变量，因此可以根据这组变换方程依次把第 j 列的信息位求解出来。假设：$0 \leqslant u \leqslant m-1$，$\beta_1 = j-i, \beta_2 = k-j$，则一定存在 l_d，l_h $(1 \leqslant l_d, l_h < m)$，满足：$\langle \beta_1 - l_d \beta_2 \rangle_m = 0$，$\langle \beta_1 + l_h \beta_2 \rangle_m = 0$，式(19)和式(20)成立。

$$c_{u,j} \oplus c_{\langle u+2\beta_1 \rangle_m, j} = \sum_{v=0}^{l_d-1} \begin{pmatrix} S_{\langle u+v\beta_2 \rangle_m}^{(0)} \oplus S_{\langle u+k+v\beta_2 \rangle_m}^{(1)} \oplus \\ S_{\langle u+\beta_1+(v+1)\beta_2-k \rangle_m}^{(2)} \oplus S_{\langle u+\beta_1+(v+1)\beta_2 \rangle_m}^{(0)} \end{pmatrix} \tag{19}$$

$$c_{u,j} \oplus c_{\langle u+2\beta_1 \rangle_m, j} = \sum_{v=0}^{l_h-1} \begin{pmatrix} S_{\langle u-(v+1)\beta_2 \rangle_m}^{(0)} \oplus S_{\langle u+k-(v+1)\beta_2 \rangle_m}^{(1)} \oplus \\ S_{\langle u+\beta_1-v\beta_2-k \rangle_m}^{(2)} \oplus S_{\langle u+\beta_1-v\beta_2 \rangle_m}^{(0)} \end{pmatrix} \tag{20}$$

式(19)和式(20)成立的证明方法完全一样，本文只给出式(19)的详细证明。

证明　根据校验子计算公式，对 $0 \leqslant u \leqslant m-1$，可得式(21)~式(24)成立。

$$S_u^{(0)} = c_{u,i} \oplus c_{u,j} \oplus c_{u,k} \tag{21}$$

$$S_{\langle u+k \rangle_m}^{(1)} = c_{\langle u+\beta_2+\beta_1 \rangle_m, i} \oplus c_{\langle u+\beta_2 \rangle_m, j} \oplus c_{u,k} \tag{22}$$

$$S_{\langle u+\beta_1+\beta_2-k \rangle_m}^{(2)} = c_{u,i} \oplus c_{\langle u+\beta_1 \rangle_m, j} \oplus c_{\langle u+\beta_1+\beta_2 \rangle_m, k} \tag{23}$$

$$S_{\langle u+\beta_1+\beta_2 \rangle_m}^{(0)} = c_{\langle u+\beta_1+\beta_2 \rangle_m, i} \oplus c_{\langle u+\beta_1+\beta_2 \rangle_m, j} \oplus c_{\langle u+\beta_1+\beta_2 \rangle_m, k} \tag{24}$$

因此，可得只含 j 的数据单元式(25)成立。

$$c_{u,j} \oplus c_{\langle u+\beta_2 \rangle_m, j} \oplus c_{\langle u+\beta_1+\beta_2 \rangle_m, j} \oplus c_{\langle u+\beta_2 \rangle_m, j} = \widetilde{S}_{\langle u \rangle_m}^{(0)} \oplus \widetilde{S}_{\langle u+k \rangle_m}^{(1)} \oplus \widetilde{S}_{\langle u+\beta_1+\beta_2-k \rangle_m}^{(2)} \oplus \widetilde{S}_{\langle u+\beta_1+\beta_2 \rangle_m}^{(0)} \tag{25}$$

