中国科学技术大学

博士学位论文

数据存储中的编码问题

作者姓名：　叶左

学科专业：　应用数学

导师姓名：　张先得 特任教授　葛根年 教授

完成时间：　二〇二二年五月二十一日

University of Science and Technology of China

A dissertation for doctor's degree

Coding problems in data storage

Author: Zuo Ye

Speciality: Applied Mathematics

Supervisors: Prof. Xiande Zhang, Prof. Gennian Ge

Finished time: May 21, 2022

中国科学技术大学学位论文原创性声明

本人声明所呈交的学位论文，是本人在导师指导下进行研究工作所取得的成果。除已特别加以标注和致谢的地方外，论文中不包含任何他人已经发表或撰写过的研究成果。与我一同工作的同志对本研究所做的贡献均已在论文中作了明确的说明。

作者签名：_____ 签字日期：_____

中国科学技术大学学位论文授权使用声明

作为申请学位的条件之一，学位论文著作权拥有者授权中国科学技术大学拥有学位论文的部分使用权，即：学校有权按有关规定向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅，可以将学位论文编入《中国学位论文全文数据库》等有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。本人提交的电子文档的内容和纸质论文的内容相一致。

保密的学位论文在解密后也遵守此规定。

☑ 公开 ☐ 保密（____ 年）

作者签名：_____ 导师签名：_____

签字日期：_____ 签字日期：_____

摘　要

现代社会离不开数据的存储。现实生活中，根据应用场景的不同，人们对数据存储设备的要求是多种多样的，例如高存储密度、高存取速度、高可靠性、低功耗、存储时间长等等。闪存是一种电子非易失性计算机存储介质（即断电数据也不会丢失），可进行电擦除和重新编程。其因为具有存储密度高、读写速度快、功耗低、成本较低等特点而被广泛地应用到现实生活中。另一方面，由于具有远大于如今所有存储设备的存储密度以及能长时间存储数据这两个特点，DNA 存储在近些年得到国内外研究人员的大量研究。因为各种客观原因，数据在存储或读取过程中不可避免地会发生错误。因此，有必要将编码技术应用到数据存取中。本学位论文的主旨是利用代数、数论以及组合的工具来研究与闪存和 DNA 存储中编码有关的数学问题。

在第一章绪论部分，我们介绍本文所涉及课题的研究背景，并简要陈述本文对该领域所做的贡献。

在第二章中，我们研究分解集，其与闪存中的编码问题密切相关。闪存设备单元编程（电荷注入）和单元擦除（电荷移除）之间固有的不对称性，以及电荷的缓慢流失，是导致闪存中数据发生错误的两类常见原因。根据这两个错误类型的特点，我们可以把非平衡有限量级错误模型应用到多级闪存技术上。在这个模型下，多级闪存中的编码问题就转换成了分解集的构造问题，并且完美分解集就对应着完美码，而完美码是应用中一个十分感兴趣的码类。对于这个问题，我们推进了已有的工作。首先，我们用代数工具给出了非奇异完美 $B[-k_1, k_2](p)$ 集存在的充要条件，其中 $0 \leqslant k_1 \leqslant k_2 = 4$，从而完全解决了 $k_2 = 4$ 的情形。当存在性的条件满足时，我们给出了较为简单的具体的构造方法。其次，我们利用数论中的工具，在满足特定条件的参数下，给出了非奇异完美分解集存在性的更加简单的刻画。然后，我们给出了准完美分解集的四种新无穷类的构造。最后，我们将分解集和凯莱图联系起来，这对我们使用数学软件计算最大的分解集十分有帮助。

第三章中，我们考虑序列重构问题，其与 DNA 存储相关。序列重构问题是 Levenshtein 于 2000 年左右开始研究的，作为传统纠错码的推广，其旨在用多个噪声读取重构出原来的序列。基于序列重构问题在赛道内存和 DNA 存储中的潜在应用价值，Cai 和 Yaakobi 等人于 2020 年开始研究 Levenshtein 问题的反问题：在噪声读取的数目 N 给定时，构造冗余尽可能小的码。在本章中，我们考虑恰好发生两个插入错误的信道。首先，我们完全确定两个错误球相交的大小等于某些给定值的充要条件。然后我们再用这些条件来构造相应的码：对所有的 $N > 6$,

我们给出了码的渐近最优冗余；对于 $N = 6$，我们将冗余的已知最好的上界从 $4log_2(n)$ 改进到了 $2log_2(n)$，其中 n 是码长。

第四章中，我们对其他工作进行简单的汇报。

关键词：闪存；分解集；插入信道；重构码；DNA 存储

ABSTRACT

Data storage can be seen everywhere in modern society. In real life, according to different application scenarios, people have various requirements for data storage devices, such as high storage density, high access speed, high reliability, low power consumption and long storage time. Flash memory is a non-volatile storage device and it can be electrically erased and re-programmed. It is widely used in reality because of its high storage density, fast reading and writing speed, low power consumption and low cost. On the other hand, DNA storage has been studied by many researchers in recent years because of its two characteristics: the storage density is much higher than that of all existing storage devices and it is capable of storing data for an extremely long time. Due to various reasons, there may be inevitable errors in the process of data storage. Therefore, it is necessary to apply coding technique to data storage. The main purpose of this thesis is to utilize tools form algebra, number theory and combinatorics to study mathematical problems related to coding schemes in flash memory and DNA storage.

In Chapter 1, we introduce the research backgrounds of the subjects involved in this thesis, and briefly state our contributions to these fields.

In Chapter 2, we study splitter sets, which have a close connection with coding problems in flash memories. The inherent asymmetry between cell programming (charge injection into cells) and cell erasure (charge removal from cells), as well as the slow process of charge leakage in cells, are two common reasons for data errors in flash memory. Taking into account these two error types and their properties, it is reasonable for us to apply the unbalanced limited-magnitude error model to the multi-level flash memory technology. In this model, the coding problem in multi-level flash memory is transformed into the problem of constructing splitter sets. Besides, perfect splitter sets correspond to perfect codes, which is of interest in practice. As for this problem, we forward the existing works. Firstly, we use tools from algebra to determine the necessary and sufficient conditions under which there exists a nonsingular perfect $B[-k_1, k_2](p)$ set, where $0 \leqslant k_1 \leqslant k_2 = 4$, and thus completely solve the problem for the case $k_2 = 4$. When the conditions are satisfied, we present explicit constructions of perfect splitter sets. Secondly, using the tools from number theory, we give a simpler characterization of the existence of nonsingular perfect splitter sets when the parameters satisfy certain conditions. Thirdly, we give four new constructions of quasi-perfect splitter sets. Lastly, we connect splitter sets with Cayley graphs, which is helpful for us to find the maximum

splitter sets via mathematical software.

In Chapter 3, we study the sequence reconstruction problem, which has a close connection with DNA storage. The study of sequence reconstruction problem was initiated by Levenshtein in 2001. As a generalization of the classical error-correction, the reconstruction problem aims to correct errors by several noisy reads. In 2020, motivated by applications in racetrack memeories and DNA storages, Cai and Yaakobi et al. began to study the dual problem, that is, designing codes with redundancy as small as possible for a given number N of noisy reads. In this chapter, the minimum redundancy of such codes for binary channels with exactly two insertions are determined asymptotically for all values of $N > 6$. For $N = 6$, we reduce the current best known upper bound on the redundancy from $4log_2(n)$ to $2log_2(n)$ for length-n binary codes. The explicit constructions of codes are based on completely characterizing the conditions under which two binary sequences have a fixed number of common supersequences.

In Chapter 4, we briefly introduce the author's other research works when pursuing his PhD degree.

Key Words: flash memory; splitter set; insertion channel; reconstruction code; DNA storage

目　录

插 图 清 单

表 格 清 单

第 1 章 绪 论

现代社会是一个信息社会，数据存储在现代社会中无处不在。根据应用场景的不同，人们对数据存储设备性能的要求是多种多样的，例如高存储密度、高存取速度、高可靠性、低功耗、存储时间长等等。闪存是一种电子非易失性计算机存储介质（即断电数据也不会丢失），可进行电擦除和重新编程。自从 1980 年被日本东芝公司发明以来，闪存技术得到了极大的发展。此外，闪存因为具有较高的存储密度、较快的读写速度、低功耗、较低的成本等优点而被广泛地应用到现实生活中，例如个人电脑、数字视频播放器、数码相机、移动电话和嵌入系统，等等。这些应用场景都有一个共同特点，即数据会被经常使用。现实中我们也会碰到一些不常用却需要长时间保存的数据，譬如政府文件、历史档案等。此时被广泛使用的存储设备包括机械硬盘、磁带等等。但是现代社会的数据量是指数级增长的，现有的存储设备的存储密度将会越来越满足不了实际需求[1]。因此，寻找下一代信息存储设备和研究相关的存储技术越来越重要。因具有远大于如今所有存储设备的存储密度以及能长时间存储数据这两个特点，DNA 存储在近些年得到国内外研究人员的大量研究[2-7]。

因为许多客观原因，数据在存储或读取过程中不可避免地会发生错误。因此，我们有必要将编码技术应用到数据存取中。本学位论文中，我们针对闪存和 DNA 存储中特定的错误类型，利用代数、数论以及组合的工具来研究与闪存和 DNA 存储中编码有关的数学问题。下面我们具体介绍这两个子课题的研究背景，并简要介绍本文在各个课题上所做的研究工作。

1.1 分解集及其在多级闪存技术中的应用

1.1.1 闪存及其错误类型

闪存（flash memory）是一种电子非易失性计算机存储介质（即断电数据也不会丢失），可进行电擦除和重新编程，其在现实中有着非常广泛的应用。闪存单元（cell）采用浮栅技术，利用捕获的电荷来存储信息。通过测量单个闪存单元中的电荷水平并将其与预定的阈值水平集进行比较，人们可以将电荷水平量化为 q 个值之一。一般从数学角度而言，我们用 $\mathbb{Z}_q$ 中的元素表示这些量化的值。起初，q 只限定成 2，即每个闪存单元只存储一个比特的信息。为了提高闪存的存储密度，B. Eitan 和 A. Roy 在 1999 年提出了多级（multi-level）闪存单元这个概念[8]，用以增加每个单元中存储的信息比特的数目。多级闪存技术允许 q 取更大的值，从而使得每个闪存单元能存储 $\log_2(q)$ 个比特的信息。和所有的存储设

备一样，由于客观因素，闪存中存储的信息可能会发生错误。为了纠正可能发生的错误，许多已有的编码方案已经被应用到了闪存技术中[9-10]。然而，这些方案的主要缺点就是它们并不是针对闪存中特有的错误类型设计的，因此这些码的效率并不高。

闪存设备表现出多种复杂的错误类型和行为，但所有类型的闪存存储都有一个共同点，那就是单元编程（电荷注入到存储单元中去）和单元擦除（电荷从存储单元移除）之间固有的不对称性。前者很容易在单个的存储单元上操作，但是后者必须是对多个单元一起操作。因此，为了让一个存储单元能存事先设定好的比特数目的数据，人们会将电荷分多次注入到某个存储单元中，且每次注入的电荷都很少，直到该存储单元的电荷量达到预定的值为止。然而在这个过程中，存储单元可能会出现电荷注入过多的情况。如果没有应用编码技术，当遇到这种情况的时候，我们只能将这个存储单元以及和它相邻的多个存储单元中的电荷全部移除，然后再对它们重新注入电荷。这样一来，闪存设备的工作效率就很低。闪存中另一种常见的错误是由电荷的缓慢流失造成的，其会导致存储单元中的电荷量减少[11]。在第一种情形下，存储单元发生的错误指的就是注入了超过预设的值的电荷量；在第二种情形下，存储单元发生的错误指的就是电荷量的流失。根据前面的描述我们可知，这两种错误的量级都非常小，而且和字母集的大小无关。

根据以上两个错误类型及其特性，我们有理由把非平衡有限量级错误模型[12] 应用到多级闪存技术上。在这个模型下，一个码字 $\boldsymbol{x} \in \mathbb{Z}_q^n$，被一个错误向量 $\boldsymbol{e} \in \mathbb{Z}_q^n$ 作用后变成了向量 $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$。这里 $\boldsymbol{e}$ 的汉明重量是 0 或者 1（这里我们只考虑至多有一个存储单元发生错误的情况）；当 $\boldsymbol{e}$ 的汉明重量等于 1 的时候，其非零分量 e_i 满足 $-k_1 \leqslant e_i \leqslant k_2$（其中 k_1, k_2 是给定的非负整数，且比 q 要小得多）。

1.1.2　分解集及其在闪存中的应用

设 $q, k_1, k_2 \in \mathbb{Z}$ 且满足 $q \geqslant 2$，$0 \leqslant k_1 \leqslant k_2$，设 $\boldsymbol{B}$ 是 $\mathbb{Z}_q$ 的一个子集。如果对每一个 $b \in \boldsymbol{B}$，集合 $\{bm \pmod q \mid -k_1 \leqslant m \leqslant k_2 \text{ 且} m \neq 0\}$ 都有 $k_1 + k_2$ 个非零元素，并且这 $|\boldsymbol{B}|$ 个集合两两不相交，则称 $\boldsymbol{B}$ 是一个分解集。我们把这样的分解集记作 $\boldsymbol{B}[-k_1, k_2](q)$ 集。如果 $|\boldsymbol{B}| = \frac{q-1}{k_1+k_2}$，我们称 $\boldsymbol{B}$ 是完美的；如果 $q \not\equiv 1 \pmod{k_1 + k_2}$ 且 $|\boldsymbol{B}| = \lfloor \frac{q-1}{k_1+k_2} \rfloor$，则称 $\boldsymbol{B}$ 是准完美的。

假设 $\boldsymbol{B} = \{b_1, \cdots, b_n\}$ 是一个 $\boldsymbol{B}[-k_1, k_2](q)$ 集，我们用

$$\boldsymbol{H} = \begin{pmatrix} b_1, \cdots, b_n \end{pmatrix}$$

作为一个校验矩阵构造码

$$C = \left\{ \boldsymbol{c} = (c_1, \cdots, c_n) \in \mathbb{Z}_q^n \mid \sum_{i=1}^{n} b_i c_i \equiv 0 \pmod{q} \right\}.$$

因为 $\boldsymbol{B}$ 是一个 $\boldsymbol{B}[-k_1, k_2](q)$ 集且 $\boldsymbol{H}\boldsymbol{y}^T = \boldsymbol{H}(\boldsymbol{x}+\boldsymbol{e})^T = \boldsymbol{H}\boldsymbol{e}^T$，所以我们能根据 $\boldsymbol{H}\boldsymbol{y}^T$ 唯一的解出 $\boldsymbol{e}$。这样一来，我们就能够解出 $\boldsymbol{x}$，即完成了解码。

一方面，应用了这个码以后，在注入电荷的过程中，我们不需要严格的达到预定的值，即使注入的电荷稍微过量也没关系，而具体能超过多少取决于所构造的码的纠错能力，即 k_2 的大小。另一方面即使长时间存放导致了电荷流失，我们也能恢复原来的数据，而能容忍流失的电荷量取决于 k_1 的大小。

1.1.3　我们的结果

本小节中，我们简单陈述我们的主要贡献。如果 $\gcd(k_2!, q) = 1$，我们称一个 $\boldsymbol{B}[-k_1, k_2](q)$ 集是非奇异的。首先，我们应用代数工具得到了非奇异完美分解集存在的充要条件，即如下主要结果。

定理 1.1　(i) 令 $p \equiv 1 \pmod 6$ 是一个素数，则存在一个非奇异完美 $\boldsymbol{B}[-2,4](p)$ 集当且仅当 $\mathrm{ord}_p(-\frac{3}{4})$ 是奇数，并且 $2 \notin \langle 6, 8\rangle$。

(ii) 设 $p \equiv 1 \pmod 8$ 是一个素数，则存在一个非奇异完美 $\boldsymbol{B}[-4,4](p)$ 集当且仅当 $\pm 4 \notin \langle 6, 16\rangle$。

(iii) 设 $p \equiv 1 \pmod 4$ 是一个素数，则存在一个非奇异完美 $\boldsymbol{B}[0,4](p)$ 集当且仅当 $4 \notin \langle 6, 16\rangle$。

当这些条件满足的时候，我们给出了分解集的具体构造方法，具体的内容可参见上述定理的证明过程以及文中相应的例子。对于上面的三种情形，当 $\frac{p-1}{k_1+k_2}$ 和 $k_1 + k_2$ 互素的时候（其中 $(k_1, k_2) \in \{(2,4), (0,4), (4,4)\}$），我们能得到更简单的充要条件。然后我们利用这个更简单的条件以及数论中的知识，得到了下面更精确的结果。

定理 1.2　设 $p \equiv 1 \pmod 6$ 是一个素数，并且 $\gcd(\frac{p-1}{6}, 6) = 1$。则存在一个非奇异完美 $\boldsymbol{B}[-2,4](p)$ 集当且仅当存在整数 k, l，使得下面三个条件之一成立：

1) $p = 1296k^2 - 648kl + 324l^2 + 36k + 72l + 7$。

2) $p = 1296k^2 - 648kl + 324l^2 + 1764k - 360l + 607$。

3) $p = 36k^2 - 108kl + 324l^2 - 102k + 558l + 241$，其中 $k + 3l \equiv 1$ 或3 $\pmod 6$。

除了完美分解集外，我们还研究了准完美分解集，并给出了下面四种新的构造。相关概念请见第二章。

定理 1.3　设 k, m 是两个正整数，且满足 $\gcd(k!, m) = 1$。令 $a = (-k)^{-1} \pmod m$，则

$$\boldsymbol{B} = \left\{ ik + 1 \mid i \in [0, m-1] \text{并且} i \neq a \right\}$$

是一个准完美 $B[0,k](km)$ 集。

定理 1.4　令 $k>0$ 是一个整数，p 是一个素数且满足 $k<p<2k$，则

$$B=\{k+1\}\cup\{1+(2k+2)i \mid i\in[0,p-1]\}$$

是一个准完美 $B[-k,k](p(2k+2))$ 集。

定理 1.5　设 $k\geqslant 2$ 是一个偶数，$m\geqslant 1$ 是一个正整数。对于 $i=0,1$，令 $T_i=\{x \mid x\equiv i \pmod 2, x\in[1,k]\}$，则 $|T_i|=\frac{k}{2}$。设 $p\equiv 1 \pmod{2^m k}$ 是一个素数，令 g 是一个模 p 的本原根且满足 $g\equiv 1 \pmod 2$，记 $v\triangleq 2^{m-1}k$。如果存在 $\mathbb{Z}_v$ 的一个大小为 2^m 的子集 A，使得对每一个 $i=0,1$，$\mathbb{Z}_v=A+\{\mathrm{ind}_g(x) \pmod v \mid x\in T_i\}$ 都是一个唯一分解，则

$$B\triangleq\{g^{i+jv} \mid i\in A, j\in[0,n-1]\}$$

是一个准完美 $B[-k,k](2p)$ 集，其中 $n=\frac{p-1}{2^m k}=\frac{p-1}{2v}$。

定理 1.6　设 k 是一个正整数，p 是一个素数且满足 $k<p<\frac{4k-1}{3}$，则集合

$$B=\{k+1\}\cup\{1+(2k+2)i : i\in[0,p-1]\}$$

是一个准完美 $B[-(k-1),k](p(2k+2))$ 集。

最后，当 p 是素数的时候，我们在非奇异 $B[-k_1,k_2](p)$ 集和凯莱（Cayley）图之间建立起联系。利用这个联系，我们可以用一些数学软件（比如 Maple）来计算最大的分解集。

1.2　重构码及其应用

序列的有效重构问题是由 V.I. Levenshtein 于 2000 年左右开始研究的[13-15]。他研究这个问题的动机是其在许多科学领域中都有应用，例如信息科学、分子生物学、化学等等。在这些应用场景中，我们除了将要传输的信息重复多次传输以外，别无他法。这个问题模型可描述为：信息的发送方将信息通过 N 个不同的噪声信道传输出去；信息的接收方能够接收到所有 N 个信道的输出（我们称为有噪声的读取（noisy read））；然后接收方的目标是利用这 N 个有噪声读取 $\boldsymbol{y}_1,\cdots,\boldsymbol{y}_N$ 来重构发送方发送的信息，见图1.1。注意，当 $N=1$ 时，这个问题就是经典的纠错码问题。因此，序列重构问题可以看成纠错码问题的一个推广。一般而言，序列重构问题可以划分为两大类：概率模型和组合模型。在概率模型中，被传输的序列 $\boldsymbol{x}$ 的每个位置都按照一定的概率分布发生错误；接收方的目标是使得成功重构出 $\boldsymbol{x}$ 的概率尽可能地大，并同时使得噪声读取的个数（即 N 的值）尽可能地小。在组合模型中，我们假设信息在每个信道中都发生最大数目的错

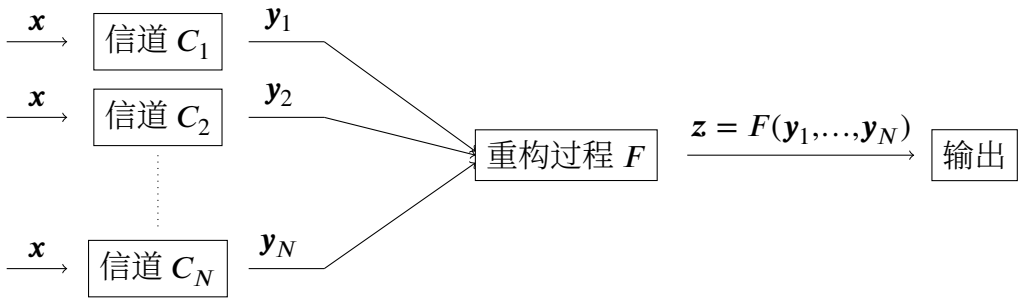

图 1.1　序列重构问题模型

误；此时接收方的目标是找到最小的能够精确重构出 $\boldsymbol{x}$ 所需要的噪声读取的个数（即 N 的值）。本学位论文中只考虑组合信道模型下的序列重构问题，关于概率信道模型下此类问题的研究情况，感兴趣的读者可以查看文献 [14,16-21]，以及这些文献所引用的参考文献。

对于组合信道，我们要求每个信道的输出都是不同的[14]。如此一来，这个问题就转换成了求两个不同的错误球（error ball）相交的大小的最大值的问题。在文献 [14-15] 中，Levenshtein 针对很多种错误类型解决了该问题，例如替换（substitutions）、换位（transpositions）、非对称错误（asymmetric errors）、删除错误（deletions）以及插入错误（insertions）。文献 [22-24] 分析了置换错误。关于一般的错误图（error graphs），读者可以查看文献 [14,25-26]。注意，上述提到的研究工作中，被传输的序列是从整个空间中选取的，即被研究的都是未编码的情形。

最近一些年，由于在 DNA 存储和无限感知网络等场景中的应用，这个问题又吸引了大量研究人员的兴趣[27-29]。许多研究者开始在编码的情形下考虑这个问题, 即被传输的序列是从某个具有一定纠错能力的码中选取的。在文献 [30] 中，作者考虑了最小 Kendall τ 距离等于 $1, 2, 2r$ 的置换码（permutation code）。Gabrys 和 Yaakobi 等人在文献 [28,31] 中研究了这样的情形：被传输的序列是从一个单删除纠错码中选取的，并且每个信道恰好发生 t 个删除错误。他们成功地推导出了两个不同的 t-删除球（deletion ball）相交大小的最大值的递归公式（假定这两个球的中心之间的 Levenshtein 距离大于等于 2）。他们研究这个问题的一个动机就是其在无限感知网络中的应用[28,32]。在 2017 年，Sala 等人在文献 [27] 研究了插入信道——对任何的 $l \geqslant 0$，他们找到了当两个不同的插入球（insertion ball）的中心之间的编辑距离（edit distance）大于等于 $2l$ 时，这两个球相交大小的最大值的一个精确公式（事实上，他们得到了更加一般的结果），这个公式推广了文献 [14-15] 中的结果。此外，对于删除信道，他们改进了文献 [28,31] 中的结果，即他们给出了一个精确的公式，而不是一个递归型的公式。他们研究这个问题的动机是：这个问题在系统基因学（phylogenomics）和数据存储中有应用（例如 DNA 存储）。到目前为止，我们提到的工作都是假设每个信道造成的最大错

误的个数是相同的。然而，现实中碰到的情况并不都是如此。例如，当读取存储在 DNA 链中的数据时，可能会出现这种情况——有些读取发生的错误要比其他读取所发生的错误要多[33]。受此启发，Horovitz 和 Yaakobi 在文献 [29] 中推广了 Levenshtein 的模型。在那篇文章中，他们考虑了这样的一个组合信道模型：每个信道不一定是同性的，即每个信道能发生的最大错误的个数不一定相同。

以上所提到的所有研究工作都有一个共同的特点，即他们考虑的都是先给定一个码，然后研究以不同码字为中心的两个不同的错误球相交大小的最大值。然而，在大多数应用场景中，噪声读取的个数（即 N 的值）是一个预先给定的系统参数。在 2020 年，受 DNA 数据存储和赛道内存（racetrack memory）中的应用启发，Cai 和 Nguyen 等人[34-35] 以及 Chrisnata 和 Yaakobi 等人[36] 率先研究了这个问题：设计一个码（称为重构码），使得以它的不同码字为中心的两个不同的错误球相交的大小的最大值小于 N，其中 N 给定。在文献 [35-36] 中，作者主要考虑了发生一个编辑错误（edit error）的信道 (即一个替换错误、一个插入错误或一个删除错误）以及它们的变种，并对所有的 N 都给出了码的构造。特别地，当字母表大小为 2 的时候，他们确定了码的冗余的渐近最优值。

本学位论文中，我们继续推进文献 [34-36] 的研究工作，并且我们只考虑插入信道且字母表大小是 2 的情形。对所有的 $N > 6$，我们完全解决了这个问题；对于 $N = 6$，我们成功构造出了一个码，并且这个码的冗余很小。我们的主要工作分为以下三个个方面，其中涉及到的符号和定义请见第三章。

首先，我们研究了当两个 1-插入球相交的大小恰好为 1 的时候，它们 t-插入球相交的大小，其中 $t \geqslant 2$。然后利用这个结果，我们完全刻画了两个错误球相交的大小恰好等于 $n+4, n+5$ 或 6 的充要条件，即下面的定理1.7和定理1.8。

定理 1.7　设 $\boldsymbol{x} = \boldsymbol{u}a\bar{a}\boldsymbol{v}b\boldsymbol{w}$ 和 $\boldsymbol{y} = \boldsymbol{u}\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}$ 是长度为 n 的两个不同序列，其中 $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \Sigma_2^*$，$a, b \in \Sigma_2$，并且 $\boldsymbol{v}$ 不满足以下两个条件中的任何一个：

$$\boldsymbol{v} = (a\bar{a})^m (m \geqslant 0) \text{且} a = b,$$
$$\boldsymbol{v} = (a\bar{a})^m a (m \geqslant 0) \text{且} a = \bar{b}.$$

则我们有如下结论：

(i) $\left|I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})\right| = n+5$ 当且仅当

- 如果 $a = b$，则存在 $i, j \geqslant 0$，使得 $\boldsymbol{v} \in \{(a\bar{a})^i a (a\bar{a})^j, (a\bar{a})^i (\bar{a}a)^j \bar{a}\}$。
- 如果 $a = \bar{b}$，则存在 $i, j \geqslant 0$，使得 $\boldsymbol{v} \in \{(a\bar{a})^i (\bar{a}a)^j, (a\bar{a})^i aa (\bar{a}a)^j\}$。

(ii) $\left|I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})\right| = n+4$ 当且仅当 a, b 和 $\boldsymbol{v}$ 满足表3.1中所列的条件之一。

定理 1.8　令 $n \geqslant 2$, 设 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 Σ_2^n 中两个不同的序列。则 $\left|I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})\right| = 6$ 当且仅当存在满足条件 $a\boldsymbol{d} \neq \boldsymbol{e}\bar{b}$ 和 $\boldsymbol{d}b \neq \bar{a}\boldsymbol{e}$ 的 $\boldsymbol{u}, \boldsymbol{w}, \boldsymbol{d}, \boldsymbol{e} \in \Sigma_2^*$ 以及 $a, b \in \Sigma_2$，使

得

$$\begin{cases} \boldsymbol{x} = \boldsymbol{u}a\boldsymbol{d}b\boldsymbol{w} \\ \boldsymbol{y} = \boldsymbol{u}\bar{a}\boldsymbol{e}\bar{b}\boldsymbol{w} \end{cases},$$

这里 $\boldsymbol{d}$ 和 $\boldsymbol{e}$ 满足下面的条件:

(i) 当 $a = b$ 时，$\boldsymbol{d}$ 和 $\boldsymbol{e}$ 必须满足表A.1中某一行的条件（见附录A）。

(ii) 当 $a = \bar{b}$ 时，$\boldsymbol{d}$ 和 $\boldsymbol{e}$ 必须满足表A.2中某一行的条件（见附录A）。

最后，我们利用上面的结论给出了码的构造。

定理 1.9　对任何的 $n \geqslant 3, P \geqslant 12$，其中 $6 \mid P$，令 $c \in \mathbb{Z}_{1+\frac{P}{2}}$ 以及 $d \in \mathbb{Z}_2$。我们将 $\boldsymbol{C}(n; c, d)$ 定义为满足下面所有条件的序列 $\boldsymbol{x} = x_1 \cdots x_n \in \Sigma_2^n$ 的全体构成的集合:

- $\mathrm{Inv}\,(\boldsymbol{x}) \equiv c \pmod{1 + \frac{P}{2}}$;
- $\sum_{i=1}^{n} x_i \equiv d \pmod 2$;
- $\boldsymbol{x} \in R(n, 2, \frac{P}{3})$.

则 $\boldsymbol{C}(n; c, d)$ 是一个 $(n, n{+}5; B_2^{I(2)})$-重构码。进一步地,如果我们取 $\frac{P}{3} = \lceil \log_2(n) \rceil + 3$, 则可以取到 c 和 d,使得 $\boldsymbol{C}(n; c, d)$ 的冗余至多为 $1{+}\log_2(P{+}2) = \log_2 \log_2(n){+}O(1)$。

运用类似的方法，我们也成功构造出了 $(n, n+4; B_2^{I(2)})$-重构码和 $(n, 6; B_2^{I(2)})$-重构码。特别地，当 $N = n+4$ 和 $n+5$ 的时候，我们构造的码的冗余是渐近最优的; 当 $N = 6$ 的时候, 我们将冗余已知的最好的上界 $4\log_2(n)$ 改进到了 $2\log_2(n)$。

第 2 章　分解集及其在存储编码中的应用

2.1　介绍

闪速存储器（闪存）是一种电子非易失性存储介质（即断电数据也不会丢失），可进行电擦除和重新编程。因为存储密度高、功耗低以及可靠性高等特点，其目前在现实生活中有着非常广泛的应用，例如个人电脑、数字视频播放器、数码相机、移动电话和嵌入系统，等等。

为了提高闪存的存储密度，人们采用了多级闪存单元技术来增加每个单元中存储的信息比特的数目。如果一个存储单元有 q 级，则这个单元中存储的电荷数可量化成 q 个值（例如与 $\mathbb{Z}_q$ 中的值对应）之一。这样一来，每个存储单元可以存储 $\log_2(q)$ 个比特的数据。电荷的缓慢注入（在读写数据的时候发生）和电荷擦除这两个过程的不对称性，以及长期存放导致的电荷缓慢流失，是闪存可能发生的错误的两大来源。此外，实验结果表明这些错误的量级远小于字母集的大小，即 q 的大小。因此，为了纠正这种错误，我们可以应用非平衡有限量级错误模型[12,37-39]。

分解集这个概念是上个世纪 S. Stein、D. Hickerson 和 S. Sabó 等人在研究欧氏空间的格镶嵌问题的时候提出的[40-46]。近十年来，由于其在多级闪存技术上的应用，分解集又吸引了研究人员的广泛的关注，详细内容可见参考文献 [12,37,39,47-55]。利用分解集 $\boldsymbol{B}[-k_1, k_2](q)$ 得到的校验矩阵构造得到的码，我们能够纠正字符 $x \in \mathbb{Z}_q$ 变成字符 $x + e$ 的错误，这里 $e \in [-k_1, k_2]$。

就在闪存中的应用而言，人们在研究分解集的时候，主要关注三个方面：完美分解集的存在性及其构造；准完美分解集的存在性及其构造；给定参数时，最大的分解集的构造。当 $k_1 = 0$ 时，文献 [37] 给出了一个完美分解集的构造。文献 [43,48] 对 $k_1 = k_2$ 时的一些完美分解集做了研究。当 $1 \leqslant k_1 < k_2$ 时，文献 [12,47,52] 构造了一些完美分解集。Wodar 在 1991 年给出了当 $k_1 = 0$ 时，纯奇异完美分解集存在的必要条件。在文献 [12,50] 中，Moshe Schwartz 对一般的 $1 \leqslant k_1 < k_2$ 给出了完美分解集存在的必要条件。张韬等人在文献 [51-53] 中证明了当 $1 \leqslant k_1 < k_2$ 并且 $k_1 + k_2$ 是奇数的时候，非奇异完美分解集是不存在的。2020 年，袁平之等人给出了当 $k_1 = 1, k_2 = 3$ 时，非奇异完美分解集存在的充分必要条件。当 $k_1 = k_2 = 4$ 时，Tamm[46] 列出了很多使得完美分解集存在的素数 q。2011 年，T. Kløve 等人[56] 给出了当 $k_1 = 0$ 时，准完美分解集的一种构造。2012 年，T. Kløve 和罗金权等人[48] 构造了几类满足条件 $k_1 = k_2$ 的准完美分解集。文献 [51] 给出了一些满足条件 $1 \leqslant k_1 < k_2$ 的准完美分解集的构造。当 $0 \leqslant k_1 \leqslant k_2 \leqslant 4$ 时，一些最大分解集的构造可以在文献 [39,47-48,55-56] 中找到。

本章中，我们首先给出三大类完美分解集的存在性的充分必要条件并给出具体的构造方法——具体地说，我们彻底解决了当 $k_2 = 4$ 的时候，非奇异完美分解集的存在性及其构造的问题。其次，我们给出准完美分解集的四种新的构造方法。

2.2　准备工作

本节中，我们给出必要的记号、定义以及一些在后续内容中会用到的结论。

2.2.1　一些记号

- 给定两个整数 m, n，满足条件 $m \leqslant n$，我们用 $[m, n]$ 表示集合 $\{x \mid x\text{是整数且}m \leqslant x \leqslant n\}$。此外，我们用 $[m, n]^*$ 表示 $[m, n] \setminus \{0\}$。
- 对任何一个大于等于 2 的整数 q，用 $\mathbb{Z}_q$ 表示模 q 的剩余类环。
- 我们用 $\mathbb{Z}$ 表示所有整数构成的集合。
- 如果 $a \in \mathbb{Z}_q$ 且 $S \subseteq \mathbb{Z}$，我们用 aS 表示集合 $\{as \pmod q \mid s \in S\}$。
- 对于一个群 G 以及它的一个子集 S，我们用 $\langle S \rangle$ 表示 G 的由 S 生成的子群。
- 设 p 是素数，令 $\mathbb{Z}_p^* \triangleq \mathbb{Z}_p \setminus \{0\}$。众所周知，$\mathbb{Z}_p^*$ 是一个循环群；若 $\mathbb{Z}_p^* = \langle g \rangle$，即 $\mathbb{Z}_p^*$ 由 g 生成，则称 g 是一个模 p 的本原根。此时对于任何一个 $b \in \mathbb{Z}_p^*$，必存在唯一的整数 $i \in [0, p-1]$ 使得 $g^i = b$，我们将这样的 i 记为 $\mathrm{ind}_g(b)$。对任意的 $x \in \mathbb{Z}_p^*$，令 $\mathrm{ord}_p(x)$ 表示 x 在群 $\mathbb{Z}_p^*$ 中的阶数。
- 给定任一个有限集 A，我们用 $|A|$ 表示 A 的大小，即 A 所包含的元素的个数。

2.2.2　一些定义

定义 2.1 (分解集)　设 $q, k_1, k_2 \in \mathbb{Z}$ 且满足 $q \geqslant 2$，$0 \leqslant k_1 \leqslant k_2$，设 $\boldsymbol{B}$ 是 $\mathbb{Z}_q$ 的一个子集。如果对每一个 $b \in \boldsymbol{B}$，集合 $b\left[-k_1, k_2\right]^*$ 都有 $k_1 + k_2$ 个非零元素，并且这些集合两两不相交，则称 $\boldsymbol{B}$ 是一个分解集（splitter set）。我们把这样的分解集记作 $\boldsymbol{B}[-k_1, k_2](q)$ 集。

由以上定义可知，若 $\boldsymbol{B}$ 是一个 $\boldsymbol{B}[-k_1, k_2](q)$ 集，则 $|\boldsymbol{B}| \leqslant \frac{q-1}{k_1+k_2}$。如果 $|\boldsymbol{B}| = \frac{q-1}{k_1+k_2}$，我们称 $\boldsymbol{B}$ 是完美的（perfect）。很显然，只有当 $q \equiv 1 \pmod{k_1 + k_2}$ 时，完美 $\boldsymbol{B}[-k_1, k_2](q)$ 集才存在。如果 $q \not\equiv 1 \pmod{k_1 + k_2}$，且 $|\boldsymbol{B}| = \lfloor \frac{q-1}{k_1+k_2} \rfloor$，则我们称 $\boldsymbol{B}$ 是准完美的（quasi-perfect）。当 $\gcd(q, k_2!) = 1$ 的时候，我们称一个 $\boldsymbol{B}[-k_1, k_2](q)$ 集是非奇异的（nonsingular）；否则的话，我们称 $\boldsymbol{B}[-k_1, k_2](q)$ 集是奇异的（singular）。

分解集的概念与下面这个群论中的概念有着密切的联系。

定义 2.2　设 $(G,\cdot)$ 是一个有限交换群，A, B 是 G 的两个子集。如果给定 G 中任一个元素 g，都存在唯一的 $a \in A$ 以及 $b \in B$ 使得 $g = a \cdot b$，则我们称 $G = A \cdot B$ 是 G 的一个唯一分解，并称 A（或 B）是 G 的一个分解因子。

注　当 $p > k_1 + k_2$ 是一个素数时，我们可以将 $[-k_1, k_2]^*$ 看作 $\mathbb{Z}_p^*$ 的子集。根据分解集和唯一分解的定义，我们可以看出 B 是一个完美 $B[-k_1, k_2](p)$ 集当且仅当 $\mathbb{Z}_p^* = B[-k_1, k_2]^*$ 是一个唯一分解。

2.2.3　一些有用的结论

下面两个定理来自于文献 [47,50]。

定理 2.1　[50] 假设存在一个完美 $B[-k_1, k_2](q)$ 集，则对于 q 的任何一个与 $k_2!$ 互素的正因子 d，存在一个完美的 $B[-k_1, k_2](\frac{q}{d})$ 集。

定理 2.2　[47] 设 B_1 是一个 $B\left[-k_1, k_2\right]\left(q_1\right)$ 集，B_2 是一个 $B\left[-k_1, k_2\right]\left(q_2\right)$ 集，其中 $\gcd\left(q_2, k_2!\right) = 1$。令

$$B_1 \odot B_2 = \left\{c + rq_1 : \ c \in B_1, r \in \left[0, q_2 - 1\right]\right\} \cup \left\{q_1 c : \ c \in B_2\right\}.$$

则

1) $B_1 \odot B_2$ 是一个 $B\left[-k_1, k_2\right]\left(q_1 q_2\right)$ 集；

2) $\left|B_1 \odot B_2\right| = q_2\left|B_1\right| + \left|B_2\right|$；

3) 若 B_1 和 B_2 都是完美的，则 $B_1 \odot B_2$ 也是完美的。

由以上两个定义，我们很容易看出：存在一个非奇异完美 $B[-k_1, k_2](q)$ 集当且仅当对 q 的每个素因子 p，存在一个非奇异 $B[-k_1, k_2](p)$ 集。因此本章接下来的内容中，当谈及非奇异完美 $B[-k_1, k_2](p)$ 集的时候，我们总假设 p 是一个素数。

我们在后面的内容中会经常用到下面这个关于非奇异完美 $B[-k_1, k_2](p)$ 集存在性的必要条件。

引理 2.3　[51] 设 k_1, k_2 是两个满足 $0 \leqslant k_1 \leqslant k_2$ 的整数，p 是一个素数。如果 B 是一个完美 $B[-k_1, k_2](p)$ 集，则对于任何的 $a \in \mathbb{Z}_p^*$，$|B \cap a[-k_1, k_2]^*| = 1$ 都成立。

2.3　完美分解集存在性的等价条件及其构造

在本节中，我们将给出非奇异完美 $B[-k_1, k_2](p)$ 集存在的充分必要条件，其中 $(k_1, k_2) \in \{(0,4),(2,4),(4,4)\}$，且 $p \equiv 1 \pmod{k_1 + k_2}$ 是一个素数。由于当 $1 \leqslant k_1 < k_2$ 且 $k_1 + k_2$ 时不存在非奇异完美 $B[-k_1, k_2](p)$ 集[53]，因此我们完全

解决了当 $k_2 = 4$ 的时候，非奇异完美 $\boldsymbol{B}[-k_1, k_2](p)$ 集存在性的问题。

2.3.1　完全刻画

首先，我们有下面这个引理。这个引理告诉我们非奇异完美分解集要满足的一个必要条件。

引理 2.4　设 k 是一个正整数，$p \equiv 1 \pmod{2k+2}$ 是一个素数。设 $\boldsymbol{B}$ 是一个非奇异的完美 $\boldsymbol{B}[-k, k+2](p)$ 集。如果 $i \in \boldsymbol{B}$，则

$$i\left\langle -\frac{k+1}{k+2}\right\rangle \subseteq \boldsymbol{B},$$

这里 $\left\langle -\frac{k+1}{k+2}\right\rangle$ 表示乘法群 $\mathbb{Z}_p^*$ 中由 $-\frac{k+1}{k+2}$ 生成的子群。特别地，元素 $-\frac{k+1}{k+2}$ 在群 $\mathbb{Z}_p^*$ 中的阶数是奇数。

证明　因为 $\boldsymbol{B}$ 是一个非奇异的完美 $\boldsymbol{B}[-k, k+2](p)$ 集，所以根据引理2.3，对于任意的 $a \in \mathbb{Z}_p^*$，等式 $|\boldsymbol{B} \cap a[-k, k+2]^*| = 1$ 都成立。对 $\boldsymbol{B}$ 中任何一个给定的元素 i，取 $a = i$，我们得到

$$\left|\boldsymbol{B} \cap i[-k, k+2]^*\right| = 1. \tag{2.1}$$

因为 $i \in \boldsymbol{B} \cap i[-k, k+2]^*$ 并且 $-i \in i[-k, k+2]^*$，所以 $-i \notin \boldsymbol{B}$。接下来，取 $a = \pm\frac{i}{k+2}$，则可以得到下面的式子

$$\left|\boldsymbol{B} \bigcap \frac{i}{k+2}[-k, k+2]^*\right| = 1, \tag{2.2}$$

$$\left|\boldsymbol{B} \bigcap \left(-\frac{i}{k+2}\right)[-k, k+2]^*\right| = 1. \tag{2.3}$$

根据式子 (2.2) 以及 $i \in \boldsymbol{B} \bigcap \frac{i}{k+2}[-k, k+2]^*$ 这个事实，我们得到 $\boldsymbol{B} \bigcap \frac{i}{k+2}[-k, k+1]^* = \varnothing$。注意到 $\left(-\frac{i}{k+2}\right)[-k, k+2]^* = \left(\frac{i}{k+2}[-k, k]^*\right) \bigcup \{-\frac{k+1}{k+2}i, -i\}$，于是利用（2.3）我们能推出 $-\frac{k+1}{k+2}i \in \boldsymbol{B}$。接下来用 $-\frac{k+1}{k+2}i$ 替换（2.1），（2.2），（2.3）中的 i，然后重复上述推导过程，我们可得到 $i\left\langle -\frac{k+1}{k+2}\right\rangle \subseteq \boldsymbol{B}$。若 $\mathrm{ord}_p(-\frac{k+1}{k+2})$ 是偶数，则 $-1 \in \left\langle -\frac{k+1}{k+2}\right\rangle$。所以 $-i \in \boldsymbol{B}$，矛盾。因此 $\mathrm{ord}_p(-\frac{k+1}{k+2})$ 是奇数。 ∎

下面的引理可以由文献 [57] 中的引理 2.3 和引理 2.5 推出。在这里我们简略地陈述其证明过程，因为这个过程告诉了我们怎么得到一个分解集。

引理 2.5　设 $k_2 \geqslant k_1 \geqslant 0$ 是两个非负整数，$p \equiv 1 \pmod{k_1 + k_2}$ 是一个素数，以及 $\boldsymbol{M} = [-k_1, k_2]^*$，则存在一个非奇异完美 $\boldsymbol{B}[-k_1, k_2](p)$ 集当且仅当 $\boldsymbol{M}$ 是子群 $\boldsymbol{H} = \langle -1, 2, \cdots, k_2\rangle \subset \mathbb{Z}_p^*$ 的一个分解因子。

证明　设 $\boldsymbol{B}$ 是一个非奇异完美 $\boldsymbol{B}[-k_1, k_2](p)$ 集。令 $\boldsymbol{B}' = \boldsymbol{B} \cap \boldsymbol{H}$，则容易验证 $\boldsymbol{H} = \boldsymbol{M}\boldsymbol{B}'$ 是一个唯一分解。

现在设 $H = MB'$ 是一个唯一分解。令 $\{b_1, \cdots, b_s\}$ 是 H 在 $\mathbb{Z}_p^*$ 中的所有陪集代表元构成的集合，则 $B = \bigcup_{i=1}^{s} b_i B'$ 是一个非奇异完美 $B[-k_1, k_2](p)$ 集。 ∎

现在，我们可以给出本节中的主要结果了。

定理 2.6　令 $p \equiv 1 \pmod 6$ 是一个素数，则存在一个非奇异完美 $B[-2,4](p)$ 集当且仅当 $\mathrm{ord}_p(-\frac{3}{4})$ 是奇数，并且 $2 \notin \langle 6, 8\rangle$。

证明　必要性可以由引理2.4和文献 [51] 中的定理 5.8 直接得到。下面我们来证明充分性。首先，很容易验证下面的式子（2.4）：

$$(-1)^x 2^y 3^z = \begin{cases} (-1)^{x+\frac{y-z}{3}} \cdot 6^{\frac{y+2z}{3}} \left(-\frac{4}{3}\right)^{\frac{y-z}{3}}, & \text{若} y \equiv z \pmod 3, \\ (-1)^{x+\frac{y-z-1}{3}} \cdot 2 \cdot 6^{\frac{y+2z-1}{3}} \left(-\frac{4}{3}\right)^{\frac{y-z-1}{3}}, & \text{若} y \equiv z+1 \pmod 3, \\ 3 \cdot 6^{\frac{y+2z-2}{3}} \left(-\frac{4}{3}\right)^{\frac{y-z+1}{3}}, & \text{若} y \equiv z+2 \pmod 3 \text{且} x + \frac{y-z+1}{3} \text{是偶数}, \\ 4 \cdot 6^{\frac{y+2z-2}{3}} \left(-\frac{4}{3}\right)^{\frac{y-z-2}{3}}, & \text{若} y \equiv z+2 \pmod 3 \text{且} x + \frac{y-z+1}{3} \text{是奇数}. \end{cases} \tag{2.4}$$