因此，

$$\begin{aligned} &\sum_{v=0}^{l_d-1} \begin{pmatrix} S_{\langle u+v\beta_2 \rangle_m}^{(0)} \oplus S_{\langle u+k+v\beta_2 \rangle_m}^{(1)} \oplus \\ S_{\langle u+\beta_1+(v+1)\beta_2-k \rangle_m}^{(2)} \oplus S_{\langle u+\beta_1+(v+1)\beta_2 \rangle_m}^{(0)} \end{pmatrix} \\ = \; & c_{u,j} \oplus \not{c}_{\langle u+\beta_2 \rangle_m, j} \oplus \not{c}_{\langle u+\beta_2 \rangle_m, j} \oplus \not{c}_{\langle u+2\beta_2 \rangle_m, j} \oplus c_{\langle u+\beta_1 \rangle_m, j} \oplus \not{c}_{\langle u+\beta_1+\beta_2 \rangle_m, j} \oplus \not{c}_{\langle u+\beta_1+\beta_2 \rangle_m, j} \oplus \not{c}_{\langle u+\beta_1+2\beta_2 \rangle_m, j} \oplus \\ & \cdots \oplus \not{c}_{\langle u+(l_d-2)\beta_2 \rangle_m, j} \oplus \not{c}_{\langle u+(l_d-1)\beta_2 \rangle_m, j} \oplus \\ & \cdots \oplus \not{c}_{\langle u+(l_d-1)\beta_2 \rangle_m, j} \oplus c_{\langle u+l_d\beta_2 \rangle_m, j} \oplus \\ & \cdots \oplus \not{c}_{\langle u+\beta_1+(l_d-2)\beta_2 \rangle_m, j} \oplus \not{c}_{\langle u+\beta_1+(l_d-1)\beta_2 \rangle_m, j} \oplus \\ & \cdots \oplus \not{c}_{\langle u+\beta_1+(l_d-1)\beta_2 \rangle_m, j} \oplus c_{\langle u+\beta_1+l_d\beta_2 \rangle_m, j} \end{aligned} \tag{26}$$

又因为 $\langle \beta_1 - l_d \beta_2 \rangle_m = 0$，所以 $c_{\langle u+\beta_1 \rangle_m, j} = c_{\langle u+l_d\beta_2 \rangle_m, j}$，因此式(27)成立。

$$c_{u,j} \oplus c_{\langle u+2\beta_1 \rangle_m, j} = \sum_{v=0}^{l_d-1} \begin{pmatrix} S_{\langle u+v\beta_2 \rangle_m}^{(0)} \oplus S_{\langle u+k+v\beta_2 \rangle_m}^{(1)} \oplus \\ S_{\langle u+\beta_1+(v+1)\beta_2-k \rangle_m}^{(2)} \oplus S_{\langle u+\beta_1+(v+1)\beta_2 \rangle_m}^{(0)} \end{pmatrix} \tag{27}$$

并且由于 $1 \leqslant \beta_1 = j-i \leqslant m-1$，因此 $u \neq \langle u+2\beta_1 \rangle_m$，$c_{u,j}$ 与 $c_{\langle u+2\beta_1 \rangle_m, j}$ 肯定是 j 列中 2 个不同未知数据单元。证毕。

根据 l_d, l_h，选择 2 个数之间较小的变换公式得到，只含 j 列至多只含有 2 个未知源数据单元的方程。令 $u = m-1, c_{m-1,j} = 0$，得到只含有一个未知数据单元的方程 $c_{\langle 2\beta_1 - 1 \rangle_m, j}$ 作为解码链，第 j 列源数据单元依次求解，再根据 RDP 双容错译码算法依次

恢复出其余 2 列的失效数据。

实例，假若 $m=5$，失效源数据列 $i=0$、$j=1$、$k=3$，恢复第 j 列源数据单元译码过程如图 3 所示。

从图 3 图可以看出，通过 4 个校验算子进行两轮迭代运算，最后得到只含有 j (即第 1 列)的源数据单元。图 3(a)中，4 条几何直线构成一个环路图 $a\to b\to c\to d$，对应的 4 个校验算子迭代如式(28)所示。

$$c_{1,1}\oplus c_{2,1}\oplus c_{3,1}\oplus a_{4,1}=S_1^{(0)}\oplus S_4^{(1)}\oplus S_1^{(2)}\oplus S_4^{(0)} \quad (28)$$

同理图 3(b)中，$a'\to b'\to c'\to d'$ 对应的 4 个校验算子迭代如式(29)所示。

$$a_{0,1}\oplus c_{1,1}\oplus c_{2,1}\oplus c_{3,1}=S_0^{(0)}\oplus S_3^{(1)}\oplus S_0^{(2)}\oplus S_3^{(0)} \quad (29)$$