式子（2.4）说明 $\langle -1, 2, 3\rangle \subseteq M\langle 6, -\frac{4}{3}\rangle$，这里 $M = [-2,4]^*$。另一方面，对任何的 $s, t \geqslant 0$，等式 $6^s \left(-\frac{4}{3}\right)^t = (-1)^t 2^{s+2t} 3^{s-t}$ 均成立。因此根据引理2.5，我们只需要验证 $\langle -1, 2, 3\rangle = MB$ 是一个唯一分解即可，其中

$$B = \begin{cases} \left\langle 6, -\frac{4}{3} \right\rangle, & \text{如果} \mathrm{ord}_p(6) \text{ 是奇数}, \\ \left\langle 6, -\frac{4}{3} \right\rangle / \{1, -1\}, & \text{如果} \mathrm{ord}_p(6) \text{ 是偶数}. \end{cases}$$

注意到当 $\mathrm{ord}_p(6)$ 是偶数的时候，$-1 \in \left\langle 6, -\frac{4}{3} \right\rangle$。因此式子 $B = \left\langle 6, -\frac{4}{3} \right\rangle / \{1, -1\}$ 的含义为：对任何一个 $i \in \left\langle 6, -\frac{4}{3} \right\rangle$，$B$ 都恰好包含 i 和 $-i$ 中的一个。

因为 $p \equiv 1 \pmod 6$，我们可以假设 $p = 2^a 3^b c + 1$，其中 $a, b, c \geqslant 1$ 且满足 $\gcd(c, 6) = 1$。令 g 是一个模 p 的本原根，并假设

$$\begin{aligned} 2 &\equiv g^{2^{u_1} 3^{v_1} r_1} \pmod p, \\ 3 &\equiv g^{2^{u_2} 3^{v_2} r_2} \pmod p, \\ -1 &\equiv g^{2^{a-1} 3^b c} \pmod p, \end{aligned}$$

其中 $u_1 u_2, v_1, v_2 \geqslant 0, r_1, r_2 \geqslant 1$，$2 \nmid r_1 r_2$，$3 \nmid r_1 r_2$，以及 $2^{u_1} 3^{v_1} r_1, 2^{u_2} 3^{v_2} r_2 < p - 1$。

容易看出

$$\mathrm{ind}_g(4) \equiv 2 \times \mathrm{ind}_g(2) \pmod{p-1}$$

以及

$$\mathrm{ind}_g(-\frac{3}{4}) \equiv 2^{u_2} 3^{v_2} r_2 - \mathrm{ind}_g(4) + 2^{a-1} 3^b c \pmod{p-1},$$

所以 $\mathrm{ord}_p(-\frac{3}{4})$ 是奇数当且仅当

$$2^{u_2}3^{v_2}r_2 - 2^{u_1+1}3^{v_1}r_1 + 2^{a-1}3^b c \equiv 0 \pmod{2^a}. \tag{2.5}$$

根据同余式（2.5），如果 $\min\{u_1+1, u_2\} \geqslant a$，则 $2^a \mid 2^{a-1}3^b c$，这不可能。类似地，如果 $\max\{u_1+1, u_2\} \geqslant a$，则 $\min\{u_1+1, u_2\} = a-1$；如果 $\max\{u_1+1, u_2\} \leqslant a-1$，则 $u_1 + 1 = u_2 \leqslant a-2$。因此，$u_1$ 和 u_2 的取值只有以下三种可能性：

$$\begin{cases} u_2 = a-1, & \text{如果} u_1 \geqslant a-1; \\ u_2 \geqslant a, & \text{如果} u_1 = a-2; \\ u_2 = u_1 + 1, & \text{其他情况。} \end{cases} \tag{2.6}$$

因为 $6 = 2 \times 3$ 且 $8 = 2^3$，所以

$$6 \equiv g^{2^{u_1}3^{v_1}r_1 + 2^{u_2}3^{v_2}r_2} \pmod{p}$$

以及

$$8 \equiv g^{2^{u_1}3^{v_1+1}r_1} \pmod{p}.$$

令 $d = \gcd\left(2^{u_1}3^{v_1}r_1 + 2^{u_2}3^{v_2}r_2, 2^{u_1}3^{v_1+1}r_1\right)$，则 $\langle 6, 8\rangle = \langle g^{2^{u_1}3^{v_1}r_1 + 2^{u_2}3^{v_2}r_2}, g^{2^{u_1}3^{v_1+1}r_1}\rangle = \langle g^d\rangle$。在下面的证明中，我们将频繁地用到这个事实。

断言 2.6.1　$v_1 = v_2$。

断言*2.6.1*的证明：我们将这个证明分成四种情况讨论。

如果 $u_1 \geqslant u_2$ 且 $v_1 > v_2$，则

$$d = 2^{u_2}3^{v_2}\gcd\left(2^{u_1-u_2}3^{v_1-v_2}r_1 + r_2, 2^{u_1-u_2}3^{v_1-v_2+1}r_1\right).$$

令 $r = \gcd\left(2^{u_1-u_2}3^{v_1-v_2}r_1 + r_2, 2^{u_1-u_2}3^{v_1-v_2+1}r_1\right)$。容易看出 $2 \nmid r$ 且 $3 \nmid r$，所以 $r \mid r_1$。这样一来我们能得到 $d \mid 2^{u_2}3^{v_2}r_1$，于是 $d \mid 2^{u_1}3^{v_1}r_1$。所以 $2 \in \langle 6, 8\rangle$，矛盾。

如果 $u_1 \geqslant u_2$ 且 $v_1 < v_2$，则

$$d = 2^{u_2}3^{v_1}\gcd\left(2^{u_1-u_2}r_1 + 3^{v_2-v_1}r_2, 2^{u_1-u_2}3r_1\right).$$

如果 $u_1 < u_2$ 且 $v_1 > v_2$，则

$$d = 2^{u_1}3^{v_2}\gcd\left(3^{v_1-v_2}r_1 + 2^{u_2-u_1}r_2, 3^{v_1-v_2+1}r_1\right).$$

如果 $u_1 < u_2$ 且 $v_1 < v_2$ 则

$$d = 2^{u_1}3^{v_1}\gcd\left(r_1 + 2^{u_2-u_1}3^{v_2-v_1}r_2, 3r_1\right).$$

和第一种情况推导过程类似，从后面三种情况的每一种情况我们都能够推出 $2 \in \langle 6, 8\rangle$，矛盾。到此，我们完成了断言2.6.1的证明。

断言 2.6.2　$v_1 = v_2 \leqslant b-1$。

断言*2.6.2*的证明：通过计算，我们得到

$$\begin{aligned}|\langle -1,2,3\rangle| &= \frac{p-1}{\gcd\left(\mathrm{ind}_g(-1),\mathrm{ind}_g(2),\mathrm{ind}_g(3),p-1\right)}\\ &= \frac{p-1}{\gcd\left(2^{u_1}3^{v_1}r_1, 2^{u_2}3^{v_2}r_2, 2^{a-1}3^b c\right)},\end{aligned}$$

以及

$$\begin{aligned}|\langle 6,8\rangle| &= \frac{p-1}{\gcd(d,p-1)}\\ &= \frac{p-1}{\gcd\left(2^{u_1}3^{v_1}r_1 + 2^{u_2}3^{v_2}r_2, 2^{u_1}3^{v_1+1}r_1, 2^a 3^b c\right)}.\end{aligned}$$

根据断言2.6.1，$v_1 = v_2$ 恒成立。下面我们用反证法来证明断言2.6.2。如果 $v \triangleq v_1 = v_2 \geqslant b$，则

$$\begin{aligned}&\frac{|\langle -1,2,3\rangle|}{|\langle 6,8\rangle|}\\ =&\frac{\gcd\left(2^{u_1}3^{v}r_1 + 2^{u_2}3^{v}r_2, 2^{u_1}3^{v+1}r_1, 2^a 3^b c\right)}{\gcd\left(2^{u_1}3^{v}r_1, 2^{u_2}3^{v}r_2, 2^{a-1}3^b c\right)}\\ =&\frac{\gcd\left(2^{u_1}3^{v-b}r_1 + 2^{u_2}3^{v-b}r_2, 2^{u_1}3^{v-b+1}r_1, 2^a c\right)}{\gcd\left(2^{u_1}3^{v-b}r_1, 2^{u_2}3^{v-b}r_2, 2^{a-1}c\right)}.\end{aligned}$$

若 $u_1 + 1 = u_2 \leqslant a-2$，则

$$\begin{aligned}&\frac{|\langle -1,2,3\rangle|}{|\langle 6,8\rangle|}\\ =&\frac{\gcd\left(3^{v-b}r_1 + 2\cdot 3^{v-b}r_2, 3^{v-b+1}r_1, 2^{a-u_1}c\right)}{\gcd\left(3^{v-b}r_1, 2\cdot 3^{v-b}r_2, 2^{a-1-u_1}c\right)}\\ =&\frac{\gcd\left(r_1+r_2, r_1, c\right)}{\gcd\left(r_1, r_2, c\right)} = 1.\end{aligned}$$

另一方面，容易看出 $\langle 6,8\rangle \subseteq \langle -1,2,3\rangle$，所以 $\langle 6,8\rangle = \langle -1,2,3\rangle$，这与 $2 \notin \langle 6,8\rangle$ 矛盾。

类似地，如果 $u_1 \geqslant a-1, u_2 = a-1$，则

$$\begin{aligned}&\frac{|\langle -1,2,3\rangle|}{|\langle 6,8\rangle|}\\ =&\frac{\gcd\left(2^{u_1-u_2}3^{v-b}r_1 + 3^{v-b}r_2, 2^{u_1-u_2}3^{v-b+1}r_1, 2c\right)}{\gcd\left(2^{u_1-u_2}3^{v-b}r_1, 3^{v-b}r_2, c\right)}\\ =&1.\end{aligned}$$

如果 $u_1 = a-2, u_2 \geqslant a$，则

$$\begin{aligned}&\frac{|\langle -1,2,3\rangle|}{|\langle 6,8\rangle|}\\ =&\frac{\gcd\left(3^{v-b}r_1 + 2^{u_2-u_1}3^{v-b}r_2, 3^{v-b+1}r_1, 4c\right)}{\gcd\left(3^{v-b}r_1, 2^{u_2-u_1}3^{v-b}r_2, 2c\right)}\\ =&1.\end{aligned}$$

所以对于以上两种情况而言，我们都能得出 $\langle 6,8\rangle = \langle -1,2,3\rangle$，这与 $2 \notin \langle 6,8\rangle$ 矛盾。

至此，我们完成了断言2.6.2的证明。

根据断言2.6.1和断言2.6.2，从现在开始，我们令 $v \triangleq v_1 = v_2$，则 $v \leqslant b-1$。注意到

$$\mathrm{ord}_p(6) = \frac{p-1}{\gcd(2^{u_1}3^v r_1 + 2^{u_2}3^v r_2, p-1)},$$

所以容易看出 $\mathrm{ord}_p(6)$ 是奇数当且仅当 $2^{u_1}3^v r_1 + 2^{u_2}3^v r_2 \equiv 0 \pmod{2^a}$。我们还能通过计算得到下面的式子（2.7）和（2.8）：

$$\frac{|\langle -1,2,3\rangle|}{\left|\left\langle 6, -\frac{3}{4}\right\rangle\right|} = \frac{\gcd\left(2^{u_1}3^v r_1 + 2^{u_2}3^v r_2, 2^{u_2}3^v r_2 - 2^{u_1+1}3^v r_1 + 2^{a-1}3^b c, 2^a 3^b c\right)}{\gcd\left(2^{u_1}3^v r_1, 2^{u_2}3^v r_2, 2^{a-1}3^b c\right)} \tag{2.7}$$

$$= \frac{\gcd\left(2^{u_1} r_1 + 2^{u_2} r_2, 2^{u_2} r_2 - 2^{u_1+1} r_1 + 2^{a-1}3^{b-v} c, 2^a 3^{b-v} c\right)}{\gcd\left(2^{u_1} r_1, 2^{u_2} r_2, 2^{a-1}3^{b-v} c\right)}. \tag{2.8}$$

接下来，我们将证明分成两大类情况讨论。

情形 1：$\mathrm{ord}_p(6)$ 是奇数。

这种情形下，容易看出同余式 $2^{u_1}3^v r_1 + 2^{u_2}3^v r_2 \equiv 0 \pmod{2^a}$ 恒成立。所以要么 $u_1, u_2 \geqslant a$，要么 $u_1 = u_2 \leqslant a-1$。但是式子（2.6）迫使我们只能取到 $u_1 = u_2 = a-1$。这样一来，式子（2.8）就变成了

$$\begin{aligned}\frac{|\langle -1,2,3\rangle|}{\left|\left\langle 6, -\frac{3}{4}\right\rangle\right|} &= \frac{\gcd\left(r_1 + r_2, r_2 + 3^{b-v}c - 2r_1, 2\times 3^{b-v}c\right)}{\gcd\left(r_1, r_2, 3^{b-v}c\right)}\\ &= \frac{\gcd\left(r_1 + r_2, r_2 + 3^{b-v}c - 2r_1, 2\times 3^{b-v}c\right)}{\gcd\left(r_1, r_2, c\right)}.\end{aligned}$$

因为 $u_1 = u_2 = a-1$，所以

$$d = 2^{u_2}3^v \gcd\left(r_1 + r_2, 3r_1\right).$$

如果 $3 \nmid \gcd\left(r_1 + r_2, 3r_1\right)$，则 $d \mid \mathrm{ind}_g(2)$，所以 $2 \in \langle 6,8\rangle$，矛盾。于是同余式 $r_1 + r_2 \equiv 0 \pmod 3$ 必然成立。这样一来，很容易验证

以下两个整除关系：$2 \mid \gcd\left(r_1+r_2, r_2+3^{b-v}c-2r_1, 2\cdot 3^{b-v}c\right)$ 以及 $3 \mid \gcd\left(r_1+r_2, r_2+3^{b-v}c-2r_1, 2\cdot 3^{b-v}c\right)$。因此，考虑到 $2 \nmid r_1r_2$，$3 \nmid r_1r_2$ 以及 $\gcd(c,6)=1$，我们可推出

$$\frac{\gcd\left(r_1+r_2, r_2+3^{b-v}q-2r_1, 2\cdot 3^{b-v}c\right)}{\gcd\left(r_1, r_2, c\right)} \geqslant 6.$$

上面这个不等式表明 $\frac{|\langle -1,2,3\rangle|}{\left|\left\langle 6,-\frac{3}{4}\right\rangle\right|} \geqslant 6$。另一方面，

$$|\langle -1,2,3\rangle| = \left|M\left\langle 6,-\frac{3}{4}\right\rangle\right| \leqslant |M|\left|\left\langle 6,-\frac{3}{4}\right\rangle\right| = 6\left|\left\langle 6,-\frac{3}{4}\right\rangle\right|.$$

所以，$\langle -1,2,3\rangle = \boldsymbol{MB}$ 是一个唯一分解。

情形 2： $\mathrm{ord}_p(6)$ **是偶数**。

对于这种情况，只需要证明

$$\frac{|\langle -1,2,3\rangle|}{\left|\left\langle 6,-\frac{3}{4}\right\rangle\right|} \geqslant 3.$$

我们分成以下三种子情形讨论。

子情形 1: $u_1 \geqslant a-1, u_2 = a-1$。

这时候，容易得到

$$d = 2^{u_2}3^v \gcd\left(2^{u_1-u_2}r_1+r_2, 2^{u_1-u_2}3r_1\right).$$

如果 $3 \nmid \gcd\left(2^{u_1-u_2}r_1+r_2, 2^{u_1-u_2}3r_1\right)$，则 $2 \in \langle 6,8\rangle$，矛盾。于是 $r_2+2^{u_1-u_2}r_1 \equiv 0 \pmod 3$，因此 $r_2-2^{u_1-u_2+1}r_1 \equiv 0 \pmod 3$。则从式子（2.8）可以得到

$$\frac{|\langle -1,2,3\rangle|}{\left|\left\langle 6,-\frac{3}{4}\right\rangle\right|} \geqslant 3.$$

子情形 2: $u_1 = a-2, u_2 \geqslant a$。

这时候，等式

$$d = 2^{u_1}3^v \gcd\left(r_1+2^{u_2-u_1}r_2, 3r_1\right).$$

成立。如果 $3 \nmid \gcd\left(r_1+2^{u_2-u_1}r_2, 3r_1\right)$，则 $2 \in \langle 6,8\rangle$，矛盾。于是 $r_1+2^{u_2-u_1}r_2 \equiv 0 \pmod 3$，所以 $2^{u_2-u_1}r_2-2r_1 \equiv 0 \pmod 3$。则从式子（2.8）我们得到

$$\frac{|\langle -1,2,3\rangle|}{\left|\left\langle 6,-\frac{3}{4}\right\rangle\right|} \geqslant 3.$$

子情形 3: $u_1+1 = u_2 \leqslant a-2$。

这时候，易得到

$$d = 2^{u_1}3^v \gcd\left(r_1+2r_2, 3r_1\right).$$

如果 $3 \nmid \gcd\left(r_1+2r_2, 3r_1\right)$，则 $2 \in \langle 6,8\rangle$，矛盾。于是 $r_1+2r_2 \equiv 0 \pmod 3$，因此 $r_2-r_1 \equiv 0 \pmod 3$。则从式子（2.8）我们得到

$$\frac{|\langle -1,2,3\rangle|}{|\left\langle 6,-\frac{3}{4}\right\rangle|} \geqslant 3.$$

∎

定理 2.7　设 $p \equiv 1 \pmod 8$ 是一个素数，则存在一个非奇异完美 $B[-4,4](p)$ 集当且仅当 $\pm 4 \notin \langle 6,16\rangle$。

证明　我们先证明必要性。假设 B 是一个非奇异完美 $B[-4,4](p)$ 集。令 $\pm B = B \cup (-B)$，$M = \{\pm 1, \pm 2, \pm 3, \pm 4\}$ 以及 $M' = \{1,2,3,4\}$。因为 B 是一个完美 $B[-4,4](p)$ 集，所以根据引理2.3，对于任何一个 $a \in \mathbb{Z}_p^*$，等式 $|B \cap aM| = 1$ 都成立。容易验证 $|B \cap aM| = 1$ 当且仅当 $|(\pm B) \cap aM'| = 1$。类似地，$\mathbb{Z}_p^* = MB$ 是一个唯一分解当且仅当 $\mathbb{Z}_p^* = M'(\pm B)$ 是唯一分解。

注意到，如果 $\mathbb{Z}_p^* = MB$ 是唯一分解，则 $\mathbb{Z}_p^* = MB'$ 也是唯一分解，其中 $B' = b^{-1}B$（对某个 $b \in B$）。因此不失一般性，我们可以假设 $1 \in \pm B$。如果 $r \in \pm B$, 则由 $|\pm B \cap rM'| = 1$, 我们可以得到 $2r, 3r, 4r \notin \pm B$; 由 $|\pm B \cap \frac{1}{2}rM'| = 1$, 我们可以得到 $\frac{3}{2}r \notin \pm B$；由 $|\pm B \cap \frac{1}{3}rM'| = 1$，我们能得到 $\frac{2}{3}r, \frac{4}{3}r \notin \pm B$。因为 $6r = 1 \cdot (6r) = 2 \cdot (3r) = 3 \cdot (2r) = 4 \cdot (\frac{3}{2}r)$，但是 $2r, 3r, \frac{3}{2}r \notin \pm B$，所以 $6r \in \pm B$。由 $|\pm B \cap 2rM'| = 1$，$|\pm B \cap 3rM'| = 1$ 以及 $|\pm B \cap 4rM'| = 1$，我们可推出 $8r, 9r, 12r \notin \pm B$，$16r \in \pm B$。

根据以上讨论以及 $1 \in \pm B$ 这个事实，容易看出 $\langle 6,16\rangle \subseteq \pm B$ 且 $\langle 6,16\rangle \cap \{\pm 2, \pm 3, \pm 4, \pm 8, \pm\frac{2}{3}, \pm\frac{4}{3}\} = \varnothing$。由此可导出 $\pm 4 \notin \langle 6,16\rangle$。

接下来我们证明充分性。假设 $\pm 4 \notin \langle 6,16\rangle$, 则 $2, 4, 8 \notin \langle 6,16\rangle$（若 $8 \in \langle 6,16\rangle$, 则 $2 \in \langle 6,16\rangle$）以及 $16 \in \langle 6,16\rangle$。所以 $2\langle 6,16\rangle$ 在商群 $\langle -1,2,3\rangle/\langle 6,16\rangle$ 中的阶数是 4。因为 $3 \times 16 = 8 \times 6$，所以 $3\langle 6,16\rangle = 8\langle 6,16\rangle$。这样一来，$2\langle 6,16\rangle$ 在 $\langle -1,2,3\rangle/\langle 6,16\rangle$ 中生成的子群就是

$$\langle 2\langle 6,16\rangle\rangle = \{\langle 6,16\rangle, 2\langle 6,16\rangle, 3\langle 6,16\rangle, 4\langle 6,16\rangle\}.$$

特别地，$|\langle -1,2,3\rangle| \geqslant 4|\langle 6,16\rangle|$。

断言　$-1 \in \langle 6,16\rangle$。

对该断言的证明：因为 $p \equiv 1 \pmod 8$，我们可以假设 $p = 2^b c + 1$，其中 b, c 是正整数并且满足 $b \geqslant 3$ 以及 $\gcd(c,2) = 1$。令 g 是一个模 p 的本原根，并做如下假设

$$2 \equiv g^{2^{u_1} r_1} \pmod p \text{ 以及} 3 \equiv g^{2^{u_2} r_2} \pmod p.$$

其中 $u_1, u_2 \geqslant 0, r_1, r_2 \geqslant 1$ 是整数并且 $2 \nmid r_1 r_2$。令 $d = \gcd(2^{u_1} r_1 + 2^{u_2} r_2, 2^{u_1+2} r_1)$，则 $\langle 6, 16\rangle = \langle g^d \rangle$。

如果 $u_1 > u_2$，则 $d = 2^{u_2} \gcd(2^{u_1-u_2} r_1 + r_2, 2^{u_1-u_2+2} r_1) = 2^{u_2} \gcd(r_1, r_2)$。这样的话，容易看出 $d \mid 2^{u_1} r_1$ 以及 $2 \in \langle 6, 16\rangle$，矛盾。类似地，如果 $u_1 < u_2$，我们也能够推出 $2 \in \langle 6, 16\rangle$。因此，$u_1 = u_2$。接下来我们总假设 $u \triangleq u_1 = u_2$。这样的话，$d = 2^u \gcd(r_1 + r_2, 4r_1)$。若 $4 \nmid (r_1 + r_2)$，则 $d = 2^{u+1} \gcd(r_1, r_2)$。所以 $d \mid 2^{u+1} r_1$ 并且 $4 \in \langle 6, 16\rangle$，矛盾。这说明 $4 \mid (r_1 + r_2)$ 一定成立。于是，$d = 2^{u+2} \gcd(r_1, r_2)$。如果 $u \geqslant b - 1$，则

$$\begin{aligned}
\frac{|\langle -1, 2, 3\rangle|}{|\langle 6, 16\rangle|} &= \frac{\gcd(2^{u+2} r_1, 2^{u+2} r_2, 2^b c)}{\gcd(2^u r_1, 2^u r_2, 2^{b-1} c)} \\
&= \frac{\gcd(2^{u-b+3} r_1, 2^{u-b+3} r_2, 2c)}{\gcd(2^{u-b+1} r_1, 2^{u-b+1} r_2, c)} \\
&= \frac{2 \times \gcd(2^{u-b+2} r_1, 2^{u-b+2} r_2, c)}{\gcd(r_1, r_2, c)} \\
&= \frac{2 \times \gcd(r_1, r_2, c)}{\gcd(r_1, r_2, c)} = 2.
\end{aligned}$$

这与 $|\langle -1, 2, 3\rangle| \geqslant 4|\langle 6, 16\rangle|$ 矛盾。若 $u = b - 2$，则 $\frac{|\langle -1,2,3\rangle|}{|\langle 6,16\rangle|} = 4$。所以 $\langle -1, 2, 3\rangle = \{1, 2, 3, 4\}\langle 6, 16\rangle$ 是一个唯一分解。这意味着存在某个 $i \in \{1, 2, 3, 4\}$，使得 $-\langle 6, 16\rangle = i\langle 6, 16\rangle$，即 $-i \in \langle 6, 16\rangle$。注意 $\pm 4 \notin \langle 6, 16\rangle$，所以 $i \neq 2, 3, 4$。另一方面，根据 $u = b - 2$ 可以推出

$$|\langle 6, 16\rangle| = \frac{p-1}{\gcd(d, p-1)} = \frac{c}{\gcd(r_1, r_2, c)}$$

是一个奇数。这意味着 $-1 \notin \langle 6, 16\rangle$，于是 $u \leqslant b - 3$。这样的话，

$$\begin{aligned}
|\langle 6, 16\rangle| &= \frac{p-1}{\gcd(2^{u+2} r_1, 2^{u+2} r_2, 2^b c)} \\
&= \frac{2^{b-u-2} c}{\gcd(r_1, r_2, 2^{b-u-2} c)}
\end{aligned}$$

是一个偶数，所以 $-1 \in \langle 6, 16\rangle$。到此，我们完成了该断言的证明。

现在我们继续定理的证明。因为 $-1 \in \langle 6, 16\rangle$，所以 $\langle -1, 2, 3\rangle = \langle 2, 6, 16\rangle = \{1, 2, 3, 4\}\langle 6, 16\rangle$ 是一个唯一分解。令 $a = \gcd\left(\frac{p-1}{2}, \mathrm{ind}_g(6), \mathrm{ind}_g(16)\right)$，则我们有 $\langle 6, 16\rangle = \langle g^a \rangle$。设 u 是最小的满足 $2^u a \nmid \frac{p-1}{2}$ 的正整数，则 $-1 \notin \left\langle g^{2^u a} \right\rangle$。令 S 是 $\left\langle g^{2^u a} \right\rangle$ 在 $\langle 6, 16\rangle$ 中所有陪集代表元构成的集合。因为 $-1 \in \langle 6, 16\rangle$ 并且 $-1 \notin \left\langle g^{2^u a} \right\rangle$，我们可以这样取 S：当 $s \in S$ 时，必有 $-s \in S$。令 $S' = \left\{ s \mid s \in S \text{ 且} 0 \leqslant \mathrm{ind}_g(s) < \frac{p-1}{2} \right\}$，则

$$\langle -1, 2, 3\rangle = \{\pm 1, \pm 2, \pm 3, \pm 4\} \left(\bigcup_{s \in S'} s \left\langle g^{2^u a} \right\rangle \right)$$

是一个唯一分解。因此根据引理2.5，存在一个完美 $B[-4,4](p)$ 集。 ∎

注　我们注意到完美 $B[-4,4](p)$ 集在文献 [46,58] 已经被研究过。但我们的构造更具体，计算过程也更简单。

与定理2.7类似，我们有如下定理。因为其证明过程和定理2.7的证明类似，所以我们简略陈述之。

定理 2.8　设 $p \equiv 1 \pmod 4$ 是一个素数，则存在一个非奇异完美 $B[0,4](p)$ 集当且仅当 $4 \notin \langle 6,16\rangle$。

证明　首先假设 B 是一个非奇异完美 $B[0,4](p)$ 集，并令 $M = \{1,2,3,4\}$。在定理 2.7的证明中，将 M' 和 B' 分别取成 M 和 B，然后用相同的过程我们可得到 $\langle 6,16\rangle \subseteq B$ 以及 $4 \notin \langle 6,16\rangle$。

关于充分性，和定理 2.7的证明一样，$4 \notin \langle 6,16\rangle$ 这个事实意味着

$$\langle 2\langle 6,16\rangle\rangle = \{\langle 6,16\rangle, 2\langle 6,16\rangle, 3\langle 6,16\rangle, 4\langle 6,16\rangle\}.$$

因此 $\langle 1,2,3,4\rangle = \langle 2,6,16\rangle = \{1,2,3,4\}\langle 6,16\rangle$ 是一个唯一分解。根据引理2.5，存在一个完美 $B[0,4](p)$ 集。 ∎

从引理2.5和定理2.6（定理2.7，定理2.8）的证明过程可以看出，如果存在完美 $B[-2,4](p)$ 集（完美 $B[-4,4](p)$ 集，完美 $B[0,4](p)$ 集），则我们可以将其明确地计算出来。

例 2.1　我们用三个例子来展示怎样利用上述几个定理来构造完美分解集，这里我们沿用上面讨论时所用的记号。

1) 在定理2.7中，取 $p = 97$，则通过计算可以得到 $g = 5, \mathrm{ind}_g(6) = 8, \mathrm{ind}_g(4) = 68, \mathrm{ind}_g(-4) = 20, \mathrm{ind}_g(16) = 40$ 以及 $a = 8$。因为 $8x \equiv 68 \pmod{96}$ 没有解，所以 $4 \notin \langle 6,16\rangle$。类似地，可以证明 $-4 \notin \langle 6,16\rangle$。于是根据定理2.7，存在一个完美完美 $B[-4,4](97)$ 集。更进一步地，我们有

$$\langle 6,16\rangle = \{1,6,16,22,35,36,61,62,75,81,91,96\}$$

以及（这里 $u = 2$）

$$\left\langle g^{2^u a}\right\rangle = \left\langle 5^{32}\right\rangle = \{1,35,61\}.$$

取 $S = \{1,6,91,96\}$，$S' = \{1,6\}$。另外，$T = \{1,5\}$ 是 $\langle -1,2,3\rangle$ 在 $\mathbb{Z}_{97}^*$ 里面的所有陪集代表元。所以集合

$$\bigcup_{t\in T}\bigcup_{s\in S'}\left\{sti \pmod{97} \mid i \in \left\langle g^{2^u a}\right\rangle\right\}$$

$$=\{1,5,6,14,16,30,35,61,75,78,80,84\}$$

是一个完美 $B[-4,4](97)$ 集。根据定理2.7, 我们通过跑程序算出了当 $p \leqslant 5000$ 的时候，存在完美 $B[-4,4](p)$ 集当且仅当 $p = 97, 1873, 2161, 3457$。

2) 在定理2.6中，取 $p = 139$，则 $g = 2, \mathrm{ind}_g(2) = 1$，$\mathrm{ind}_g(6) = 42$ 以及 $\mathrm{ind}_g(8) = 3$, 因此 $2 \notin \langle 6, 8\rangle$。容易看出，在 $\mathbb{Z}_{139}$ 中，$-\frac{4}{3} = 45$ 且 $\mathrm{ord}_p(45) = 23$。因此根据定理2.6, 存在一个完美 $B[-2,4](139)$ 集。此时 $\mathrm{ord}_p(6) = 23$ 是奇数, $\mathrm{ind}_g(45) = 30$ 以及 $\gcd(\mathrm{ind}_g(6), \mathrm{ind}_g(45)) = 6$。于是根据定理2.6的证明可知，集合

$$\langle 6, 45\rangle = \{2^{6i} \pmod{139} \mid 0 \leqslant i \leqslant 22\}$$

是一个完美 $B[-2,4](139)$ 集。

3) 在定理2.6中，取 $p = 181$，则 $g = 2, \mathrm{ind}_g(2) = 1$，$\mathrm{ind}_g(6) = 57$ 以及 $\mathrm{ind}_g(8) = 3$, 因此 $2 \notin \langle 6, 8\rangle$。容易看出，在 $\mathbb{Z}_{181}$ 中，$-\frac{4}{3} = 59$ 且 $\mathrm{ord}_p(59) = 5$。因此根据定理2.6, 存在一个完美 $B[-2,4](181)$ 集。此时 $\mathrm{ord}_p(6) = 60$ 是偶数, $\mathrm{ind}_g(59) = 36$ 以及 $\gcd(\mathrm{ind}_g(6), \mathrm{ind}_g(59)) = 3$。则 $\langle 6, 59\rangle = \{2^{3i} \pmod{181} \mid 0 \leqslant i \leqslant 59\}$。于是根据定理2.6的证明可知，集合

$$\{2^{3i} \pmod{181} \mid 0 \leqslant i \leqslant 29\}$$

是一个完美 $B[-2,4](181)$ 集。根据定理2.6, 我们通过跑程序算出了当 $p \leqslant 1000$ 的时候，除了文献中[47] 给的 10 个构造外，存在完美 $B[-2,4](p)$ 集当且仅当 $p = 181, 313, 421, 541, 919, 937$。

2.3.2　特殊参数下更简单的刻画

当 $\frac{p-1}{k_1+k_2}$ 和 $k_1 + k_2$ 互素的时候，对于完美分解集的存在性，我们能给出更简单的刻画。在给出我们的结果之前，我们需要两个简单的引理。

引理 2.9　[51] 设 m 和 n 是两个互素的正整数。如果 $A = \{a_1, \cdots, a_m\}$ 和 $B = \{b_1, \cdots, b_n\}$ 是两个整数集，并且集合

$$A + B := \{a_i + b_j \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\}$$

模 mn 的完全代表元集，则 A 是模 m 的完全代表元集，并且 B 是模 n 的完全代表元集。

引理 2.10　设 $k_2 \geqslant k_1 \geqslant 0$ 是整数，p 是一个素数且满足 $p \equiv 1 \pmod{k_1 + k_2}$ 和 $\gcd\left(k_1 + k_2, \frac{p-1}{k_1+k_2}\right) = 1$。令 g 是一个模 p 的本原元，记 $N = \{\mathrm{ind}_g(j) \mid j \in [-k_1, k_2]^*\}$。则存在一个非奇异完美 $B[-k_1, k_2](p)$ 集当且仅当 N 是一个模 k_1+k_2 的完全代表元集。

证明　我们先证明必要性。令 B 是一个非奇异完美 $B[-k_1, k_2](p)$ 集，$A = \{\mathrm{ind}_g(b) \mid b \in B\}$, 则 $\mathbb{Z}_{p-1} = N + A$ 是一个唯一分解。因为 $\gcd\left(k_1 + k_2, \frac{p-1}{k_1+k_2}\right) = 1$，所以根据引理2.9，$N$ 是一个模 $k_1 + k_2$ 的完全代表元集。

充分性由文献 [47] 中的定理 3 得到。 ∎

下面我们会将引理2.10应用到 $(k_1,k_2)\in\{(2,4),(0,4),(4,4)\}$。首先，容易观察到以下事实：$p\equiv 1 \pmod 6$ 且 $\gcd\left(6,\frac{p-1}{6}\right)=1$ 当且仅当 $p\equiv 7,31 \pmod{36}$；$\gcd\left(4,\frac{p-1}{4}\right)=1$ 等价于 $p\equiv 5 \pmod 8$；$\gcd\left(8,\frac{p-1}{8}\right)=1$ 等价于 $p\equiv 9 \pmod{16}$。

定理 2.11　1) 设 $p\equiv 7,31 \pmod{36}$ 是一个素数，则存在非奇异完美 $B[-2,4](p)$ 集当且仅当 6 在 $\mathbb{Z}_p$ 中是一个三次剩余，并且 2,3 在 $\mathbb{Z}_p$ 中不是三次剩余。

2) 设 $p\equiv 5 \pmod 8$ 是一个素数，则存在非奇异完美 $B[0,4](p)$ 集当且仅当 6 是一个模 p 的四次剩余。

3) 设 $p\equiv 9 \pmod{16}$ 是一个素数，则不存在非奇异完美 $B[-4,4](p)$ 集。

证明　设 g 是一个模 p 的本原根。

1). 先证必要性。假设存在一个非奇异完美 $B[-2,4](p)$ 集。根据引理2.10可知，$N=\{\mathrm{ind}_g(j) \pmod 6 \mid j\in[-2,4]^*\}=\mathbb{Z}_6$。因为 $\mathrm{ind}_g(-j)\equiv \mathrm{ind}_g(j)+\frac{p-1}{2} \pmod{p-1}$，所以 $\mathrm{ind}_g(-j)\equiv \mathrm{ind}_g(j)+3 \pmod 6$。$\mathrm{ind}_g(j)$ 模 6 的所有可能的值如下：

	情形 1	情形 2	情形 3	情形 4
$\mathrm{ind}_g(1) \pmod 6$	0	0	0	0
$\mathrm{ind}_g(-1) \pmod 6$	3	3	3	3
$\mathrm{ind}_g(2) \pmod 6$	1	2	4	5
$\mathrm{ind}_g(-2) \pmod 6$	4	5	1	2
$\mathrm{ind}_g(3) \pmod 6$	5	1	5	1
$\mathrm{ind}_g(4) \pmod 6$	2	4	2	4

所以无论是哪一种情况，整数 2 和 3 不可能是模 p 的三次剩余，并且 6 一定是模 p 的三次剩余。

再证充分性。设 $\mathrm{ind}_g(2)=x$，$\mathrm{ind}_g(3)=y$，则 $\mathrm{ind}_g(6)\equiv x+y \pmod{p-1}$。由 6 是模 p 的三次剩余可知 $x+y\equiv 0 \pmod 3$。此外，因为 2 和 3 都不是模 p 的三次剩余，所以 $\{x,y\}\equiv\{1,2\}$ 或$\{1,5\}$ 或$\{2,4\}$ 或$\{4,5\} \pmod 6$。因为 $p\equiv 7,31 \pmod{36}$，所以 3 不是 $\mathbb{Z}_p$ 中的平方元（见文献 [59] 第 55 页）。综上讨论，我们推出 x 和 y 的取值只能有以下四种可能性。无论是哪一种情况，都很容易看出 $\{\mathrm{ind}_g(j) \pmod 6 \mid j\in[-2,4]^*\}=\mathbb{Z}_6$。再根据引理2.10，我们完成了充分性的证明。

	情形 1	情形 2	情形 3	情形 4
$x \pmod 6$	2	1	5	4
$y \pmod 6$	1	5	1	5

2). 先证明必要性。假设存在一个非奇异完美 $B[0,4](p)$ 集, 则根据引理2.10可以得出 $\{\mathrm{ind}_g(j) \pmod 4 \mid j \in [0,4]^*\} = \mathbb{Z}_4$。因为 $p \equiv 5 \pmod 8$,所以 2 不是一个模 p 的二次剩余（见文献 [59] 的命题 5.1.3）。注意到 $\mathrm{ind}_g(4) \equiv 2 \times \mathrm{ind}_g(2) \pmod 4$, 所以只有两个可能性：$\mathrm{ind}_g(2) \equiv 1 \pmod 4$, $\mathrm{ind}_g(3) \equiv 3 \pmod 4$, $\mathrm{ind}_g(4) \equiv 2 \pmod 4$ 或者 $\mathrm{ind}_g(2) \equiv 3 \pmod 4$, $\mathrm{ind}_g(3) \equiv 1 \pmod 4$, $\mathrm{ind}_g(4) \equiv 2 \pmod 4$。无论哪种情况，我们都有 $\mathrm{ind}_g(6) \equiv \mathrm{ind}_g(2) + \mathrm{ind}_g(3) \equiv 0 \pmod 4$，即 6 是一个模 p 的四次剩余。

再证充分性，设 $\mathrm{ind}_g(2) = x$，$\mathrm{ind}_g(3) = y$。因为 6 是模 p 的四次剩余，所以 $\mathrm{ind}_g(6) \equiv x + y \equiv 0 \pmod 4$。此外，由于 2 不是模 p 的二次剩余，我们得到 $x \equiv 1$或$3 \pmod 4$。因此我们有如下两种情形：

	情形 1	情形 2
$\mathrm{ind}_g(1) \pmod 4$	0	0
$\mathrm{ind}_g(2) \pmod 4$	1	3
$\mathrm{ind}_g(3) \pmod 4$	3	1
$\mathrm{ind}_g(4) \pmod 4$	2	2

无论哪种情形，$\{\mathrm{ind}_g(j) \pmod 4 \mid j \in [0,4]^*\} = \mathbb{Z}_4$ 都成立。证明完成。

3). 因为 $\frac{p-1}{2} \equiv 4 \pmod 8$，所以 $\mathrm{ind}_g(1) \equiv 0 \pmod 8$ 和 $\mathrm{ind}_g(-1) \equiv 4 \pmod 8$ 总是成立。因为 $p \equiv 1 \pmod 8$，所以 2 是模 p 的二次剩余。$\mathrm{ind}_g(2)$ 的取值有以下四种情形：

- $\mathrm{ind}_g(2) \equiv 0 \pmod 8$;
- $\mathrm{ind}_g(2) \equiv 2 \pmod 8$，则 $\mathrm{ind}_g(4) \equiv 4 \pmod 8$;
- $\mathrm{ind}_g(2) \equiv 4 \pmod 8$；则 $\mathrm{ind}_g(-2) \equiv 0 \pmod 8$;
- $\mathrm{ind}_g(2) \equiv 6 \pmod 8$，则 $\mathrm{ind}_g(4) \equiv 4 \pmod 8$。

无论哪一种情形，$\{\mathrm{ind}_g(j) \pmod 8 \mid j \in [-4,4]^*\} = \mathbb{Z}_8$ 都不可能成立。所以不存在非奇异完美 $B[-4,4](p)$ 集。 ∎

对于非奇异完美 $B[-2,4](p)$ 集的存在性，我们可以借助数论的工具给出更具体的刻画。下面讨论中用到的关于数论的术语都可以在文献 [59] 中找到。

令 $\omega = \frac{-1+\sqrt{-3}}{2}$，即复数域上的三次本原单位根。设 p 是一个模 6 余 1 的素数，则我们可以假设 $p = \pi\bar{\pi}$，其中 $\pi = 3m - 1 + 3n\omega$ 是环 $\mathbb{Z}[\omega]$ 中的初等素元（primay prime），而 $\bar{\pi}$ 是 π 的复共轭。由三次互反律和文献 [59] 第九章的习题 5,

可以得到

$$\chi_\pi(2) = \chi_2(\pi) \equiv \pi \pmod 2 \quad 以及 \quad \chi_\pi(3) = \omega^{2n}.$$

因为 2 和 3 不是模 p 的三次剩余(因此也不是模 π 的三次剩余),所以 $\chi_\pi(2), \chi_\pi(3) \neq 1$。这样的话，6 是模 p 的三次剩余当且仅当

$$\begin{cases} \chi_\pi(2) = \omega \\ \chi_\pi(3) = \omega^2 \end{cases} 或者 \begin{cases} \chi_\pi(2) = \omega^2 \\ \chi_\pi(3) = \omega, \end{cases}$$

即，当且仅当

$$\begin{cases} m 是奇数, n 是奇数 \\ n \equiv 1 \pmod 3 \end{cases} 或者 \begin{cases} m 是偶数, n 是奇数 \\ n \equiv 2 \pmod 3 \end{cases}. \tag{2.9}$$

对于式子（2.9）的左边的条件，令 $m = 2k + 1$，其中 k 是整数。因为 n 是奇数并且 $n \equiv 1 \pmod 3$，所以 n 只能具有形式 $6l + 1$，其中 l 是整数。此时，我们有 $p = \pi\bar{\pi} = 36k^2 - 108kl + 324l^2 + 6k + 72l + 7$，于是 $\frac{p-1}{6} \equiv k + 1 \pmod 6$。所以 $\gcd(\frac{p-1}{6}, 6) = 1$ 当且仅当 $k \equiv 0$ 或$4 \pmod 6$，即，$m \equiv 1$ 或$9 \pmod{12}$。

对于式子（2.9）的右边的条件，令 $m = 2k$ 其中 k 是整数。因为 n 是奇数并且 $n \equiv 2 \pmod 3$，所以 n 只能具有形式 $6l + 5$，其中 l 是整数。此时，我们有 $p = \pi\bar{\pi} = 36k^2 - 108kl + 324l^2 - 102k + 558l + 241$，于是 $\frac{p-1}{6} \equiv k + 3l + 4 \pmod 6$。所以 $\gcd(\frac{p-1}{6}, 6) = 1$ 当且仅当 $k + 3l \equiv 1$ 或$3 \pmod 6$。

综上所述，我们得到以下推论。

推论 2.12　设 $p \equiv 1 \pmod 6$ 是一个素数，并且 $\gcd(\frac{p-1}{6}, 6) = 1$，则存在一个非奇异完美 $B[-2, 4](p)$ 集当且仅当存在整数 k, l，使得下面三个条件之一成立：

1) $p = 1296k^2 - 648kl + 324l^2 + 36k + 72l + 7$。这对应着式子 (2.9) 的左边的条件，且 $m \equiv 1 \pmod{12}$。
2) $p = 1296k^2 - 648kl + 324l^2 + 1764k - 360l + 607$。这对应着式子 (2.9) 左边的条件，且 $m \equiv 9 \pmod{12}$。
3) $p = 36k^2 - 108kl + 324l^2 - 102k + 558l + 241$，其中 $k + 3l \equiv 1$ 或$3 \pmod 6$。这对应着式子 (2.9) 右边的条件。

下面我们看两个例子。

例 2.2　我们给出一些应用推论2.12的例子。

1) 让 k, l 跑遍从 -100 到 100 的所有整数，则 8 个最小的形如 $p = 1296k^2 - 648kl + 324l^2 + 36k + 72l + 7$ 的素数如表2.1中所列。特别地，若令 $l = 0$，则 $p = 1296k^2 + 36k + 7$。Bunyakovsky 猜想[60]（至今仍未被证明）表明有无穷多个这样的素数。
2) 让 k, l 跑遍从 -100 到 100 的所有整数, 则 8 个最小的形如 $p = 1296k^2 - 648kl + 324l^2 + 1764k - 360l + 607$ 的素数如表2.2中所列。

表 2.1　例2.2 1) 算得的值

p	7	1087	1123	1447	1483	2239	2311	2707
k	0	1	-1	0	1	1	-1	0
l	0	1	-2	2	2	-1	1	-3

表 2.2　例2.2 2) 算得的值

p	139	571	607	751	859	1291	2011	2371
k	-1	0	0	-1	-1	0	-1	-2
l	0	1	0	1	-2	-1	2	-3

2.4　准完美分解集的四种构造

在本节中，我们给出准完美分解集的四种新的构造。

定理 2.13　设 k, m 是两个正整数，且满足 $\gcd(k!, m) = 1$。令 $a = (-k)^{-1} \pmod m$，则

$$B = \left\{ik + 1 \mid i \in [0, m-1] \text{ 且} i \neq a\right\}$$

是一个准完美 $B[0, k](km)$ 集。

证明　设 $r(ik+1) \equiv 0 \pmod{km}$，其中 $r \in [1, k]$ 并且 $i \in [0, m-1] \setminus \{a\}$。因为 $ik+1 \not\equiv 0 \pmod k$，所以 $r \equiv 0 \pmod k$，因此，$r = k$。于是 $ik+1 \equiv 0 \pmod m$。这与 $i \not\equiv (-k)^{-1} \pmod m$ 矛盾。所以对任意的 $b \in B$ 以及任意的 $t \in [1, k]$，均有 $bt \not\equiv 0 \pmod{km}$。

现在我们设 $r(ik+1) \equiv s(jk+1) \pmod{km}$，这里 $r, s \in [1, k]$ 且 $i, j \in [0, m-1] \setminus \{a\}$。对这个式子两边模 k，可以得到 $r \equiv s \pmod k$。又因为 $r, s \in [1, k]$，所以 $r = s$。由此可得 $rik \equiv rjk \pmod{km}$，这等价于 $ri \equiv rj \pmod m$。注意到我们有条件 $\gcd(m, k!) = 1$，于是 $i \equiv j \pmod m$。又因为 $i, j \in [0, m-1] \setminus \{a\}$，所以 $i = j$。