图 3(a)和图 3(b)迭代得到式(30)。

$$c_{0,1}\oplus a_{4,1}= S_1^{(0)}\oplus S_4^{(1)}\oplus S_1^{(2)}\oplus S_4^{(0)}\oplus S_0^{(0)}\oplus S_3^{(1)}\oplus S_0^{(2)}\oplus S_3^{(0)} \quad (30)$$

又因为已知 $c_{4,1}$ 为虚拟的点，因此可以依次求出 $c_{0,1}\to c_{1,1}\to c_{2,1}\to c_{3,1}$。此实例只是为了给出译码迭代过程。

Step3 通过 Step2 把失效源数据中间列 j 恢复之后，数据源数据列只有 2 列，可以采用 RDP 容双错译码算法恢复其余 2 列失效源数据列。

4 X-RDP 码性能分析

为了分析 X-RDP 码的性能，假定每个数据块的大小为 1 bit。

4.1 空间利用率和纠删能力

基于编码的数据分布策略的空间利用率可以定义为校验数据单元与源数据单元之间的比例。X-RDP 码总共 $m+2$ 列中源数据列为 $m-1$ 列，3 列为冗余数据列，其空间利用率为$(m-1)/(m+2)$。根据编码理论中 Singleton bound 定理[19]可知，3 容错编码至少需要 3 列校验数据列，X-RDP 码具有 MDS 特性，空间利用率和纠删能力达到了 3 容错编码最优。

4.2 编译码效率

在保证数据分布策略空间利用率和纠删能力达到 3 容错编码最优的情况下，码的编译码效率是衡量数据分布策略性能的一个重要参数。X-RDP 码是一类阵列码，其编译码运算只有异或运算，因此编译效率定义为每个源信息单元编译码过程需要的平均异或次数。

根据第 2.1 节 X-RDP 码 3 列校验列每个校验单元都需要 $(m-2)$ 次异或运算，总共有 $3(m-1)$ 校验单元，因此 3 列校验列总共需要 $3(m-2)(m-1)$ 次异或运算。X-RDP 码总共有 $(m-1)^2$ 列源数据，因此编码效率为 $3-3/(m-1)$，达到了容 3 错编码最优编码效率[7]。

X-RDP 码与 Bloemer 码[20]、STAR 码、EEOD 码和 Blaum 码的纠 3 错的译码性能进行比较。根据译码效率定义，由文献[17]可知，STAR 码的译码效率为 $3+(2l_d+l_h)/m$，EEOD 码译码效率为 $3+(4l_d-2)/m$ [18]，Blaum 码的译码效率为 $3+21/m$ [14]，Bloemer 码是一类 RS 码，译码效率大约为 $3L$ (其中，L 表示有限域的大小 GF(2^L))[20]。

根据第 3 节 X-RDP 码的译码算法可知，Step1 计算 3 列校验算子需要异或次数为 $3(m-5)(m-1)+2(m-2)$，Step2 需要的异或运算次数为：$(4l_d-1)\cdot(m-1)+(m-2)$。Step3 采用 RDP 容双错译码算法恢复其余失效数据列，需要的异或次数为：$4(m-2)-1$，因此，总异或操作次数为：$(4l_d+3m-16)(m-1)+7(m-2)-1$。X-RDP 码译码效率为 $3+(4l_d-9)/m$。