根据以上分析，我们可知 B 是一个 $B[0, k](km)$ 集，且 B 的大小为 $m - 1 = \lfloor \frac{km-1}{m} \rfloor$，所以 B 是一个准完美 $B[0, k](km)$ 集。 ∎

我们先看两个例子。

例 2.3　1) 令 $k = 5$，$m = 7$。根据定理2.13，集合

$$\{1, 6, 11, 16, 26, 31\}$$

是一个准完美 $B[0, 5](35)$ 集。

2) 令 $k = 6$，$m = 7$。根据定理2.13，集合

$$\{1, 13, 19, 25, 31, 37\}$$

是一个准完美 $\boldsymbol{B}[0,6](42)$ 集。

注　定理2.13是文献 [56] 中定理 1 的一个推广。上面的例子并不能通过文献 [56] 中定理 1 中的构造得到。此外，定理2.13表明给定任意的正整数 k，对所有的满足素因子均大于 k 的正整数 m，都存在准完美 $\boldsymbol{B}[0,k](km)$ 集。

定理 2.14　令 $k>0$ 是一个整数，p 是一个素数且满足 $k<p<2k$，则

$$\boldsymbol{B}=\{k+1\}\cup\{1+(2k+2)i \mid i\in[0,p-1]\}$$

是一个准完美 $\boldsymbol{B}[-k,k](p(2k+2))$ 集。

证明　首先，我们要证明对任意的 $b\in\boldsymbol{B}$ 以及任意的 $m\in[-k,k]^*$，$bm\not\equiv 0 \pmod{p(2k+2)}$ 均成立。我们用反证法。若 $(k+1)m\equiv 0 \pmod{p(2k+2)}$，则 $m\equiv 0 \pmod{p}$，这与 $k<p<2k$ 矛盾。若存在 $i\in[0,p-1]$，使得 $(1+(2k+2)i)m\equiv 0 \pmod{p(2k+2)}$，则 $m\equiv 0 \pmod{k+1}$，这与 $m\in[-k,k]^*$ 矛盾。

其次，我们要证明对任意的 $b_1,b_2\in\boldsymbol{B}$ 以及任意的 $r,s\in[-k,k]^*$，若 $b_1r\equiv b_2s \pmod{p(2k+2)}$，则必有 $b_1=b_2$ 且 $r=s$。同样地，我们将用反证法证明之。设 $r(k+1)\equiv s(k+1) \pmod{p(2k+2)}$，则 $r-s\equiv 0 \pmod{2p}$。由 $k<p<2k$ 以及 $r,s\in[-k,k]^*$，我们得到 $r=s$。

设 $r(1+(2k+2)i)\equiv s(1+(2k+2)j) \pmod{p(2k+2)}$，其中 $i,j\in[0,p-1]$，则 $r\equiv s \pmod{2k+2}$。再根据 $r,s\in[-k,k]^*$，可以得到 $r=s$。于是从 $r(1+(2k+2)i)\equiv s(1+(2k+2)j) \pmod{p(2k+2)}$，我们可以推出 $si\equiv sj \pmod{p}$。由 $s\in[-k,k]^*$ 以及 $k<p<2k$ 可知 p 与 s 互素，所以 $i\equiv j \pmod{p}$。另一方面，因为 $i,j\in[0,p-1]$，所以 $i=j$。

设 $r(k+1)\equiv s(1+(2k+2)i) \pmod{p(2k+2)}$，其中 $i\in[0,p-1]$，则 $s\equiv 0 \pmod{k+1}$，这与 $s\in[-k,k]^*$，矛盾。

根据以上分析，我们可知 $\boldsymbol{B}$ 是一个 $\boldsymbol{B}[-k,k](p(2k+2))$ 集，且 $\boldsymbol{B}$ 的大小为 $p+1=\lfloor\frac{p(2k+2)-1}{2k}\rfloor$。所以 $\boldsymbol{B}$ 是一个准完美 $\boldsymbol{B}[-k,k](p(2k+2))$ 集。 ∎

我们有以下两个例子。

例 2.4　1) 令 $k=3$，$p=5$。根据定理2.14，集合

$$\{1,4,9,17,25,33\}$$

是一个准完美 $\boldsymbol{B}[-3,3](40)$ 集。

2) 令 $k=4$，$p=7$。根据定理2.14，集合

$$\{1,5,11,21,31,41,51,61\}$$

是一个准完美 $\boldsymbol{B}[-4,4](70)$ 集。

定理 2.15　令 $k \geqslant 2$ 是一个偶数，且 $m \geqslant 1$ 是一个正整数。对于 $i = 0, 1$，令 $T_i = \{x \mid x \equiv i \pmod 2, x \in [1, k]\}$，则 $|T_i| = \frac{k}{2}$。设 $p \equiv 1 \pmod{2^m k}$ 是一个素数。令 g 是一个模 p 的本原根，且满足 $g \equiv 1 \pmod 2$。记 $v \triangleq 2^{m-1}k$。如果存在 $\mathbb{Z}_v$ 的一个大小为 2^m 的子集 A，使得对每一个 $i = 0, 1$，$\mathbb{Z}_v = A + \{\mathrm{ind}_g(x) \pmod v \mid x \in T_i\}$ 都是一个直和分解，则

$$B \triangleq \{g^{i+jv} \mid i \in A, j \in [0, n-1]\}$$

是一个准完美 $B[-k, k](2p)$ 集，其中 $n = \frac{p-1}{2^m k} = \frac{p-1}{2v}$。

证明　容易看出对任意的 $i \in A$ 和任意的 $j \in [0, n-1]$，$i + jv \leqslant nv - 1 < p - 1$ 均成立，所以 B 是 $\mathbb{Z}_{2p}$ 的子集。

首先，因为 $p > k$ 且 p 与 g 互素，所以对于任意的 $r \in [-k, k]^*$ 以及任意的 $i \in A$，$j \in [0, n-1]$，$rg^{i+jv} \not\equiv 0 \pmod p$ 均成立。这表明 $rb \not\equiv 0 \pmod{2p}$ 对任意的 $r \in [-k, k]^*$ 和任意的 $b \in B$ 都成立。

接下来我们要证明对任意的 $i_1, i_2 \in A$，任意的 $j_1, j_2 \in [0, n-1]$ 以及任意的 $s, l \in [-k, k]^*$，若

$$sg^{i_1 + j_1 v} \equiv lg^{i_2 + j_2 v} \pmod{2p}, \tag{2.10}$$

则必有 $s = l$，$i_1 = i_2$ 以及 $j_1 = j_2$。给定式子（2.10），我们得到

$$sg^{i_1 + j_1 v} \equiv lg^{i_2 + j_2 v} \pmod p.$$

因此

$$\mathrm{ind}_g(s) + i_1 + j_1 v \equiv \mathrm{ind}_g(l) + i_2 + j_2 v \pmod{p-1}. \tag{2.11}$$

对上面的式子两边模 $v = 2^{m-1}k$，则有

$$\mathrm{ind}_g(s) + i_1 \equiv \mathrm{ind}_g(l) + i_2 \pmod v.$$

因为 $g \equiv 1 \pmod 2$，所以由式子（2.10）可以得到 $s \equiv l \pmod 2$，这说明 $s, l \in T_0 \cup (-T_0)$ 或者 $s, l \in T_1 \cup (-T_1)$。然而，由于 $\mathrm{ind}_g(-1) \equiv \frac{p-1}{2} \pmod v \equiv 0 \pmod v$，容易看出 $\mathrm{ind}_g(s) \pmod v$ 和 $\mathrm{ind}_g(l) \pmod v$ 这两个值总是在 $\{\mathrm{ind}_g(x) \pmod v : x \in T_i\}$ 中（$i = 0$ 或 1）。即便当 $s \in -T_i$ 或 $l \in -T_i$ 的时候，这个结论也是成立的。于是根据 A 的定义，我们有 $i_1 = i_2$ 以及 $s = l$ 或 $s = -l$。

若 $s = l$，则式子（2.11）表明 $j_1 - j_2 \equiv 0 \pmod n$。又因为 $j_1, j_2 \in [0, n-1]$，所以 $j_1 = j_2$。

若 $s = -l$，则式子（2.11）表明 $\frac{p-1}{2} + j_1 v \equiv j_2 v \pmod{p-1}$，所以 $\frac{p-1}{2} \mid v(j_1 - j_2)$。也就是说，$n \mid (j_1 - j_2)$，这意味着 $j_1 = j_2$。

由以上讨论我们可以知道 B 的确是一个 $B[-k, k](2p)$ 集。另一方面，容易看出 $|B| = 2^m \times n = \frac{p-1}{k} = \lfloor \frac{2p-1}{2k} \rfloor$。所以 B 是一个准完美 $B[-k, k](2p)$ 集。　∎

注　我们很难将定理2.15中的构造推广到准完美 $B[-k,k](tp)$ 集，其中 $t>2$。事实上,设 k 是 t 的倍数。我们根据模 t 的剩余类将 $[1,k]$ 划分成 t 个子集。运用和定理2.15中相同的证明方法, 我们能推导出 $s\equiv l \pmod t$。由此可得出 $s,l\in T_i\cup T_{t-i}$。然而我们并不能够由此得出关键的结论：$\mathrm{ind}_g(s) \pmod v$ 和 $\mathrm{ind}_g(l) \pmod v$ 这两个值总是在 $\{\mathrm{ind}_g(x) \pmod v \mid x\in T_i\}$ 中。

例 2.5　如表2.3所示，我们找到了一些满足定理2.15中条件的参数 k,m,p。

下面我们给出一个例子来比较定理2.15中的构造和文献 [51] 中定理 5 中的构造。令 $p=13729$，$k=8$，$m=1$，则 $g=23$ 是一个模 p 本原根。此外，通过计算得到

$$\begin{aligned}
&\mathrm{ind}_g(-8)=6654, \quad \mathrm{ind}_g(-7)=11084, \quad \mathrm{ind}_g(-6)=6376,\\
&\mathrm{ind}_g(-5)=9594, \quad \mathrm{ind}_g(-4)=11300, \quad \mathrm{ind}_g(-3)=11022,\\
&\mathrm{ind}_g(-2)=2218, \quad \mathrm{ind}_g(-1)=6864, \quad \mathrm{ind}_g(1)=0,\\
&\mathrm{ind}_g(2)=9082, \quad \mathrm{ind}_g(3)=4158, \quad \mathrm{ind}_g(4)=4436,\\
&\mathrm{ind}_g(5)=2730, \quad \mathrm{ind}_g(6)=13240, \quad \mathrm{ind}_g(7)=4220,\\
&\mathrm{ind}_g(8)=13518.
\end{aligned}$$

容易看出

$$\begin{aligned}
&\{\mathrm{ind}_g(i) \pmod 8 \mid i=1,3,5,7\}\\
=&\{\mathrm{ind}_g(i) \pmod 8 \mid i=2,4,6,8\}=\{0,2,4,6\}.
\end{aligned}$$

则根据定理2.15可知，$\{23^{i+8j} \pmod{27458} \mid i\in[0,1], j\in[0,857]\}$ 是一个准完美 $B[-8,8](27458)$ 集。

在参考文献 [51] 的定理 5 中，令 $t=2$，$\theta=\gcd\{\mathrm{ind}_g(k) \mid k\in[-8,8]^*\}$，我们得到

$$\left\{\frac{\mathrm{ind}_g(i)}{2} \pmod 8 \mid i=\pm1,\pm3,\pm5,\pm7\right\}=\{0,5,6,7\}$$

和

$$\left\{\frac{\mathrm{ind}_g(i)}{2} \pmod 8 \mid i=\pm2,\pm4,\pm6,\pm8\right\}=\{2,4,5,7\}.$$

然而这两个集合的大小都是 $4\neq\frac{k_1+k_2}{t}=8$，因此准完美 $B[-8,8](27458)$ 集并不能由文献 [51] 的定理 5 中得到。

定理 2.16　设 k 是一个正整数，p 是一个素数且满足 $k<p<\frac{4k-1}{3}$，则集合

$$B=\{k+1\}\cup\{1+(2k+2)i \mid i\in[0,p-1]\}$$

是一个准完美 $B[-(k-1),k](p(2k+2))$ 集。

表 2.3　由定理2.15得到的准完美 $B[-k,k](2p)$ 集的例子

k	m	p
4	1	97, 241, 409, 457, 1009, 1129, 1489, 1873, 2017, 2161
4	2	577, 1201, 4801, 5233, 7393, 10513, 14401, 14449, 14593
4	3	13441, 49633, 122497, 136993, 147457, 149377
8	1	12721, 13729, 33889, 65809

证明　这个定理的证明和定理2.14的证明类似，因此我们简略地叙述之。

设 $r(k+1) \equiv s(k+1) \pmod{p(2k+2)}$，其中 $r, s \in [-(k-1), k]^*$，则 $r \equiv s \pmod{2p}$，因此 $r = s$。

设 $r(k+1) \equiv s(1+(2k+2)i) \pmod{p(2k+2)}$，其中 $r, s \in [-(k-1), k]^*$ 以及 $i \in [0, p-1]$，则 $s \equiv 0 \pmod{k+1}$，矛盾。

设 $r(1+(2k+2)i) \equiv s(1+(2k+2)j) \pmod{p(2k+2)}$, 其中 $r, s \in [-(k-1), k]^*$ 以及 $i, j \in [0, p-1]$, 则 $r \equiv s \pmod{2k+2}$, 因此 $r = s$。这意味着 $r(2k+2)i \equiv r(2k+2)j \pmod{p(2k+2)}$, 于是 $ri \equiv rj \pmod{p}$。注意到 $p > k$ 是一个素数, 所以 $\gcd(r, p) = 1$。于是 $i \equiv j \pmod{p}$，所以 $i = j$。

综上所述，我们可以看出 $\boldsymbol{B}$ 是一个大小为 $p+1 = \left\lfloor \frac{p(2k+2)-1}{2k-1} \right\rfloor$ 的 $B[-(k-1), k](p(2k+2))$ 集。所以 $\boldsymbol{B}$ 是一个准完美 $B[-(k-1), k](p(2k+2))$ 集。 ∎

例 2.6　1) 令 $k = 6$，$m = 7$。根据定理2.16，集合

$$\{1, 7, 15, 29, 43, 57, 71, 85\}$$

是一个准完美 $\boldsymbol{B}[-5, 6](98)$ 集。

2) 令 $k = 9$，$m = 11$。根据定理2.16，集合

$$\{1, 10, 21, 41, 61, 81, 101, 121, 141, 161, 181, 201\}$$

是一个准完美 $\boldsymbol{B}[-8, 9](220)$ 集。

2.5　分解集和凯莱图的联系

在这一节中，我们将建立起分解集和凯莱图（Cayley graph）的联系。本节当中所涉及到的关于图论的术语均可以在文献 [61-62] 中找到。为了读者方便，我们在这里简单的介绍其中的一些概念。

设 $\boldsymbol{H}$ 是一个有限的乘法交换群，其单位元为 e。令 $\boldsymbol{S}$ 是 $\boldsymbol{H}$ 的一个不包含 e 的子集，且满足以下条件：对 $\boldsymbol{H}$ 中任意的非单位元 s，要么 s 和 s^{-1} 同时在 $\boldsymbol{S}$ 中，要么 s 和 s^{-1} 同时不在 $\boldsymbol{S}$ 中。这样，由 $\boldsymbol{H}$ 和 $\boldsymbol{S}$ 可以定义一个凯莱图 $\boldsymbol{G} \triangleq (\boldsymbol{V}, \boldsymbol{E})$。

其中 $V = H$ 被称为 G 的顶点集, V 中的每个元素被称为 G 的顶点, $E \subseteq V \times V$ 被称为 G 的边集。对任意两个不同的顶点 $x, y \in V$, $\{x, y\} \in E$ 当且仅当 $xy^{-1} \in S$。我们将由这样的方式构造得到的图记为 $G = Cay(H, S)$。凯莱图已经被广泛的研究了，关于其详细内容可见参考文献 [63-65]。

给定一个图 $G = (V, E)$ 以及 V 的一个子集 I，若对于 I 中任意两个不同顶点 x, y，均有 $\{x, y\} \in E$，则称 I 是 G 的一个独立集。G 的独立集的最大的大小被称为图 G 的独立数，记为 $\alpha(G)$。若对 G 的任一个顶点 $x \in V$，都恰好存在 d 个其他顶点 $y \in V$，使得 $\{x, y\} \in E$，则称 G 是 d-正则的。设 $P = x_0 x_1 \cdots x_n$，其中 $n \geqslant 1$。若 $\{x_i, x_{i+1}\} \in E$ 对任意的 $i = 0, \cdots, n-1$ 都成立，则称 P 是图 G 中一条连接顶点 x_0 和顶点 x_n 的路。如果对于 G 的任意两个不同顶点 x 和 y，G 中都存在一条路连接它们，则称 G 是一个连通图。G 的任意一个极大连通子图被称为 G 的一个连通分支。一个 2-正则的连通图称为圈。给定两个（不一定不同）图 $G_1 = (V_1, E_1)$ 和 $G_2 = (V_2, E_2)$，若存在一个双射 $f: V_1 \longrightarrow V_2$ 使得 $\{x, y\} \in E_1$ 当且仅当 $\{f(x), f(y)\} \in E_2$，则称图 G_1 和图 G_2 是同构的。

在本节接下来的内容中，我们一直假设 $k_2 \geqslant k_1 \geqslant 0$ 是两个整数，$M = [-k_1, k_2]^*$。因为完美 $B[0, 1](p)$ 集和完美 $B[-1, 1](p)$ 集是平凡的，且对任意的整数 q，最大的 $B[-k_1, 2](q)$ 集已经被完全求出来了[47-48,56]，所以在这一节中我们总假设 $k_2 \geqslant 3$。对任一个大于 $k_1 + k_2$ 的素数 p, 我们可以将 M 看成 $\mathbb{Z}_p^*$ 的一个子集。令 $S = \{xy^{-1} \mid x, y \in M \text{ 且} x \neq y\}$, $G = Cay(\mathbb{Z}_p^*, S)$ 以及 $G' = Cay(\langle M \rangle, S)$。令 $\langle S \rangle$ 和 $\langle M \rangle$ 分别表示 $\mathbb{Z}_p^*$ 的由 S 和 M 生成的子群。容易验证 $\langle S \rangle = \langle M \rangle$。于是我们有以下结论：$G'$ 是 G 的一个连通分支[65] 且 G 的任一个连通分支都和 G' 同构。

首先，我们观察到以下一个简单的结论。

命题 2.17　$\mathbb{Z}_p^*$ 的一个子集 B 是一个 $B[-k_1, k_2](p)$ 集当且仅当 B 是图 G 的一个独立集。

证明　我们首先证明必要性。设 B 是一个 $B[-k_1, k_2](p)$ 集。如果 B 中存在两个不同的元素 b_1, b_2 使得 $\{b_1, b_2\} \in E(G)$，则 $x, y \in M$ 中存在两个不同的元素 x, y 使得 $b_1 b_2^{-1} = xy^{-1}$，即 $xb_2 = yb_1$。因为 B 是一个 $B[-k_1, k_2](p)$ 集，所以 $x = y$ 且 $b_1 = b_2$，矛盾。因此 B 是图 G 的一个独立集。

现在我们证明充分性。设 B 是图 G 的一个独立集。若存在 $b_1, b_2 \in B$ 以及 $x, y \in M$ 使得 $xb_1 = yb_2$，则 $b_1 b_2^{-1} = yx^{-1}$。如果 $b_1 \neq b_2$，则根据 G 的定义可知 $\{b_1, b_2\} \in E(G)$，这与设 B 是图 G 的一个独立集矛盾。所以 $b_1 = b_2$ 且 $x = y$，从而可知 B 是一个 $B[-k_1, k_2](p)$ 集。 ∎

由命题2.17可知,一个 $B[-k_1, k_2](p)$ 集等价于图 G 中的一个独立集。下面的引

理是 Brooks 定理[66] 的一个推论。我们可以用这个引理给出最大的 $B[-k_1, k_2](p)$ 集的大小的一个下界。其中 $p > k_1 + k_2 + 1$，$0 \leqslant k_1 \leqslant k_2$ 且 $k_2 \geqslant 3$。据我们所了解，之前并没有人给出过最大的 $B[-k_1, k_2](p)$ 集的大小的一个一般的下界。在陈述下面的引理之前，我们先回忆一下两个需要用到的概念。给定一个图 Γ，若 $x, y \in V(\Gamma)$ 对 Γ 的任意两个不同的顶点都成立，则称 Γ 是一个完全图。一个奇圈指的是有奇数个顶点的圈。

引理 2.18　设 Γ 是一个 d-正则图。如果 Γ 的任何一个连通分支既不是完全图也不是奇圈，则

$$\alpha(\Gamma) \geqslant \frac{|V(\Gamma)|}{d}.$$

否则，

$$\alpha(\Gamma) \geqslant \frac{|V(\Gamma)|}{d+1}.$$

根据定义，我们很容易验证 G 和 G' 都是 $|S|$-正则图。如果 $p > k_1 + k_2 + 2$ 且 $k_2 \geqslant 3$，则 $|S| > 2$。因此 G' 不是一个奇圈。因为 G' 是 $|S|$-正则图，所以 $|\langle M\rangle| \geqslant |S| + 1$。更进一步地，如果 $|\langle M\rangle| \geqslant |S| + 2$，则 G' 不可能是一个完全图。于是，我们有下面的推论。

推论 2.19　令 B 是一个最大的 $B[-k_1, k_2](p)$ 集。如果 $p > k_1 + k_2 + 1$ 且 $k_2 \geqslant 3$，则

$$|B| \geqslant \left\lceil \frac{p-1}{|S|+1} \right\rceil.$$

进一步地，如果 $|\langle M\rangle| \geqslant |S| + 2$ 且 $p > k_1 + k_2 + 2$，则

$$|B| \geqslant \left\lceil \frac{p-1}{|S|} \right\rceil.$$

将分解集和凯莱图联系起来还有另一个好处：我们可以用一些数学软件（比如 Maple）来计算出一个图的最大的独立集，从而能够直接算出一个最大的 $B[-k_1, k_2](p)$ 集。下面我们给出一个例子。

例 2.7　取 $k_1 = 0, k_2 = 3$，我们算得了表2.4中列出的一些值。其中第三行是根据推论 2.19得到的下界；第四行是用 Maple 中的 *IndependenceNumber* 命令算到的值；最后一行是用 Maple 中的 *MaximumIndependentSet* 命令算出的最大独立集（即一个最大的分解集）。

2.6　小结

本章中，我们考虑了分解集的存在性问题。我们给出了非奇异完美 $B[-k_1, k_2](p)$ 集存在的充分必要条件，其中 $(k_1, k_2) \in \{(0,4), (2,4), (4,4)\}$。为了方便读者参考，我们将已有的结果列在了表 2.5中，其中 p 是一个素数，g

表 2.4　例2.7：$k_1 = 0, k_2 = 3$

p	7	11	13	17	19	23	29	31	37
$\|S\|$	4	6	6	6	6	6	6	6	6
推论 2.19	2	2	2	3	3	4	5	5	6
$\alpha(G)$	2	2	3	4	5	5	8	8	12
最大独立集（最大分解集）	{1,6}	{1,5}	{1,4,11}	{1,4,13,16}	{1,6,8,14,15}	{1,4,5,6,7}	{1,5,6, 7,8,11, 19,26}	{1,4,9, 10,14,23, 25,26}	{1,6,8, 10,11,14, 23,26,27, 29,31,36}

表 2.5　非奇异完美分解集的存在性

非奇异完美分解集	充要条件	参考文献
$B[-k,k](p)$，其中 k 是奇素数	$p \equiv 1 \pmod{2\mu k}$ 且 $\left\|\left\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod k : j \in [1,k]\right\}\right\| = k$	[53] 定理 3.2
$B[0,k](p)$，其中 k 是奇素数	$p \equiv 1 \pmod{\mu k}$ 且 $\left\|\left\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod k : j \in [1,k]\right\}\right\| = k$	[53] 定理 3.3
$B[-k_1,k_2](p)$，$\gcd(\frac{p-1}{k_1+k_2}, k_1+k_2) = 1$	$p \equiv 1 \pmod{\mu(k_1+k_2)}$ 且 $\left\|\left\{\frac{\mathrm{ind}_g(j)}{\mu} \pmod k : j \in [-k_1,k_2]^*\right\}\right\| = k_1+k_2$	[53] 定理 3.5
$B[0,2](p)$	$p \equiv 1 \pmod 2$ 且 $\mathrm{ord}_p(2)$ 是偶数	[37] 定理 2
$B[-2,2](p)$	$p \equiv 1 \pmod 4$ 且 $v_2(\mathrm{ord}_p(2)) \geqslant 2$	[48] 推论 3
$B[-1,3](p)$	$p \equiv 5 \pmod 8$，6 是一个模 p 的四次剩余	[54] 定理 4.4
	$p \equiv 1 \pmod 8$，$\mathrm{ord}_p(-\frac{3}{2})$ 是奇数且 $4 \mid \mathrm{ord}_p(2)$	[54] 定理 4.5
$B[-2,4](p)$	$p \equiv 1 \pmod 6$，$\mathrm{ord}_p(-\frac{3}{4})$ 是奇数且 $2 \notin \langle 6,8\rangle$	定理2.6
$B[-4,4](p)$	$p \equiv 1 \pmod 8$ 且 $\pm 4 \notin \langle 6,16\rangle$	定理2.7
$B[0,4](p)$	$p \equiv 1 \pmod 4$ 且 $4 \notin \langle 6,16\rangle$	定理2.8

是一个模 p 的本原根，$\mu = \gcd\{\mathrm{ind}_g(j) : j \in [-1,k]^*\}$（对于 $B[-k,k](p)$ 集），或 $\mu = \gcd\{\mathrm{ind}_g(j) : j \in \{2,\cdots,k,p-1\}\}$（对于 $B[0,k](p)$ 集），或 $\mu = \gcd\{\mathrm{ind}_g(j) : j \in [-1,k_2]^*\}$（对于 $B[-k_1,k_2](p)$ 集）。

此外，我们也给出了准完美分解集的四种新的构造。最后，通过将分解集和凯莱图联系起来，对任何的素数 $p > k_1 + k_2 + 1$ 和任何的 $k_2 \geqslant k_1 \geqslant 0$，我们给出了最大 $B[-k_1,k_2](p)$ 集大小的一个一般性的下界。

对于以后的研究，我们给出以下几个问题

1. 证明文献 [53,67] 中关于纯奇异完美分解集不存在性的猜想。
2. 构造最大的 $B[-k_1,k_2](n)$ 集。当 $0 \leqslant k_1 \leqslant k_2 \leqslant 2$ 时，这个问题已经被完全解决了，详见文献 [37,47-48]。
3. 给出更多的关于非奇异完美 $B[-k_1,k_2](p)$ 集的存在性的结果。文献 [53] 的作者证明了当 $1 \leqslant k_1 < k_2$ 且 $k_1 + k_2$ 是奇数时，不存在非奇异完美 $B[-k_1,k_2](p)$ 集。其他的结果请见表2.5。本章中,我们完全给出了非奇异完美 $B[-k_1,k_2](p)$ 集存在性的充分必要条件, 其中 $(k_1,k_2) \in \{(0,4),(2,4),(4,4)\}$。接下来可以考虑的情形是 $(k_1,k_2) = (1,5)$。
4. 给出更多的准完美分解集的构造。

5. 给出更多的最大分解集的构造——可以试着将文献 [48] 中表 V 所列出的分解集推广到一般情形。

第 3 章　重　构　码

3.1　介绍

本章的研究主题是重构码，其在 DNA 存储中有潜在的应用。序列的有效重构问题是由 V.I. Levenshtein 于 2000 年左右开始研究的[13-15]。他研究这个问题的动机是其在许多科学领域中都有应用，例如信息科学、分子生物学、化学，等等。在这些应用场景中，我们除了将要传输的信息重复多次传输以外，别无他法。这个问题模型可描述为：信息的发送方将信息 $\boldsymbol{x}$ 通过 N 个不同的噪声信道传输出去；信息的接收方能够接收到所有 N 个信道的输出（我们称为有噪声的读取（nosiy read）），然后接收方的目标是利用这 N 有噪声读取来重构发送方发送的信息。最近一些年，由于在 DNA 存储、无限感知网络和赛道内存等场景中的应用，这个问题又吸引了大量研究人员的兴趣。许多研究者开始在编码的情形下考虑这个问题，即被传输的序列是从某个具有一定纠错能力的码中选取的[27-33]。

在 2020 年，受 DNA 数据存储和赛道内存（racetrack memory）中的应用启发，Cai 和 Nguyen 等人[34-35] 以及 Chrisnata 和 Yaakobi 等人[36] 率先研究了这个问题：设计一个码（称为重构码），使得以它的不同码字为中心的两个不同的错误球相交的大小的最大值小于 N，其中 N 给定。在文献 [35-36] 中，作者主要考虑了发生一个编辑错误（edit error）的信道 (即一个替换错误、一个插入错误或一个删除错误）以及它们的变种，并对所有的 N 都给出了码的构造。特别地，当字母表大小为 2 的时候，他们确定了码的冗余的渐近最优值。

我们在本章目的是研究每个信道发生两个插入错误的时候，相应的重构码的构造。

3.2　准备工作

本节中，我们介绍一些必要的概念和已有的结果。

我们用 Σ_2 表示二元字母表 $\{0,1\}$。对任何的非负整数 n，令 $\Sigma_2^n \triangleq \{\boldsymbol{x} = x_1 \cdots x_n \mid x_i \in \Sigma_2$ 对任意的 $1 \leqslant i \leqslant n$都成立$\}$。$\Sigma_2^n$ 中的一个元素 $\boldsymbol{x}$ 被称为一个序列；称 n 为序列 $\boldsymbol{x}$ 的长度并记作 $|\boldsymbol{x}|$。需要指出的是，如果 $n = 0$，则 $\boldsymbol{x} = \varnothing$ 是空序列。令 $\Sigma_2^* \triangleq \bigcup_{n=0}^{\infty} \Sigma_2^n$，即由所有长度有限的序列构成的集合。

令 t 是一个满足 $1 \leqslant t \leqslant n$ 的正整数。设 $\boldsymbol{x} = x_1 \cdots x_n \in \Sigma_2^n$ 和 $\boldsymbol{y} = y_1 \cdots y_t \in \Sigma_2^t$ 是两个序列。如果存在 $1 \leqslant i_1 < \cdots < i_t \leqslant n$ 使得 $y_j = x_{i_j}$ 对所有的 $1 \leqslant j \leqslant t$ 都成立，则我们说 $\boldsymbol{y}$ 是 $\boldsymbol{x}$ 的一个子序列（subsequence），或者说 $\boldsymbol{x}$ 是 $\boldsymbol{y}$ 的一个超序列（supersequence）。特别地，如果 $i_{j+1} = i_j + 1$ 对所有的 $1 \leqslant j < t$ 都成立，我们称

$\boldsymbol{y}$ 是 $\boldsymbol{x}$ 的一个子字（subword）.

对任何的 $\boldsymbol{x} \in \Sigma_2^n$ 和任何的 $t \geqslant 0$，令 $I_t(\boldsymbol{x}) \triangleq \{\boldsymbol{y} \in \Sigma_2^{n+t} \mid \boldsymbol{y}$是$\boldsymbol{x}$的超序列$\}$。我们称 $I_t(\boldsymbol{x})$ 是一个以 $\boldsymbol{x}$ 为中心的 t-插入球。众所周知，$\left|I_t(\boldsymbol{x})\right|$ 与 $\boldsymbol{x}$ 的选取无关（请看下面的推论3.2）。于是, 我们可以定义 $I_2(n,t) \triangleq \left|I_t(\boldsymbol{x})\right|$。对任何的 $1 \leqslant s \leqslant n$，令 $D_s(\boldsymbol{x}) \triangleq \{\boldsymbol{y} \in \Sigma_2^{n-s} \mid \boldsymbol{y}$是$\boldsymbol{x}$的子序列$\}$。我们称 $D_s(\boldsymbol{x})$ 是一个以 $\boldsymbol{x}$ 为中心的 s-删除球。与插入的情形不同的是，$D_s(\boldsymbol{x})$ 的大小是依赖于 $\boldsymbol{x}$ 的选取的，详见文献 [68-71]。

定义 3.1　如果序列 $\boldsymbol{x} = x_1 \cdots x_n \in \Sigma_2^n$（$n \geqslant 2$）满足 $x_1 \neq x_2$，且当 $n \geqslant 3$ 时，$x_i = x_{i+2}$ 对所有的 $1 \leqslant i \leqslant n-2$ 都成立，则称 $\boldsymbol{x}$ 是一个交错序列。为了方便，我们也把空序列和长度等于 1 的序列看成交错序列。

例 3.1　根据定义3.1可知，$\varnothing$，1，0，10，01，101，101010，0101010 都是交错序列。

定义 3.2　对两个不同的序列 $\boldsymbol{x}, \boldsymbol{y} \in \Sigma_2^n$，令 $d_L(\boldsymbol{x}, \boldsymbol{y})$ 表示最小的使得 $I_\ell(\boldsymbol{x}) \cap I_\ell(\boldsymbol{y})$ 非空（等价地，$D_\ell(\boldsymbol{x}) \cap D_\ell(\boldsymbol{y})$ 非空）的非负整数 ℓ，并称 $d_L(\boldsymbol{x}, \boldsymbol{y})$ 是 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 之间的 Levenshitein 距离。

由定义可知，$0 \leqslant d_L(\boldsymbol{x}, \boldsymbol{y}) \leqslant n$ 以及 $d_L(\boldsymbol{x}, \boldsymbol{y}) = 0$ 当且仅当 $\boldsymbol{x} = \boldsymbol{y}$。

对给定的满足条件 $n, t \geqslant \ell \geqslant 0$ 的整数 n, t, ℓ 令

$$N_2^+(n,t,\ell) \triangleq \max\{\left|I_t(\boldsymbol{x}) \cap I_t(\boldsymbol{y})\right| \mid \boldsymbol{x}, \boldsymbol{y} \in \Sigma_2^n \text{ 且} d_L(\boldsymbol{x}, \boldsymbol{y}) \geqslant \ell\}.$$

我们有以下公式。

引理 3.1　[27]对任何满足条件 $n, t \geqslant \ell \geqslant 0$ 的整数 n, t, ℓ，以下公式都成立:

$$N_2^+(n,t,\ell) = \sum_{j=\ell}^{t} \sum_{i=0}^{t-j} \binom{2j}{j} \binom{t+j-i}{2j} \binom{n+t}{i} (-1)^{t+j-i}.$$

推论 3.2　[27] 在引理3.1中取 $\ell = 0$，则对所有的 $n, t \geqslant 0$，下面的式子成立:

$$I_2(n,t) = \sum_{i=0}^{t} \binom{n+t}{i}.$$

对所有的整数 $n, t \geqslant 0$ 令

$$N_2^+(n,t) \triangleq \max\{\left|I_t(\boldsymbol{x}) \cap I_t(\boldsymbol{y})\right| \mid \boldsymbol{x}, \boldsymbol{y} \in \Sigma_2^n \text{且} \boldsymbol{x} \neq \boldsymbol{y}\}.$$

由定义可知 $N_2^+(n,0) = 0$。当 $t \geqslant 1$ 时，有以下结果。

推论 3.3　[15,27] 在引理3.1中取 $\ell = 1$，则对所有的 $n, t \geqslant 1$，下面的式子成立:

$$N_2^+(n,t) = \sum_{i=0}^{t-1} \binom{n+t}{i} (1 - (-1)^{t-i}).$$

为了引入下面的定义，我们先介绍一些记号。设 $\boldsymbol{x}, \boldsymbol{y} \in \Sigma_2^*$ 以及 $S \subseteq \Sigma_2^*$。我们用 $\boldsymbol{xy}$ 表示由 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 串联得到的序列；类似地，$\boldsymbol{x}S \triangleq \{\boldsymbol{xy} \mid \boldsymbol{y} \in S\}$。如果 $\boldsymbol{u} = u_1 \cdots u_n \in \Sigma_2^*$，我们定义 $\overline{\boldsymbol{u}} = (1-u_1)\cdots(1-u_n)$。

定义 3.3　(A 类易混淆) 设 $\boldsymbol{x}, \boldsymbol{y} \in \Sigma_2^n$，如果存在 $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \Sigma_2^*$ 使得下面两个条件同时成立：

(i) $\boldsymbol{x} = \boldsymbol{uwv}$ 以及 $\boldsymbol{y} = \boldsymbol{u}\overline{\boldsymbol{w}}\boldsymbol{v}$，

(ii) $\boldsymbol{w}$ 是长度至少为 1 的交错序列，

则称 $\boldsymbol{x}, \boldsymbol{y}$ 是 A 类易混淆的。

注　“A 类易混淆”（Type-A confusability）这个概念首先出现在 [35] 的定义 8 中。然而，定义3.3和文献 [35] 的定义 8 中给的定义稍微有一点差别。具体地说，我们在定义3.3中包含了汉明距离等于 1 的情形，但是文献 [35] 的定义 8 中并没有包含这种情形。

根据推论3.3我们知道 $\left|I_1(\boldsymbol{x}) \cap I_1(\boldsymbol{y})\right| \leqslant 2$ 对任何 $\boldsymbol{x}, \boldsymbol{y} \in \Sigma_2^n$ 都成立。下面的引理能告诉我们更多的信息。

引理 3.4　[35] 设 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 Σ_2^n 中两个不同的序列，则 $\left|I_1(\boldsymbol{x}) \cap I_1(\boldsymbol{y})\right| = 2$ 当且仅当 $\boldsymbol{x}, \boldsymbol{y}$ 是 A 类易混淆的。

对 Σ_2^n 的任何至少包含 2 个元素的子集 $\mathcal{C}$，令

$$\nu_t(\mathcal{C}) \triangleq \max\{\left|I_t(\boldsymbol{x}) \cap I_t(\boldsymbol{y})\right| \mid \boldsymbol{x}, \boldsymbol{y} \in \mathcal{C} \text{且} \boldsymbol{x} \neq \boldsymbol{y}\}.$$

很显然，如果 $\nu_t(\mathcal{C}) < N$，则给定 $\mathcal{C}$ 中任一个序列 $\boldsymbol{c}$，我们能用 $\boldsymbol{c}$ 的任意 N 个不同的超序列来唯一的重构 $\boldsymbol{c}$。因此，当 $\nu_t(\mathcal{C}) < N$ 的时候，我们称 $\mathcal{C}$ 是一个 $(n, N; B_2^{I(t)})$-重构码。对于删除信道，我们能给出类似的定义。此时，我们用“$(n, N; B_2^{D(t)})$-重构码”来称呼这样的码。

特别地，当 $N = 1$ 时，一个 $(n, 1; B_2^{I(t)})$-重构码（$(n, 1; B_2^{D(t)})$-重构码也被称为 t-插入纠错码（t-删除纠错码）。众所周知，一个码是 t-删除纠错码当且仅当它是一个 t-插入纠错码。最近几年，这类码得到了大量的研究，详细内容可见文献 [72-76]。对于 $t = 1$，我们有如下著名的 Varshmov-Tenengolts 码（VT 码）[68,77]：

$$VT_a(n) \triangleq \left\{ \boldsymbol{x} = x_1 \cdots x_n \in \Sigma_2^n \mid \sum_{i=1}^{n} i x_i \equiv a \pmod{n+1} \right\},$$

其中 a 是一个在 0 和 n 之间的整数。当 $a = 0$ 的时候，这个码能达到渐近最优冗余 $\log_2(n+1)$。

当研究重构码的时候，下面的量非常重要。

$$\rho(n, N; B_2^{I(t)}) \triangleq \min\{n - \log_2 |\mathcal{C}| \mid \mathcal{C} \subseteq \Sigma_2^n \text{且} \nu_t(\mathcal{C}) < N\}.$$

这是一个 $(n, N; B_2^{I(t)})$-重构码能达到的最小的冗余。N 的值和冗余的大小是判断一个码好坏的两个非常重要的量：实际应用中希望 N 和冗余都尽可能的小。

在文献 [35] 定理 24 中，Kui Cai 等人对所有的 $N \geqslant 1$ 找到了 $\rho(n, N; B_2^{I(1)})$ 的渐近最优值。为了方便读者参考，我们将他们的结果列在下面的定理3.5中。

定理 3.5　在 [35] 定理 24 中，取 $q = 2$，我们有

$$\rho(n, N; B_2^{I(1)}) = \begin{cases} \log_2(n) + \Theta(1), & \text{如果} N = 1, \\ \log_2 \log_2(n) + \Theta(1), & \text{如果} N = 2, \\ 0, & \text{如果} N \geqslant 3. \end{cases}$$

因此，我们本章的目标就是对尽可能多的 N 和 $t = 2$，构造 $(n, N; B_2^{I(t)})$-重构码，使得其冗余尽可能小。

3.3　t-插入球的相交大小

本节中的主要结果是定理3.10，其对于我们在下一节中的分析非常有用。这个定理给出了当 $|I_1(\boldsymbol{x}) \cap I_1(\boldsymbol{y})| = 1$ 时，$\left|I_t(\boldsymbol{x}) \cap I_t(\boldsymbol{y})\right|$ 的一个上界，其中 $t \geqslant 2$。

定义 3.4　[36]（B 类易混淆）设 $\boldsymbol{x}, \boldsymbol{y} \in \Sigma_2^n$。如果存在 $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \Sigma_2^*$ 使得

$$\boldsymbol{x} = \boldsymbol{u}a\bar{a}\boldsymbol{v}b\boldsymbol{w}, \ \boldsymbol{y} = \boldsymbol{u}\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w},$$

（其中 $a, b \in \Sigma_2$），则称 $\boldsymbol{x}, \boldsymbol{y}$ 是 B 类易混淆的。

注　根据定义3.3和定义3.4，我们容易验证以下结论：

- 如果 $\boldsymbol{x} = \boldsymbol{u}\boldsymbol{w}\boldsymbol{v}$ 和 $\boldsymbol{y} = \boldsymbol{u}\overline{\boldsymbol{w}}\boldsymbol{v} \in \Sigma_2^n$ 是 A 类易混淆的，则它们是 B 类易混淆的当且仅当存在 $m \geqslant 2$ 使得 $\boldsymbol{w} \in \{(10)^m, (01)^m\}$，或存在 $m \geqslant 1$ 使得 $\boldsymbol{w} \in \{(10)^m 1, (01)^m 0\}$。
- 如果 $\boldsymbol{x} = \boldsymbol{u}a\bar{a}\boldsymbol{v}b\boldsymbol{w}, \boldsymbol{y} = \boldsymbol{u}\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w} \in \Sigma_2^n$ 是 B 类易混淆的，则它们是 A 类易混淆的当且仅当下面两个条件有一个成立：
  (1) $\boldsymbol{v} = (a\bar{a})^m$ $(m \geqslant 0)$ 且 $a = b$；
  (2) $\boldsymbol{v} = (a\bar{a})^m a$ $(m \geqslant 0)$ 且 $a = \bar{b}$。

引理 3.6　设 $\boldsymbol{x}, \boldsymbol{y} \in \Sigma_2^n$。如果 $\left|I_1(\boldsymbol{x}) \cap I_1(\boldsymbol{y})\right| = 1$，则 $\boldsymbol{x}, \boldsymbol{y}$ 是 B 类易混淆的；特别地，$n \geqslant 3$。

证明　根据引理3.4可知 $d_H(\boldsymbol{x}, \boldsymbol{y}) \geqslant 2$，于是我们可以假设

$$\begin{cases} \boldsymbol{x} = \boldsymbol{u}a\boldsymbol{d}b\boldsymbol{w} \\ \boldsymbol{y} = \boldsymbol{u}\bar{a}\boldsymbol{e}\bar{b}\boldsymbol{w} \end{cases},$$

其中 $a, b \in \Sigma_2$ 且 $\boldsymbol{u}, \boldsymbol{d}, \boldsymbol{e}, \boldsymbol{w} \in \Sigma_2^*$。设 i, j 分别是最左边和最右边的使得 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 不相等的下标。

首先，假设 $\boldsymbol{d}=\boldsymbol{e}=\varnothing$。若 $a=\bar{b}$，则 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 A 类易混淆的，矛盾。若 $a=b$，则 $|wt(\boldsymbol{x})-wt(\boldsymbol{y})|=2$。所以 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=0$，矛盾。所以 $\boldsymbol{d}$ 和 $\boldsymbol{e}$ 都是非空的。令 $\{\boldsymbol{z}\}=I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})$。

设 k 和 ℓ 分别是 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 中插入发生的位置，则只能有两种可能性：$k\leqslant i$ 且 $\ell>j$，或者 $k>j$ 且 $\ell\leqslant i$。

如果 $k\leqslant i$ 且 $\ell>j$，则 $\boldsymbol{z}=\boldsymbol{u}\bar{a}a\boldsymbol{d}b\boldsymbol{w}=\boldsymbol{u}\bar{a}\boldsymbol{e}\bar{b}b\boldsymbol{w}$。这表明存在 $\boldsymbol{v}\in\Sigma_2^*$ 使得 $\boldsymbol{d}=\boldsymbol{v}\bar{b}$ 和 $\boldsymbol{e}=a\boldsymbol{v}$ 同时成立，因此 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 B 类易混淆的。

当 $k>j$ 且 $\ell\leqslant i$ 时，证明与上面类似，我们不再赘述。 ∎

结合推论3.3，我们可以将引理3.4和引理3.6总结为以下推论。这个推论在本章会被经常使用。

推论 3.7　设 $\boldsymbol{x},\boldsymbol{y}\in\Sigma_2^n$ 是两个不同的序列。

- $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=0$ 当且仅当 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 既不是 A 类易混淆的，也不是 B 类易混淆的。
- $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=1$ 当且仅当 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 B 类易混淆的，但不是 A 类易混淆的。
- $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=2$ 当且仅当 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 A 类易混淆的。

在本章接下来的内容中，对任意的 $S\subseteq\Sigma_2^*$ 以及任意的 $a,b\in\Sigma_2$ 我们定义 $S^a\triangleq\{\boldsymbol{x}\in S\mid \boldsymbol{x}\text{的第一位是}a\}$，$S_b\triangleq\{\boldsymbol{x}\in S\mid \boldsymbol{x}\text{的最后一位是}b\}$，$S_b^a\triangleq\{\boldsymbol{x}\in S\mid \boldsymbol{x}\text{的第一位是}a\text{且最后一位是}b\}$。

引理 3.8　令 $n\geqslant 3$，$\boldsymbol{x},\boldsymbol{y}\in\Sigma_2^n$。设存在 $a,b\in\Sigma_2$ 以及 $\boldsymbol{v}\in\Sigma_2^{n-3}$ 使得

$$\boldsymbol{x}=a\bar{a}\boldsymbol{v}b,\ \boldsymbol{y}=\bar{a}\boldsymbol{v}b\bar{b}.$$

如果 $I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})=\{\boldsymbol{z}\}$，则

$$\left|I_t(\boldsymbol{x})\cap I_t(\boldsymbol{y})\right|\leqslant\left|I_{t-1}(\boldsymbol{z})\right|+N_2^+(n-1,t-1)=I_2(n+1,t-1)+N_2^+(n-1,t-1),$$

对任意的 $t\geqslant 2$ 都成立。特别地，当 $t=2$ 的时候，我们有：$\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|\in\{n+3,n+4,n+5\}$。更进一步地，