5 类编码每比特源数据需要译码次数如表 2 所示。

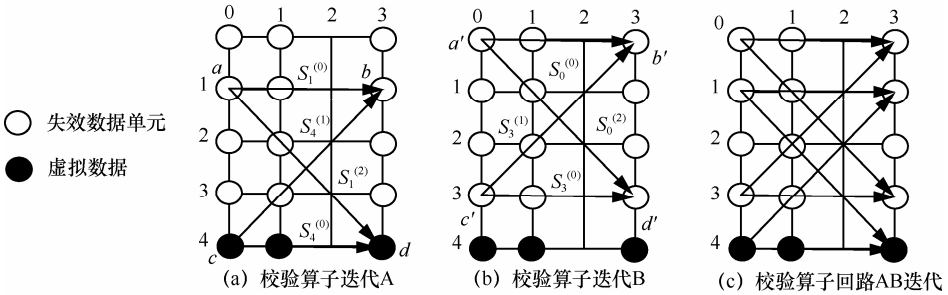

图 3 恢复中间失效数据几何示意

表 2　5 类纠删码每比特译码所需异或次数

磁盘数	Blaum 码	EEOD 码	STAR 码	X-RDP 码	Bloemer 码
5	7.2	3.62	3.55	3	9
7	6	3.68	3.714 3	3.8	9
11	4.909	3.81	3.836 4	3.533 3	12
13	4.615	3.846	3.865 4	3.8	12
17	4.235	3.882	3.900 7	3.848 5	15
19	4.105	3.894	3.912 3	3.9	15
23	3.913	3.85	3.928 9	3.926 3	15
29	3.74	3.931	3.944 6	3.952 4	15
31	3.678	3.935	3.948 4	3.956 3	15

从表 2 中可以看出，码的长度(信息列的列数) 比较短时，STAR 码、EEOD 码、X-RDP 码每比特需要的平均译码异或总数大约为 3~4，而 Blaum 码则超过 4，随着数据列数的增加，STAR 码、EEOD 码、X-RDP 码、Blaum 码趋近于 4，译码效率接近，Bloemer 码与有限域的大小 L 相关，译码复杂度最高。

4.3　小写性能平衡性的分析

存储设备的小写(small writes)定义为当一次输入数据远远小于(或等于)一个数据单元时，称为小写。当存储设备源数据单元修改时，同时需要修改与源数据单元相关联的校验单元，会带来额外的存储设备读写开销，影响系统 I/O 性能，因此在保证系统可靠性的前提下，要求所采用的数据分布策略小写，额外开销尽可能小且均衡。

根据文献[17]和文献[18]可知，STAR 码和 EEOD 码修改源数据单元不参与调节因子计算时，只与 3 个校验单元相关联，即 1 次小写需要 4 次 RMW(read modify write)操作。参与调节因子计算时，则需要 m 个校验单元相关联，则需要 $m+1$ 次 RMW 操作。不参与调节因子计算的源数据单元为 $m(m-3)$ 个，参与调节因子计算的源数据单元有 $2(m-1)$ 个，因此 STAR 码和 EEOD 码总的小写操作为 $6(m-1)(m-1)$，每个源数据的平均小写操作为 $6-1/m$。

X-RDP 码源数据单元修改，若只参与 3 个校验单元的计算，则一次小写需要 6 次 RMW，若只参与 2 个校验单元的计算，则只需要 4 次 RMW。根据 X-RDP 编码可知，参与 3 个校验单元有 $(m-1)\cdot(m-3)$，参与 2 个校验单元有 $2(m-1)$，因此总共需要 $(m-1)(6m-10)$ 次操作，因此每个数据单元平均需要的小写操作为 $6-4/(m-1)$。

随着 m 值的增大，X-RDP 码、STAR 码和 EEOD 码每个源数据修改平均小写次数为 6，小写性能接近。但是 STAR 码和 EEOD 码中，参与调节因子计算需要 $m+1$ 次，不参与计算 4 次，容易造成小写操作不均衡，影响存储系统的 I/O 性能。X-RDP 码源数据修改的小写操作为 6 次或者 4 次，小写操作没有集中到某些源数据单元，而是分散到每个源数据单元上，小写性能均衡，有利于解决系统 I/O 瓶颈问题。

5　结束语

随着物联网和云存储的发展，给出一种具有高的可靠性、高吞吐量、好 I/O 性能以及简单编译码算法的数据分布策略具有重要的实际意义和理论研究价值。本文在 RDP 码的基础上，提出了一类新的基于 X-RDP 码的数据分布策略，不但可以容许任意 3 个设备失效，而且保留了 RDP 小写性能好的特点，并且编译码复杂度和更新复杂度都相对较低。适用于实时性较强的物联网和云存储，提高了系统的可靠性。