- $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=n+5$ 当且仅当 $a\bar{a}\boldsymbol{v}$ 和 $\boldsymbol{v}b\bar{b}$ 是 A 类易混淆的。
- $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=n+4$ 当且仅当 $a\bar{a}\boldsymbol{v}$ 和 $\boldsymbol{v}b\bar{b}$ 是 B 类易混淆的，但不是 A 类易混淆的。
- $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=n+3$ 当且仅当 $a\bar{a}\boldsymbol{v}$ 和 $\boldsymbol{v}b\bar{b}$ 既不是 B 类易混淆的，也不是 A 类易混淆的

证明　容易看出 $\boldsymbol{z}=a\bar{a}\boldsymbol{v}b\bar{b}$。

令 $S = I_t(\boldsymbol{x}) \cap I_t(\boldsymbol{y})$，则 $S = S^a \cup S_{\bar{b}} \cup S_b^{\bar{a}}$ 且

$$\begin{aligned} S^a &= a\left(I_t(\bar{a}\boldsymbol{v}b) \cap I_{t-1}(\bar{a}\boldsymbol{v}b\bar{b})\right) = aI_{t-1}(\bar{a}\boldsymbol{v}b\bar{b}) \subseteq I_{t-1}(\boldsymbol{z}), \\ S_{\bar{b}} &= \left(I_{t-1}(a\bar{a}\boldsymbol{v}b) \cap I_t(\bar{a}\boldsymbol{v}b)\right)\bar{b} = I_{t-1}(a\bar{a}\boldsymbol{v}b)\bar{b} \subseteq I_{t-1}(\boldsymbol{z}), \\ S_b^{\bar{a}} &= \bar{a}\left(I_{t-1}(a\bar{a}\boldsymbol{v}) \cap I_{t-1}(\boldsymbol{v}b\bar{b})\right)b. \end{aligned}$$

如果 $a\bar{a}\boldsymbol{v} = \boldsymbol{v}b\bar{b}$，则 $\boldsymbol{v} = (a\bar{a})^m$（$m \geqslant 0$）且 $a = b$，或者 $\boldsymbol{v} = (a\bar{a})^m a$（$m \geqslant 0$）且 $a = \bar{b}$。这两种情形都和 $\left|I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})\right| = 1$ 矛盾，所以 $a\bar{a}\boldsymbol{v} \neq \boldsymbol{v}b\bar{b}$。这样一来我们可以得到 $\left|I_t(\boldsymbol{x}) \cap I_t(\boldsymbol{y})\right| = |S| = |S^a \cup S_{\bar{b}}| + |S_b^{\bar{a}}| \leqslant \left|I_{t-1}(\boldsymbol{z})\right| + N_2^+(n-1, t-1)$，等式成立当且仅当 $I_{t-1}(\boldsymbol{z}) = S^a \cup S_{\bar{b}}$ 且 $I_{t-1}(a\bar{a}\boldsymbol{v}) \cap I_{t-1}(\boldsymbol{v}b\bar{b})$ 的大小达到最大值。

若 $t = 2$，容易看出 $I_1(\boldsymbol{z}) = S^a \cup S_{\bar{b}}$。因此，$I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y}) = I_1(\boldsymbol{z}) \cup S_b^{\bar{a}}$ 并且 $\left|I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})\right| = \left|I_1(\boldsymbol{z})\right| + \left|S_b^{\bar{a}}\right| = n + 3 + \left|I_1(a\bar{a}\boldsymbol{v}) \cap I_1(\boldsymbol{v}b\bar{b})\right|$。此时，根据推论3.7我们可得到结论。 ∎

引理 3.9　令 $n \geqslant 3$，设 $\boldsymbol{x}, \boldsymbol{y} \in \Sigma_2^n$ 是 B 类易混淆的。如果 $I_1(\boldsymbol{x}) \cap I_1(\boldsymbol{y}) = \{\boldsymbol{z}\}$，则

$$I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y}) = I_1(\boldsymbol{z}) \cup J(\boldsymbol{x}, \boldsymbol{y}),$$

其中 $|J(\boldsymbol{x}, \boldsymbol{y})| \leqslant 2$。特别地，

$$\left|I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})\right| \leqslant I_2(n+1, 1) + N_2^+(n-1, 1).$$

证明　因为 $\boldsymbol{x}, \boldsymbol{y} \in \Sigma_2^n$ 是 B 类易混淆的，所以我们可以假设 $\boldsymbol{x} = \boldsymbol{u}a\bar{a}\boldsymbol{v}b\boldsymbol{w}$，$\boldsymbol{y} = \boldsymbol{u}\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}$，其中 $a, b \in \Sigma_2$ 且 $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \Sigma_2^*$。则 $\boldsymbol{z} = \boldsymbol{u}a\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}$。令 $S = I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})$。下面我们对 n 用归纳法。

初始情形为 $\boldsymbol{u} = \boldsymbol{w} = \varnothing$。此时在引理3.8的证明中，我们可令 $J(\boldsymbol{x}, \boldsymbol{y}) = S_b^{\bar{a}}$，于是结论成立。

假设我们已经对所有的 $n \leqslant k-1$ 证明了结论的正确性。现在我们要证明 $n = k$ 的情形。不失一般性，我们可以假设存在 $c \in \Sigma_2$ 和 $\boldsymbol{u}^* \in \Sigma_2^*$ 使得 $\boldsymbol{u} = c\boldsymbol{u}^*$，则 $S^{\bar{c}} = \{\bar{c}\boldsymbol{z}\} = I_1(\boldsymbol{z})^{\bar{c}}$ 并且 $S^c = c\left(I_2(\boldsymbol{u}^*a\bar{a}\boldsymbol{v}b\boldsymbol{w}) \cap I_2(\boldsymbol{u}^*\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w})\right)$。记 $\boldsymbol{X} = \boldsymbol{u}^*a\bar{a}\boldsymbol{v}b\boldsymbol{w}$，$\boldsymbol{Y} = \boldsymbol{u}^*\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}$，则根据归纳可知，$I_2(\boldsymbol{X}) \cap I_2(\boldsymbol{Y}) = I_1(\boldsymbol{u}^*a\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}) \cup J(\boldsymbol{X}, \boldsymbol{Y})$，其中 $|J(\boldsymbol{X}, \boldsymbol{Y})| \leqslant 2$。因为 $S^c = c\left(I_2(\boldsymbol{X}) \cap I_2(\boldsymbol{Y})\right) = cI_1(\boldsymbol{u}^*a\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}) \cup cJ(\boldsymbol{X}, \boldsymbol{Y}) = I_1(\boldsymbol{z})^c \cup cJ(\boldsymbol{X}, \boldsymbol{Y})$，所以 $S = S^{\bar{c}} \cup S^c = I_1(\boldsymbol{z}) \cup cJ(\boldsymbol{X}, \boldsymbol{Y})$。令 $J(\boldsymbol{x}, \boldsymbol{y}) = cJ(\boldsymbol{X}, \boldsymbol{Y})$，则证明完成。 ∎

定理 3.10　令 $n \geqslant 3$ 并设 $\boldsymbol{x}, \boldsymbol{y} \in \Sigma_2^n$。如果 $\left|I_1(\boldsymbol{x}) \cap I_1(\boldsymbol{y})\right| = 1$，则

$$\left|I_t(\boldsymbol{x}) \cap I_t(\boldsymbol{y})\right| \leqslant I_2(n+1, t-1) + N_2^+(n-1, t-1),$$

对任何的 $t \geqslant 2$ 都成立。

证明　因为 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=1$, 所以我们可以假设存在 $a,b\in\Sigma_2$ 和 $\boldsymbol{u},\boldsymbol{v},\boldsymbol{w}\in\Sigma_2^*$ 使得 $\boldsymbol{x}=\boldsymbol{u}a\bar{a}\boldsymbol{v}b\boldsymbol{w}$, $\boldsymbol{y}=\boldsymbol{u}\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}$。令 $n_0=|a\bar{a}\boldsymbol{v}b|$, 则 $n\geqslant n_0$。令 $S=I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})$。我们通过对 n 和 t 进行归纳来证明这个定理。

初始情形是 $n=n_0$ 或 $t=2$, 此时分别由引理3.8和引理3.9可知结论正确。现在我们假设对所有的 $n'<n$ 以及 $t'<t$, 定理都是正确的。不失一般性, 我们可以假设存在 $c\in\Sigma_2$ 以及 $\boldsymbol{u}^*\in\Sigma_2^*$ 使得 $\boldsymbol{u}=c\boldsymbol{u}^*$。很显然, $S=S^{\bar{c}}\cup S^c$ 且

$$\begin{aligned}S^{\bar{c}}&=\bar{c}\left(I_{t-1}(\boldsymbol{x})\cap I_{t-1}(\boldsymbol{y})\right),\\ S^c&=c\left(I_t(\boldsymbol{u}^*a\bar{a}\boldsymbol{v}b\boldsymbol{w})\cap I_t(\boldsymbol{u}^*\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w})\right).\end{aligned}$$

根据归纳, 我们有 $|S^{\bar{c}}|\leqslant I_2(n+1,t-2)+N_2^+(n-1,t-2)$ 以及 $|S^c|\leqslant I_2(n,t-1)+N_2^+(n-2,t-1)$。根据推论3.2和推论3.3中的公式, 我们可以得到下面两个恒等式

$$\begin{aligned}I_2(n+1,t-1)&=I_2(n+1,t-2)+I_2(n,t-1),\\ N_2^+(n-1,t-1)&=N_2^+(n-1,t-2)+N_2^+(n-2,t-1).\end{aligned}$$

证明完成。 ∎

3.4　2-插入信道

本节中, 我们考虑恰好发生两个插入错误的信道。除非特别申明, 我们总假设 $n\geqslant 2$ 是一个整数。

首先, 根据推论3.3可知 $N_2^+(n,2)=2n+4$。所以对任何的 $N>n+4$, 均有 $\rho(n,N;B_2^{I(2)})=0$。

其次, 若两个不同的 $\boldsymbol{x},\boldsymbol{y}\in\Sigma_2^n$ 满足 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|\geqslant 1$, 则推论3.2表明 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|\geqslant n+3$。这说明, 当 $1\leqslant N\leqslant n+3$ 时, 如果 $\mathcal{C}$ 是一个 $(n,N;B_2^{I(2)})$-重构码, 则 $\mathcal{C}$ 一定是一个 $(n,1;B_2^{I(1)})$-重构码。于是, $\rho(n,N;B_2^{I(2)})=\Omega(\log_2(n))$ 对任意的 $1\leqslant N\leqslant n+3$ 都成立 (见定理3.5)。进一步地, 当 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=0$ 时, 引理3.1表明 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|\leqslant N_2^+(n,2,2)=6$。因此, 当 $6<N\leqslant n+3$ 时, $\nu_2(\mathcal{C})<N$ 当且仅当 $\mathcal{C}$ 是一个 $(n,1;B_2^{I(1)})$-重构码。所以 $\rho(n,N;B_2^{I(2)})=\log_2(n)+\Theta(1)$ (见定理3.5)。

引理 3.11　设 $\boldsymbol{x}\neq\boldsymbol{y}\in\Sigma_2^n$, 其中 $n\geqslant 2$, 则 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=2n+4$ 当且仅当 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=2$。

证明　如果 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=0$, 在引理3.1中令 $\ell=2$, 我们得到 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|\leqslant 6<2n+4$。如果 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=1$, 则定理3.10表明 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|\leqslant n+5<2n+4$。因此必要性得证。

现在我们证明充分性。首先显然有 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|\leqslant 2n+4$。因为 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|$

$=2$，所以一定存在 $\boldsymbol{u},\boldsymbol{w}\in\Sigma_2^*$，$a\in\Sigma_2$ 以及 $m\geqslant 0$，使得

$$\begin{cases}\boldsymbol{x}=\boldsymbol{u}(a\bar{a})^{m+1}\boldsymbol{w}\\ \boldsymbol{y}=\boldsymbol{u}(\bar{a}a)^{m+1}\boldsymbol{w}\end{cases}\text{或者}\begin{cases}\boldsymbol{x}=\boldsymbol{u}(a\bar{a})^{m}a\boldsymbol{w}\\ \boldsymbol{y}=\boldsymbol{u}(\bar{a}a)^{m}\bar{a}\boldsymbol{w}\end{cases}.$$

对于左边的情形，容易验证 $I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})=\{\boldsymbol{u}(\bar{a}a)^{m+1}\bar{a}\boldsymbol{w},\boldsymbol{u}(a\bar{a})^{m+1}a\boldsymbol{w}\}$ 以及 $I_1(\boldsymbol{u}(\bar{a}a)^{m+1}\bar{a}\boldsymbol{w})\cap I_1(\boldsymbol{u}(a\bar{a})^{m+1}a\boldsymbol{w})=\{\boldsymbol{u}(\bar{a}a)^{m+2}\boldsymbol{w},\boldsymbol{u}(a\bar{a})^{m+2}\boldsymbol{w}\}$。又因为 $\left|I_1(\boldsymbol{u}(\bar{a}a)^{m+1}\bar{a}\boldsymbol{w})\right|=\left|I_1(\boldsymbol{u}(a\bar{a})^{m+1}a\boldsymbol{w})\right|=n+3$，所以 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|\geqslant 2n+4$。因此，$\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=2n+4$。充分性得证。

对于右边的情形，证明与上述类似，我们不再赘述。 ∎

第三，如果 $\boldsymbol{x},\boldsymbol{y}\in\Sigma_2^n$ 是两个不同的序列，并且满足 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|\leqslant 1$，则根据定理3.10，我们可以得到 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|\leqslant n+5$。因此根据引理3.11，当 $n+5<N\leqslant 2n+4$ 时，$\nu_2(C)<N$ 当且仅当 C 是一个 $(n,2;B_2^{I(1)})$-重构码。所以，$\rho(n,N;B_2^{I(2)})=\log_2\log_2(n)+\Theta(1)$（见定理3.5）。

最后，设 $n+3<N\leqslant n+5$，则一个 $(n,N;B_2^{I(2)})$-重构码一定是一个 $(n,2;B_2^{I(1)})$-重构码。因此，$\rho(n,N;B_2^{I(2)})=\log_2\log_2(n)-O(1)$（见文献 [35] 定理 24 的证明）。

我们将上述讨论结果总结为以下命题。

命题 3.12

$$\rho(n,N;B^{I(2)})=\begin{cases}0, & \text{若}N>2n+4,\\ \log_2\log_2(n)+\Theta(1), & \text{若}n+5<N\leqslant 2n+4,\\ \log_2\log_2(n)-O(1), & \text{若}N=n+4,n+5,\\ \log_2(n)+\Theta(1), & \text{若}6<N\leqslant n+3,\\ \Omega(\log_2(n)), & \text{若}2\leqslant N\leqslant 6,\\ \Theta(\log_2(n)), & \text{若}N=1.\end{cases}$$

最后一个情形，即 $N=1$，对应着一个 2-插入纠错码，目前最新的结果由文献 [76] 定理 I.1 给出。这篇文章的作者给出了目前最好的构造性的（冗余的）上界 $4\log_2(n)+O(\log_2\log_2(n))$。另一方面，目前已知最好的下界是 $2\log_2(n)-O(1)$（详见文献 [68]）。

综上所述，非平凡的情形有 $N\in\{n+4,n+5\}$ 和 $2\leqslant N\leqslant 6$。

3.4.1　$N=n+4,n+5$ 的情形

设 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 Σ_2^n 中两个不同的序列，其中 $n\geqslant 3$。因为当 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=0$ 时，$\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|\leqslant 6$，所以我们只需要搞清楚当 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=1$ 时，在什么条件下 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|$ 分别等于 $n+3,n+4$ 以及 $n+5$ 即可。本小节中，我们总

假设 $\left|I_1(\boldsymbol{x}) \cap I_1(\boldsymbol{y})\right| = 1$，则根据引理3.6 和注3.3，不失一般性，我们可以取

$$\begin{cases} \boldsymbol{x} = \boldsymbol{u}a\bar{a}\boldsymbol{v}b\boldsymbol{w} \\ \boldsymbol{y} = \boldsymbol{u}\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w} \end{cases}.$$

其中 $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \Sigma_2^*$，$a, b \in \Sigma_2$，并且 $\boldsymbol{v}$ 不满足以下两个条件中的任何一个:

$$\begin{aligned} \boldsymbol{v} &= (a\bar{a})^m (m \geqslant 0) \text{且} a = b, \\ \boldsymbol{v} &= (a\bar{a})^m a (m \geqslant 0) \text{且} a = \bar{b}. \end{aligned} \tag{3.1}$$

当 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 B 类易混淆的但不是 A 类易混淆的时候，下面的结果告诉我们更多的关于 $I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})$ 的信息，这个信息可以很大程度上简化我们后续的分析。

引理 3.13　对任何的 $a, b \in \Sigma_2$ 以及任何的 $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \Sigma_2^*$，如果 $\boldsymbol{u}a\bar{a}\boldsymbol{v}b\boldsymbol{w}$ 和 $\boldsymbol{u}\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}$ 是 A 类易混淆的，则

$$\begin{aligned} &I_2(\boldsymbol{u}a\bar{a}\boldsymbol{v}b\boldsymbol{w}) \cap I_2(\boldsymbol{u}\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}) \\ &= I_1(\boldsymbol{u}a\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}) \cup \boldsymbol{u}\left(I_2(a\bar{a}\boldsymbol{v}b) \cap I_2(\bar{a}\boldsymbol{v}b\bar{b}) \setminus I_1(a\bar{a}\boldsymbol{v}b\bar{b})\right)\boldsymbol{w}. \end{aligned}$$

此外，这是一个无交并。

证明　为了方便叙述，我们记 $\boldsymbol{x} = \boldsymbol{u}a\bar{a}\boldsymbol{v}b\boldsymbol{w}$，$\boldsymbol{y} = \boldsymbol{u}\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}$，$\tilde{\boldsymbol{x}} = a\bar{a}\boldsymbol{v}b$ 以及 $\tilde{\boldsymbol{y}} = \bar{a}\boldsymbol{v}b\bar{b}$。很显然，集合 $I_1(\boldsymbol{u}a\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w})$ 和集合 $\boldsymbol{u}\left(I_2(\tilde{\boldsymbol{x}}) \cap I_2(\tilde{\boldsymbol{y}}) \setminus I_1(a\bar{a}\boldsymbol{v}b\bar{b})\right)\boldsymbol{w}$ 是不相交的，于是我们只需要证明 $I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y}) = I_1(\boldsymbol{u}a\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}) \cup \boldsymbol{u}\left(I_2(\tilde{\boldsymbol{x}}) \cap I_2(\tilde{\boldsymbol{y}}) \setminus I_1(a\bar{a}\boldsymbol{v}b\bar{b})\right)\boldsymbol{w}$。容易看出 $I_1(\boldsymbol{u}a\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}) \cup \boldsymbol{u}\left(I_2(\tilde{\boldsymbol{x}}) \cap I_2(\tilde{\boldsymbol{y}}) \setminus I_1(a\bar{a}\boldsymbol{v}b\bar{b})\right)\boldsymbol{w} \subseteq I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})$，因此我们只要证明相反方向的包含关系成立即可。令 $\boldsymbol{z} \in I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})$。设 $k_1 < k_2$ 是 $\boldsymbol{x}$ 中的两个插入位，$\ell_1 < \ell_2$ 是 $\boldsymbol{y}$ 中两个插入位置。令 i 和 j 分别是令 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 不相同的最左边下标和最右边的下标。比较 k_1, k_2 和 i 的大小，我们分成三种情况讨论：(1) $k_1, k_2 \leqslant i$；(2) $k_1 \leqslant i, k_2 > i$；(3) $k_1, k_2 > i$。

情形（1）：$k_1, k_2 \leqslant i$，则 $\ell_1, \ell_2 > j$ 或 $\ell_1 \leqslant j, \ell_2 > j$。

子情形（1）：若 $\ell_1, \ell_2 > j$，则

$$\boldsymbol{z} \in \boldsymbol{u}\left(I_2(\tilde{\boldsymbol{x}}) \cap I_2(\tilde{\boldsymbol{y}})\right)\boldsymbol{w}.$$

子情形（2）：若 $\ell_1 \leqslant j, \ell_2 > j$，则

$$\begin{aligned} \boldsymbol{z} &\in I_2(\boldsymbol{u})a\bar{a}\boldsymbol{v}b\boldsymbol{w} \cap I_1(\boldsymbol{u}\bar{a}\boldsymbol{v}b)\bar{b}b\boldsymbol{w} \\ &= \left(I_2(\boldsymbol{u})a\bar{a}\boldsymbol{v} \cap I_1(\boldsymbol{u}\bar{a}\boldsymbol{v}b)\bar{b}\right)b\boldsymbol{w}. \end{aligned}$$

对于 $I_2(\boldsymbol{u})a\bar{a}\boldsymbol{v} \cap I_1(\boldsymbol{u}\bar{a}\boldsymbol{v}b)\bar{b}$，显然有

$$\begin{aligned} &I_2(\boldsymbol{u})a\bar{a}\boldsymbol{v} \cap I_1(\boldsymbol{u}\bar{a}\boldsymbol{v}b)\bar{b} \\ &= \left(I_2(\boldsymbol{u})a\bar{a}\boldsymbol{v} \cap \boldsymbol{u}I_1(\bar{a}\boldsymbol{v}b)\bar{b}\right) \cup \left(I_2(\boldsymbol{u})a\bar{a}\boldsymbol{v} \cap I_1(\boldsymbol{u})\bar{a}\boldsymbol{v}b\bar{b}\right) \\ &= \left(I_2(\boldsymbol{u})a\bar{a}\boldsymbol{v} \cap \boldsymbol{u}I_1(\bar{a}\boldsymbol{v}b)\bar{b}\right) \cup \left(I_1(\boldsymbol{u})\bar{a}a\bar{a}\boldsymbol{v} \cap I_1(\boldsymbol{u})\bar{a}\boldsymbol{v}b\bar{b}\right). \end{aligned}$$

如果 $I_1(\boldsymbol{u})\bar{a}a\bar{a}\boldsymbol{v} \cap I_1(\boldsymbol{u})\bar{a}\boldsymbol{v}b\bar{b}$ 不是空集，则 $a\bar{a}\boldsymbol{v} = \boldsymbol{v}b\bar{b}$。这等价于存在 $m \geqslant 0$，使得 $\boldsymbol{v} = (a\bar{a})^m$ 且 $a = b$，或 $\boldsymbol{v} = (a\bar{a})^m a$ 且 $a = \bar{b}$。两种情况均意味着 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 A 类易混淆的，矛盾。因此，$I_1(\boldsymbol{u})\bar{a}a\bar{a}\boldsymbol{v} \cap I_1(\boldsymbol{u})\bar{a}\boldsymbol{v}b\bar{b}$ 是空集。于是

$$\boldsymbol{z} \in \left(I_2(\boldsymbol{u})a\bar{a}\boldsymbol{v} \cap \boldsymbol{u}I_1(\bar{a}\boldsymbol{v}b)\bar{b}\right) b\boldsymbol{w} \subseteq \boldsymbol{u}I_1(\bar{a}\boldsymbol{v}b)\bar{b}b\boldsymbol{w} \subseteq \boldsymbol{u}I_2(\tilde{\boldsymbol{y}})\boldsymbol{w}.$$

这意味着 $\boldsymbol{z} \in \boldsymbol{u}\left(I_2(\tilde{\boldsymbol{x}}) \cap I_2(\tilde{\boldsymbol{y}})\right)\boldsymbol{w}$。

情形（2）：$k_1 \leqslant i, k_2 > i$。

子情形（1）：若 $\ell_1, \ell_2 \leqslant i$，则必然有 $k_2 > j$。所以我们得到

$$\begin{aligned}\boldsymbol{z} &\in I_1(\boldsymbol{u})a\bar{a}\boldsymbol{v}bI_1(\boldsymbol{w}) \cap I_2(\boldsymbol{u})\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}\\ &= I_1(\boldsymbol{u})a\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w} \cap I_1(\boldsymbol{u})a\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}\\ &\subseteq I_1(\boldsymbol{u}a\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}).\end{aligned}$$