附录：引理 1 和引理 2 的证明

引理 1　矩阵 $\widetilde{\boldsymbol{G}}$ 的任意分块子矩阵的秩为 $r(m-1)$，$1\leqslant r\leqslant 3$，$\widetilde{\boldsymbol{G}}$ 定义为

$$\widetilde{\boldsymbol{G}}=\begin{bmatrix} \boldsymbol{Q} & \boldsymbol{Q} & \boldsymbol{Q} & \cdots & \boldsymbol{Q} \\ (\boldsymbol{E}^{0}+\boldsymbol{E}^{-1})\boldsymbol{Q} & (\boldsymbol{E}+\boldsymbol{E}^{-1})\boldsymbol{Q} & (\boldsymbol{E}^{2}+\boldsymbol{E}^{-1})\boldsymbol{Q} & \cdots & (\boldsymbol{E}^{m-2}+\boldsymbol{E}^{-1})\boldsymbol{Q} \\ (\boldsymbol{E}^{0}+\boldsymbol{E}) & (\boldsymbol{E}^{-1}+\boldsymbol{E})\boldsymbol{Q} & (\boldsymbol{E}^{-2}+\boldsymbol{E})\boldsymbol{Q} & \cdots & (\boldsymbol{E}^{-(m-2)}+\boldsymbol{E})\boldsymbol{Q} \end{bmatrix} \tag{31}$$

证明　矩阵 $\widetilde{\boldsymbol{G}}$ 的任意分块子矩阵可以分为 3 种情况。

1) $\widetilde{\boldsymbol{G}}$ 的一阶子矩阵为 $\boldsymbol{Q}$、$(\boldsymbol{E}^{-1}+\boldsymbol{E}^{\mu})\boldsymbol{Q}$、$(\boldsymbol{E}^{\mu}+\boldsymbol{E}^{-1})\boldsymbol{Q}$，其中，$0\leqslant\mu\leqslant m-1$，根据定义 1 和定义 2 可知此一阶子矩阵的秩都为 $m-1$，即一阶分块子矩阵秩为 $m-1$。

2) $\widetilde{\boldsymbol{G}}$ 的二阶子分块子矩阵有 3 种情况。

① 若二阶分块子矩阵由第 1 行和第 2 行构成，则可以表示为

$$\widetilde{\boldsymbol{G}_2}=\begin{bmatrix} \boldsymbol{Q} & \boldsymbol{Q} \\ (\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q} & (\boldsymbol{E}^{u_2}+\boldsymbol{E}^{-1})\boldsymbol{Q} \end{bmatrix} \tag{32}$$

则式(32)左右两边乘以一个矩阵，结果为

$$\begin{bmatrix} \boldsymbol{I} & 0 \\ (\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1}) & \boldsymbol{I} \end{bmatrix}\times\begin{bmatrix} \boldsymbol{Q} & \boldsymbol{Q} \\ (\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q} & (\boldsymbol{E}^{u_2}+\boldsymbol{E}^{-1})\boldsymbol{Q} \end{bmatrix} =\begin{bmatrix} \boldsymbol{Q} & \boldsymbol{Q} \\ 0 & \boldsymbol{E}^{u_1}(\boldsymbol{E}^{u_2-u_1}+\boldsymbol{I})\boldsymbol{Q} \end{bmatrix} \tag{33}$$

因为矩阵 $\boldsymbol{Q}$、$\boldsymbol{E}^{u_1}(\boldsymbol{E}^{u_2-u_1}+\boldsymbol{I})\boldsymbol{Q}$ 的秩为 $2(m-1)$[18]，因此可知 $\widetilde{\boldsymbol{G}}_2$ 的秩也为 $2(m-1)$。

② 若二阶分块子矩阵由第 1 行和第 3 行构成，则可以表示为

$$\widetilde{\boldsymbol{G}}_2=\begin{bmatrix}\boldsymbol{Q} & \boldsymbol{Q}\\ (\boldsymbol{E}^{-u_1}+\boldsymbol{E})\boldsymbol{Q} & (\boldsymbol{E}^{-u_2}+\boldsymbol{E})\boldsymbol{Q}\end{bmatrix} \tag{34}$$

式(34)同样左乘一个矩阵结果为

$$\begin{bmatrix}\boldsymbol{I} & 0\\ (\boldsymbol{E}^{-u_1}+\boldsymbol{E}) & \boldsymbol{I}\end{bmatrix}\times\begin{bmatrix}\boldsymbol{Q} & \boldsymbol{Q}\\ (\boldsymbol{E}^{-u_1}+\boldsymbol{E})\boldsymbol{Q} & (\boldsymbol{E}^{-u_2}+\boldsymbol{E})\boldsymbol{Q}\end{bmatrix}=\begin{bmatrix}\boldsymbol{Q} & \boldsymbol{Q}\\ 0 & \boldsymbol{E}^{-u_2}(\boldsymbol{E}^{u_2-u_1}+\boldsymbol{I})\boldsymbol{Q}\end{bmatrix} \tag{35}$$

同理可得 $\widetilde{\boldsymbol{G}}_2$ 的秩也为 $2(m-1)$。

③ 若二阶分块子矩阵由第 2 行和第 3 行矩阵构成，则可以表示为

$$\begin{bmatrix}(\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q} & (\boldsymbol{E}^{u_2}+\boldsymbol{E}^{-1})\boldsymbol{Q}\\ (\boldsymbol{E}^{-u_1}+\boldsymbol{E})\boldsymbol{Q} & (\boldsymbol{E}^{-u_2}+\boldsymbol{E})\boldsymbol{Q}\end{bmatrix} \tag{36}$$

式(36)同样如下左乘一个矩阵结果为

$$\begin{bmatrix}\boldsymbol{I} & 0\\ \boldsymbol{E}^{1-u_1} & \boldsymbol{I}\end{bmatrix}\times\begin{bmatrix}(\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q} & (\boldsymbol{E}^{u_2}+\boldsymbol{E}^{-1})\boldsymbol{Q}\\ (\boldsymbol{E}^{-u_1}+\boldsymbol{E})\boldsymbol{Q} & (\boldsymbol{E}^{-u_2}+\boldsymbol{E})\boldsymbol{Q}\end{bmatrix}=\begin{bmatrix}(\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q} & (\boldsymbol{E}^{u_2}+\boldsymbol{E}^{-1})\boldsymbol{Q}\\ 0 & \boldsymbol{E}^{-u_2}(\boldsymbol{E}^{u_2+1}+\boldsymbol{I})(\boldsymbol{E}^{u_2-u_1}+\boldsymbol{I})\boldsymbol{Q}\end{bmatrix} \tag{37}$$

同理可得 $\widetilde{\boldsymbol{G}}_2$ 的秩也为 $2(m-1)$。

因此根据上面 3 种情况可知，$\widetilde{\boldsymbol{G}}_2$ 的二阶任意分块子矩阵是的秩为 $2(m-1)$。

3) $\widetilde{\boldsymbol{G}}_3$ 的任意三阶子分块子矩阵为

$$\widetilde{\boldsymbol{G}}_3=\begin{bmatrix}\boldsymbol{Q} & \boldsymbol{Q} & \boldsymbol{Q}\\ (\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q} & (\boldsymbol{E}^{u_2}+\boldsymbol{E}^{-1})\boldsymbol{Q} & (\boldsymbol{E}^{u_3}+\boldsymbol{E}^{-1})\boldsymbol{Q}\\ (\boldsymbol{E}^{-u_1}+\boldsymbol{E})\boldsymbol{Q} & (\boldsymbol{E}^{-u_2}+\boldsymbol{E})\boldsymbol{Q} & (\boldsymbol{E}^{-u_3}+\boldsymbol{E})\boldsymbol{Q}\end{bmatrix} \tag{38}$$

式(38)则可以依次左乘一个矩阵可得

$$\begin{bmatrix}\boldsymbol{I} & 0 & 0\\ 0 & \boldsymbol{I} & 0\\ 0 & \boldsymbol{E}^{-u_1}(\boldsymbol{E}+\boldsymbol{E}^{-u_2}) & \boldsymbol{I}\end{bmatrix}\times\begin{bmatrix}\boldsymbol{I} & 0 & 0\\ (\boldsymbol{E}^{u_1}+\boldsymbol{E}^{-1})\boldsymbol{Q} & \boldsymbol{I} & 0\\ 0 & \boldsymbol{E}^{1-u_1} & \boldsymbol{I}\end{bmatrix} \tag{39}$$

矩阵变换结果为

$$\begin{bmatrix}\boldsymbol{Q} & \boldsymbol{Q} & \boldsymbol{Q}\\ 0 & \boldsymbol{E}^{u_1}(\boldsymbol{E}^{u_2-u_1}+\boldsymbol{I})\boldsymbol{Q} & \boldsymbol{E}^{u_1}(\boldsymbol{E}^{u_3-u_1}+\boldsymbol{I})\boldsymbol{Q}\\ 0 & 0 & \boldsymbol{E}^{-u_3}(\boldsymbol{E}^{u_3-u_2}+\boldsymbol{I})(\boldsymbol{E}^{u_3-u_1}+\boldsymbol{I})\boldsymbol{Q}\end{bmatrix} \tag{40}$$

同理可得：$\widetilde{\boldsymbol{G}}_3$ 的秩也为 $3(m-1)$。

因此，根据 1)、2)、3)三种情况可知，$\widetilde{\boldsymbol{G}}$ 的任意分块子矩阵的秩为 $r(m-1)$，$1\leqslant r\leqslant 3$。

引理 2 矩阵 $\boldsymbol{G}$ 的任意分块子矩阵为满秩，$\boldsymbol{G}$ 如式(41)所示。

$$\boldsymbol{G}=\begin{bmatrix}\boldsymbol{I}_{m-1} & \boldsymbol{I}_{m-1} & \boldsymbol{I}_{m-1} & \cdots & \boldsymbol{I}_{m-1}\\ \widetilde{\boldsymbol{Q}}(\boldsymbol{I}_{m-1}+\boldsymbol{E}^{-1})\boldsymbol{Q} & \widetilde{\boldsymbol{Q}}(\boldsymbol{E}+\boldsymbol{E}^{-1})\boldsymbol{Q} & \widetilde{\boldsymbol{Q}}(\boldsymbol{E}^{2}+\boldsymbol{E}^{-1})\boldsymbol{Q} & \cdots & \widetilde{\boldsymbol{Q}}(\boldsymbol{E}^{m-2}+\boldsymbol{E}^{-1})\boldsymbol{Q}\\ \widetilde{\boldsymbol{Q}}(\boldsymbol{I}_{m-1}+\boldsymbol{E})\boldsymbol{Q} & \widetilde{\boldsymbol{Q}}(\boldsymbol{E}^{-1}+\boldsymbol{E})\boldsymbol{Q} & \widetilde{\boldsymbol{Q}}(\boldsymbol{E}^{-2}+\boldsymbol{E})\boldsymbol{Q} & \cdots & \widetilde{\boldsymbol{Q}}(\boldsymbol{E}^{2-m}+\boldsymbol{E})\boldsymbol{Q}\end{bmatrix} \tag{41}$$

证明 矩阵 $\boldsymbol{G}=\begin{bmatrix}\widetilde{\boldsymbol{Q}} & \boldsymbol{0}_{(m-1)\times m} & \boldsymbol{0}_{(m-1)\times m}\\ \boldsymbol{0}_{(m-1)\times m} & \widetilde{\boldsymbol{Q}} & \boldsymbol{0}_{(m-1)\times m}\\ \boldsymbol{0}_{(m-1)\times m} & \boldsymbol{0}_{(m-1)\times m} & \widetilde{\boldsymbol{Q}}\end{bmatrix}\times\widetilde{\boldsymbol{G}}$，

因此分块矩阵 $\boldsymbol{G}$ 的子矩阵是由分块矩阵 $\widetilde{\boldsymbol{G}}$ 的子矩阵删除每个小矩阵最后一行而构成的，又因为 $\widetilde{\boldsymbol{G}}$ 的任意子矩阵的秩为 $r(m-1)$，$1\leqslant r\leqslant 3$，因此 $\boldsymbol{G}$ 的任意分块子矩阵的秩也为 $r(m-1)$，即为满秩。证毕。

参考文献：

[1] 王意洁，孙伟东，周松等.云计算环境下分布存储关键技术[J]. 软件学报网络优出版, 2012, 23(4):962-986.
WANG Y J, SUN W D, ZHOU S, *et al.* Key technologyies of distributed storage for cloud computing[J]. Journal of Software ,2012,23(4):962-986.

[2] 罗象宏，舒继武. 存储系统中的纠删码研究综述[J]. 计算机研究与发展, 2012, 49(1):1-11.
LUO X H, SHU J W. Summary of research for erasure code in storage system[J]. Journal of Compute Research and Development, 2012, 49(1):1-11.

[3] BLAUM M, BRADY J, BRUCK J, *et al*. EVENODD: an efficient scheme for tolerating double disk failures in RAID architectures[J]. IEEE Trans Compute, 1995, 44(2):192-202.

[4] XU L, BRUCK J. X-code: MDS array codes with optimal encoding[J]. IEEE Trans on Information Theory, 1999, 45(1):272-276.

[5] XU L, BOHOSSIAN V, BRUCK J, *et al*. Low density MDS codes and factors of complete graphs[J]. IEEE Trans on Information Theory, 1999, 45(6):1817-1826.

[6] LI M Q, SHU J W. C-codes: cyclic lowest-density MDS array codes constructed using starters or RAID 6[EB/OL]. http://arxiv.org/ abs/1104.2547.

[7] CORBETT P, ENGLISH B, GOEL A, *et al*. Row diagonal parity for double disk failure[A]. Proceedings of the Third USENIX Conference on File and Storage Technologies[C]. 2004. 1-14.

[8] WU C T, WAN S G, HE X B, *et al*. H-code:a hybrid MDS array code to optimize partial stripe writes in RAID-6[A]. Proceedings of the IEEE Congress on International Parallel&Distributed Processing Symposium[C]. USA, 2011. 782-793.

[9] LI M, SHU J, ZHENG W. GRID codes: strip-based erasure code with high fault tolerance for storage systems[J]. ACM Transactions on Storage, 2009, 4(4):1-22.

[10] HAFNER J L. HoVer erasure codes for disk arrays[EB/OL]. http://domino.

research.ibm.com/library, 2005.

[11] HAFNER J L. WEAVER codes: highly fault tolerant erasure codes for storage systems[EB/OL]. http://www.usenix.org/events/fast05, 2005.

[12] FENG G L, DENG R, BAO F, *et al*. New efficient MDS array codes for RAID, Part I: reed-solomon-like codes for tolerating three disk failures[J]. IEEE Trans Computers, 2005,54(9):1071-1080.

[13] FENG G L, DENG R, BAO F, *et al*. New efficient MDS array codes for RAID, part II: rabin-like codes for tolerating multiple (4)disk failures[J]. IEEE Trans Computers, 2005, 54(12):1473-1482.

[14] BLAUM M, BRUCK J, VARDY A. MDS array codes with independent parity symbols[J]. IEEE Trans Inform Theory, 1996, 42:529-542.

[15] SHENG L, GANG W, STONES D S, *et al*. T-code: 3 erasure longest lowest-density MDS codes[J]. IEEE Journal on Selected Areas in Communications, 2010, 28(2):289-296.

[16] CHIH-SHING T, TZONE-I W. Efficient parity placement schemes for tolerating triple disk failures in RAID architectures[A]. Proceedings of the 17th International Conference on Advanced Information Networking and Applications(AINA'03)[C]. Washington DC, USA, 2003. 132-138.

[17] HUANG C, XU L. STAR: an efficient coding scheme for correcting triple storage node failures[A]. Proceedings of the 4th USENIX Conf on File and Storage Technologies[C]. Berkeley, CA, 2005. 197-210.

[18] 万武南, 吴震. RAID-EEOD: 一种基于 3 容错阵列码 RAID 数据布局研究[J]. 计算机学报, 2007, 30(10):1-10.
WAN W N, WU Z. RAID-EEOD: the study of data placement based on toleration on triple failures array codes in RAID[J]. Chinese Journal of Compute, 2007, 30(10):1-10.

[19] PLANK J S. A tutorial on reed-solomon coding for fault-tolerance in RAID-like systems[J]. Software Practice and Experience(SPE), 1997, 27(9):995-1012.

[20] BLOEMER J M, KALFANE M, KARPINSKI R. An XOR-Based Erasure-Resilient Coding Scheme[R]. Technical report at ICSI, 1995.

作者简介：

万武南（1978-），女，江西樟树人，博士，成都信息工程学院副教授，主要研究方向为编码理论安全存储。

索望（1978-），男，重庆人，成都信息工程学院讲师，主要研究方向为密码技术。

陈运（1958-），女，河南郑州人，成都信息工程学院教授，主要研究方向为密码技术、编码理论。

王拓（1989-），男，四川广元人，成都信息工程学院硕士生，主要研究方向为密码技术。