子情形（2）：若 $\ell_1, \ell_2 > i$，则

$$\begin{aligned}\boldsymbol{z} &\in I_1(\boldsymbol{u})aI_1(\bar{a}\boldsymbol{v}b\boldsymbol{w}) \cap \boldsymbol{u}\bar{a}I_2(\boldsymbol{v}b\bar{b}\boldsymbol{w})\\ &= \boldsymbol{u}\bar{a}aI_1(\bar{a}\boldsymbol{v}b\boldsymbol{w}) \cap \boldsymbol{u}\bar{a}I_2(\boldsymbol{v}b\bar{b}\boldsymbol{w})\\ &= \boldsymbol{u}\bar{a}\left(aI_1(\bar{a}\boldsymbol{v}b\boldsymbol{w}) \cap I_2(\boldsymbol{v}b\bar{b}\boldsymbol{w})\right).\end{aligned}$$

注意到 $I_1(\bar{a}\boldsymbol{v}b\boldsymbol{w}) = I_1(\bar{a}\boldsymbol{v}b)\boldsymbol{w} \cup \bar{a}\boldsymbol{v}bI_1(\boldsymbol{w})$。于是我们得到

$$\begin{aligned}&aI_1(\bar{a}\boldsymbol{v}b\boldsymbol{w}) \cap I_2(\boldsymbol{v}b\bar{b}\boldsymbol{w})\\ &= \left(aI_1(\bar{a}\boldsymbol{v}b)\boldsymbol{w} \cap I_2(\boldsymbol{v}b\bar{b}\boldsymbol{w})\right) \cup \left(a\bar{a}\boldsymbol{v}bI_1(\boldsymbol{w}) \cap I_2(\boldsymbol{v}b\bar{b}\boldsymbol{w})\right)\\ &= \left(aI_1(\bar{a}\boldsymbol{v}b)\boldsymbol{w} \cap I_2(\boldsymbol{v}b\bar{b})\boldsymbol{w}\right) \cup \left(a\bar{a}\boldsymbol{v}bI_1(\boldsymbol{w}) \cap I_1(\boldsymbol{v}b\bar{b})I_1(\boldsymbol{w})\right).\end{aligned}$$

最后一个等式成立是因为 $I_2(\boldsymbol{v}b\bar{b}\boldsymbol{w}) = I_2(\boldsymbol{v}b\bar{b})\boldsymbol{w} \cup \boldsymbol{v}b\bar{b}I_2(\boldsymbol{w}) \cup I_1(\boldsymbol{v}b\bar{b})I_1(\boldsymbol{w})$。如果 $a\bar{a}\boldsymbol{v}bI_1(\boldsymbol{w}) \cap I_1(\boldsymbol{v}b\bar{b})I_1(\boldsymbol{w})$ 不是空集，则 $a\bar{a}\boldsymbol{v} = \boldsymbol{v}b\bar{b}$。因此 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 A 类易混淆的，矛盾。所以，$a\bar{a}\boldsymbol{v}bI_1(\boldsymbol{w}) \cap I_1(\boldsymbol{v}b\bar{b})I_1(\boldsymbol{w})$ 是空集，并且

$$\boldsymbol{z} \in \boldsymbol{u}\bar{a}\left(aI_1(\bar{a}\boldsymbol{v}b)\boldsymbol{w} \cap I_2(\boldsymbol{v}b\bar{b})\boldsymbol{w}\right) \subseteq \boldsymbol{u}\bar{a}I_2(\boldsymbol{v}b\bar{b})\boldsymbol{w} \subseteq \boldsymbol{u}I_2(\tilde{\boldsymbol{y}})\boldsymbol{w}.$$

这意味着 $\boldsymbol{z} \in \boldsymbol{u}\left(I_2(\tilde{\boldsymbol{x}}) \cap I_2(\tilde{\boldsymbol{y}})\right)\boldsymbol{w}$。

情形（3）：$k_1, k_2 > i$。此时我们必有 $\ell_1, \ell_2 \leqslant i$ 或 $\ell_1 \leqslant i, \ell_2 > i$。应用前两种情形的证明思路，我们可以得到 $\boldsymbol{z} \in \boldsymbol{u}\left(I_2(\tilde{\boldsymbol{x}}) \cap I_2(\tilde{\boldsymbol{y}})\right)\boldsymbol{w}$ 或 $\boldsymbol{z} \in I_1(\boldsymbol{u}a\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w})$。

结合情形（1）、（2）、（3），我们可以得到 $I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y}) \subseteq I_1(\boldsymbol{u}a\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}) \cup \boldsymbol{u}\left(I_2(\widetilde{\boldsymbol{x}}) \cap I_2(\tilde{\boldsymbol{y}}) \setminus I_1(a\bar{a}\boldsymbol{v}b\bar{b})\right)\boldsymbol{w}$。至此，证明完成。 ∎

令 $\boldsymbol{x}, \boldsymbol{y}$ 如前所述，令 $n' = |a\bar{a}\boldsymbol{v}b| = k + 3$，其中 $\boldsymbol{v} \in \Sigma_2^k$ 且 $k \geqslant 0$。引理3.13表明 $\left|I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})\right| = n + 3, n + 4, n + 5$ 当且仅当 $\left|I_2(a\bar{a}\boldsymbol{v}b) \cap I_2(\bar{a}\boldsymbol{v}b\bar{b})\right|$ 相应地分别等于 $n' + 3, n' + 4, n' + 5$。所以，我们可进一步地假设

$$\begin{cases}\boldsymbol{x} = a\bar{a}\boldsymbol{v}b\\ \boldsymbol{y} = \bar{a}\boldsymbol{v}b\bar{b}\end{cases},$$

表 3.1　定理3.14的情形 (ii)

	$\boldsymbol{v}$	条件
$a=b$	$(a\bar{a})^i\bar{a}^j(a\bar{a})^k$	$i\geqslant 0, j\geqslant 2, k\geqslant 0$
	$(a\bar{a})^i a^j(a\bar{a})^k$	$i\geqslant 0, j\geqslant 2, k\geqslant 0$
	$(a\bar{a})^i(\bar{a}a\bar{a})^j(\bar{a}a)^k\bar{a}$	$i\geqslant 0, j\geqslant 1, k\geqslant 0$
	$(a\bar{a})^i a(a\bar{a}a)^j(a\bar{a})^k$	$i\geqslant 0, j\geqslant 1, k\geqslant 0$
$a=\bar{b}$	$(a\bar{a})^i\bar{a}^j(\bar{a}a)^k$	$i\geqslant 0, j\geqslant 1, k\geqslant 0$
	$(a\bar{a})^i a^j(\bar{a}a)^k$	$i\geqslant 0, j\geqslant 3, k\geqslant 0$
	$(a\bar{a})^i(\bar{a}a\bar{a})^j(\bar{a}a)^k$	$i\geqslant 0, j\geqslant 1, k\geqslant 0$
	$(a\bar{a})^i a(a\bar{a}a)^j(a\bar{a})^k a$	$i\geqslant 0, j\geqslant 1, k\geqslant 0$

其中 $\boldsymbol{v}$ 不满足式子 (3.1) 所列的条件。

在本章后续内容中，我们作如下约定：给定一个序列 $\boldsymbol{x}=x_i\cdots x_j$，如果 $i=j+1$，则我们将 $\boldsymbol{x}$ 看成空序列。

到这里，我们可以给出本节的第一个主要结果（即定理3.14）了。这个定理告诉我们在什么样的条件下，$\left|I_2(a\bar{a}\boldsymbol{v}b)\cap I_2(\bar{a}\boldsymbol{v}b\bar{b})\right|=n'+3,n'+4,n'+5$ 成立。

定理 3.14　在上述假设条件下，我们有如下结论：

(i) $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=n'+5$ 当且仅当
- 如果 $a=b$，则存在 $i,j\geqslant 0$，使得 $\boldsymbol{v}\in\{(a\bar{a})^i a(a\bar{a})^j,(a\bar{a})^i(\bar{a}a)^j\bar{a}\}$。
- 如果 $a=\bar{b}$，则存在 $i,j\geqslant 0$，使得 $\boldsymbol{v}\in\{(a\bar{a})^i(\bar{a}a)^j,(a\bar{a})^i aa(\bar{a}a)^j\}$。

(ii) $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=n'+4$ 当且仅当 a,b 和 $\boldsymbol{v}$ 满足表3.1中所列的条件之一。

(iii) 上述两条都不满足的时候，$\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=n'+3$（其中 $\boldsymbol{v}$ 不满足式子 (3.1) 所列的条件）。

证明　我们只需要证明 (i) 和 (ii) 即可。为了叙述简便，我们记 $\tilde{\boldsymbol{x}}=a\bar{a}\boldsymbol{v}$，$\tilde{\boldsymbol{y}}=\boldsymbol{v}b\bar{b}$。则因为 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=1$，所以 $\tilde{\boldsymbol{x}}\neq\tilde{\boldsymbol{y}}$（见引理3.8的证明）。

(i). 根据引理3.8，我们可知 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=n'+5$ 当且仅当 $a\bar{a}\boldsymbol{v}$ 和 $\boldsymbol{v}b\bar{b}$ 是 A 类易混淆的。这意味着存在 $\boldsymbol{u},\boldsymbol{c},\boldsymbol{w}\in\Sigma_2^*$，使得

$$a\bar{a}\boldsymbol{v}=\boldsymbol{u}\boldsymbol{c}\boldsymbol{w}\ \text{且}\boldsymbol{v}b\bar{b}=\boldsymbol{u}\bar{\boldsymbol{c}}\boldsymbol{w},\tag{3.2}$$

其中 $\boldsymbol{c}$ 是一个长度大于等于 1 的交错序列。设 $|\boldsymbol{u}|=s,|\boldsymbol{w}|=t$ 以及 $\boldsymbol{v}=v_1\cdots v_k$，其中 $s,t,k\geqslant 0$。因为 $wt_H(a\bar{a}\boldsymbol{v})=wt_H(\boldsymbol{v}b\bar{b})$，所以 $|\boldsymbol{c}|=d_H(a\bar{a}\boldsymbol{v},\boldsymbol{v}b\bar{b})\geqslant 2$，因此

$s+t=k+2-|\boldsymbol{c}|\leqslant k$。从式子 (3.2) 我们能够看出

$$\begin{aligned}\tilde{x}_1\cdots\tilde{x}_s&=\tilde{y}_1\cdots\tilde{y}_s,\\ \tilde{x}_{s+1}\cdots\tilde{x}_{k+2-t}&=\overline{\tilde{y}_{s+1}\cdots\tilde{y}_{k+2-t}},\\ \tilde{x}_{k+3-t}\cdots\tilde{x}_{k+2}&=\tilde{y}_{k+3-t}\cdots\tilde{y}_{k+2},\\ \tilde{x}_{s+1}\cdots\tilde{x}_{k+2-t}&\text{是交错序列.}\end{aligned}\tag{3.3}$$

如果 $k\geqslant s+t+1$，则 $k+2-t\geqslant s+3$。式子 (3.3) 表明

$$\tilde{x}_{s+1}\tilde{x}_{s+2}\tilde{x}_{s+3}\text{是交错序列}$$

并且

$$\tilde{x}_{s+1}=\overline{\tilde{y}_{s+1}},\ \tilde{x}_{s+2}=\overline{\tilde{y}_{s+2}}.$$

如果 $s=0$, 则 $k\geqslant 1$。此时 $\tilde{x}_1\tilde{x}_2\tilde{x}_3=a\bar{a}v_1, v_1=\tilde{y}_1=\bar{a}$。但是这时候 $\tilde{x}_1\tilde{x}_2\tilde{x}_3=a\bar{a}\bar{a}$ 不是交错的。

如果 $s=1$，则 $k\geqslant 2$。此时 $\tilde{x}_2\tilde{x}_3\tilde{x}_4=\bar{a}v_1v_2$，$v_1=\tilde{y}_1=a$，$v_2=\tilde{y}_2=a$。但这时候 $\tilde{x}_2\tilde{x}_3\tilde{x}_4=\bar{a}aa$ 不是交错序列。

如果 $s\geqslant 2$, 则 $k\geqslant s+1$, 此时 $\tilde{x}_{s+1}\tilde{x}_{s+2}\tilde{x}_{s+3}=v_{s-1}v_sv_{s+1}$。从式子 (3.3) 的第一个等式我们知道 $v_1v_2\cdots v_s$ 是交错序列。另一方面，$v_{s+1}=\tilde{y}_{s+1}=\overline{\tilde{x}_{s+1}}=\bar{v}_{s-1}$。再一次地，可以看出 $\tilde{x}_{s+1}\tilde{x}_{s+2}\tilde{x}_{s+3}=v_{s-1}v_sv_s$ 不是交错序列。

综上所述，$k=s+t$ 对所有的 $s,t\geqslant 0$ 都成立。另一方面，$s+t=k+2-|\boldsymbol{c}|$, 所以 $|\boldsymbol{c}|=2$。这样一来，式子 (3.3) 就变成了

$$\begin{aligned}\tilde{x}_1\cdots\tilde{x}_s&=\tilde{y}_1\cdots\tilde{y}_s,\\ \tilde{x}_{s+1}\tilde{x}_{s+2}&=\overline{\tilde{y}_{s+1}\tilde{y}_{s+2}},\\ \tilde{x}_{s+3}\cdots\tilde{x}_{k+2}&=\tilde{y}_{s+3}\cdots\tilde{y}_{k+2},\\ \tilde{x}_{s+1}\tilde{x}_{s+2}&\text{是交错序列.}\end{aligned}\tag{3.4}$$

接下来，我们将根据 s 和 k 的取值来确定 $\boldsymbol{v}$ 的值。在这之前，令 $v_{-1}=a, v_0=\bar{a}$。事实上，v_{-1}, v_0 分别表示 $\tilde{x}_1, \tilde{x}_2$。有了这个规定之后，容易看出 $\tilde{x}_i=v_{i-2}$ 对任何的 $1\leqslant i\leqslant k+2$ 都成立。式子 (3.4) 中的前两个条件表明 $v_{-1}v_0\cdots v_s$ 是交错序列且对任何的 $s\geqslant 0$，$v_{s+1}=\bar{v}_{s-1}=v_s$ 都成立, $v_{s+2}=\bar{v}_s=v_{s-1}$。因此，对所有的 $s\geqslant 0$，下面的式子都成立：

$$v_{-1}v_0\cdots v_s=\begin{cases}(a\bar{a})^{\frac{s+2}{2}} & \text{若}s\text{是偶数},\\ (a\bar{a})^{\frac{s+1}{2}}a & \text{若}s\text{是奇数}.\end{cases}\tag{3.5}$$

注意到 $k=s+t$ 以及 $t\geqslant 0$。所以，我们分成三种情形进行讨论。

首先，假设 $k\geqslant s+2$。这种情况下，$k+2\geqslant s+4$ 并且 $t\geqslant 2$。然后根据式子 (3.4) 中的第三个恒等式，我们得出 $v_{k-1}=\tilde{y}_{k+1}=b$ 以及 $v_k=\tilde{y}_{k+2}=\bar{b}$。此外，式

子 (3.4) 的第三个等式以及 $v_{s+1} \neq v_{s+2}$ 表明 $v_{s+1}v_{s+2}\cdots v_k$ 是交错序列。现在，根据上述讨论以及式子 (3.5)，我们可以得到：对所有的 $0 \leqslant s \leqslant k-2$，当 $a = \bar{b}$ 时，

$$\boldsymbol{v} = v_1 \cdots v_k = \begin{cases} (a\bar{a})^{\frac{s}{2}}(\bar{a}a)^{\frac{k-s}{2}} & \text{若}k, s\text{都是偶数}, \\ (a\bar{a})^{\frac{s-1}{2}}aa(\bar{a}a)^{\frac{k-1-s}{2}} & \text{若}s\text{是奇数且}k\text{是偶数}, \end{cases}$$

以及当 $a = b$ 时，

$$\boldsymbol{v} = v_1 \cdots v_k = \begin{cases} (a\bar{a})^{\frac{s}{2}}(\bar{a}a)^{\frac{k-1-s}{2}}\bar{a} & \text{若}s\text{是偶数且}k\text{是奇数}, \\ (a\bar{a})^{\frac{s-1}{2}}a(a\bar{a})^{\frac{k-s}{2}} & \text{若}k, s\text{都是奇数}. \end{cases}$$

其次，当 $k = s+1$ 时，$v_{s+1} = v_s = \bar{b}$。因此，当 s 是偶数的时候，$\boldsymbol{v} = (a\bar{a})^{\frac{s}{2}}\bar{a}$ 且 $a = b$；当 s 是奇数的时候，$\boldsymbol{v} = (a\bar{a})^{\frac{s-1}{2}}aa$ 且 $a = \bar{b}$。

最后，当 $k = s$ 时，必然有 $v_s = b$ 以及 $v_{s-1} = \bar{b}$。因此，当 s 是偶数的时候，$\boldsymbol{v} = (a\bar{a})^{\frac{s}{2}}$ 并且 $a = \bar{b}$；当 s 是奇数的时候，$\boldsymbol{v} = (a\bar{a})^{\frac{s-1}{2}}a$ 并且 $a = b$。

至此，(i) 的证明已完成。

(ii). 根据引理3.8，$\left|I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})\right| = n' + 4$ 当且仅当 $a\bar{a}\boldsymbol{v}$ 和 $\boldsymbol{v}b\bar{b}$ 是 B 类易混淆的，但不是 A 类易混淆的。也就是说，存在 $\boldsymbol{u}, \tilde{\boldsymbol{v}}, \boldsymbol{w} \in \Sigma_2^*$ 以及 $\alpha, \beta \in \Sigma_2$，使得

$$a\bar{a}\boldsymbol{v} = \boldsymbol{u}\alpha\bar{\alpha}\tilde{\boldsymbol{v}}\beta\boldsymbol{w},\ \boldsymbol{v}b\bar{b} = \boldsymbol{u}\bar{\alpha}\tilde{\boldsymbol{v}}\beta\bar{\beta}\boldsymbol{w}, \tag{3.6}$$

或者

$$a\bar{a}\boldsymbol{v} = \boldsymbol{u}\bar{\alpha}\tilde{\boldsymbol{v}}\beta\bar{\beta}\boldsymbol{w},\ \boldsymbol{v}b\bar{b} = \boldsymbol{u}\alpha\bar{\alpha}\tilde{\boldsymbol{v}}\beta\boldsymbol{w}. \tag{3.7}$$

设 $|\boldsymbol{u}| = s$，$|\boldsymbol{w}| = t$。因为 $a\bar{a}\boldsymbol{v}$ 和 $\boldsymbol{v}b\bar{b}$ 的汉明重量的奇偶性相同，所以 $\beta = \bar{\alpha}$。设 $\boldsymbol{v} = v_1 \cdots v_k$，则 $k+2 = s+t+3+|\tilde{\boldsymbol{v}}|$，所以 $k \geqslant s+t+1$。

为了后面叙述的方便，令 $v_{-1} = a$，$v_0 = \bar{a}$，$v_{k+1} = b$ 以及 $v_{k+2} = \bar{b}$。则容易看出 $\tilde{x}_i = v_{i-2}$，$\tilde{y}_i = v_i$ 对任何的 $1 \leqslant i \leqslant k+2$ 都成立。式子 (3.6) 或式子 (3.7) 表明下面两个恒等式

$$\begin{matrix} v_{-1}\cdots v_{s-2} = v_1 \cdots v_s \\ v_{k-t+1}\cdots v_k = v_{k-t+3}\cdots v_{k+2} \end{matrix}, \tag{3.8}$$

对任何的 $s, t \geqslant 0$ 以及任何的 $k \geqslant s+t+1$ 都成立。根据式子 (3.8) 的第一个等式，我们可知 $v_{-1}v_0 \cdots \cdots v_s$ 和式子 (3.5) 中给出的一模一样。式子 (3.8) 中的第二个等式表明

$$v_{k-t+1}\cdots v_{k+2} = \begin{cases} (v_{k-t+1}v_{k-t+2})^{\frac{t+2}{2}} & \text{若}t\text{是偶数}, \\ (v_{k-t+1}v_{k-t+2})^{\frac{t+1}{2}}v_{k-t+1} & \text{若}t\text{是奇数}. \end{cases} \tag{3.9}$$

由式子 (3.9) 可以看出：如果 $t \geqslant 2$ 偶数或者 $t \geqslant 1$ 是奇数，则 $\bar{b} = v_{k+2} = v_k$。然而，如果 $t = 0$，我们并不能从式子 (3.9) 得到任何有用的信息。进一步地，当 t 是偶

数时，$v_{k+1} = v_{k-t+1}$，$v_{k+2} = v_{k-t+2}$；当 t 是奇数时，$v_{k+1} = v_{k-t+2}$，$v_{k+2} = v_{k-t+1}$。因此根据 $v_{k+1} \neq v_{k+2}$ 我们得出 $v_{k-t+1} \neq v_{k-t+2}$。

现在根据式子 (3.6) 或式子 (3.7)，我们把讨论分成两种情形。

- 首先，如果式子 (3.6) 成立，则

$$\begin{aligned} &v_{s-1} = \alpha = \bar{v}_s = \bar{v}_{s+1}, \\ &v_{k-t} = \beta = \bar{v}_{k-t+2} = v_{k-t+1}, \\ &v_{s+1} \cdots v_{k-t-1} = v_{s+2} \cdots v_{k-t}. \end{aligned} \tag{3.10}$$

上面的三个恒等式表明

$$\bar{v}_{s-1} = v_s = \cdots = v_{k-t+1} = \bar{v}_{k-t+2}. \tag{3.11}$$

所以，如果 $t = 0$，则 $\bar{b} = v_{k+2} = \bar{v}_k$. 。结合式子 (3.5)，(3.9)，(3.11)，可知对所有的 $s, t \geqslant 0$ 以及所有的 $k \geqslant s + t + 1$，下面结论成立：

$$\boldsymbol{v} = v_1 \cdots v_k = \begin{cases} (a\bar{a})^{\frac{s}{2}} \bar{a}^{k-s-t} (\bar{a}a)^{\frac{t}{2}}, & s, t\text{都是偶数}, \\ (a\bar{a})^{\frac{s}{2}} \bar{a}^{k-s-t} (\bar{a}a)^{\frac{t-1}{2}} \bar{a}, & s\text{是偶数，}t\text{是奇数}, \\ (a\bar{a})^{\frac{s-1}{2}} a^{k+1-s-t} (a\bar{a})^{\frac{t}{2}}, & s\text{是奇数，}t\text{是偶数}, \\ (a\bar{a})^{\frac{s-1}{2}} a^{k+1-s-t} (a\bar{a})^{\frac{t-1}{2}} a, & s, t\text{都是奇数}。 \end{cases} \tag{3.12}$$

其中第一个和第四个等式对应着 $a = \bar{b}$ 的情形，而第二个和第三个等式对应着 $a = b$ 的情形。

- 其次，如果式子 (3.7) 成立，与式子 (3.6) 对应的情形比较可知，唯一的区别在于式子 (3.10) 变成了

$$\begin{aligned} &v_{s-1} = v_{s+2} = \bar{v}_{s+1}, \\ &\bar{v}_{k-t} = v_{k-t+2} = v_{k-t-1}, \\ &v_s \cdots v_{k-t-2} = v_{s+3} \cdots v_{k-t+1}. \end{aligned} \tag{3.13}$$

所以，如果 $t = 0$，则 $\bar{b} = v_{k+2} = \bar{v}_k$。如前所述，$k \geqslant s + t + 1$。事实上，从式子 (3.13) 的前两个等式可以推出 $k \geqslant s + t + 2$。若不然，式子 (3.13) 的前两个等式会导致 $v_{s-1} = \bar{v}_{s+1} = v_s$，这与式子 (3.5) 矛盾。这样一来，式子 (3.13) 的三个等式就表明 $v_{s+1} \cdots v_{l-t+1}$ 是一个周期等于 3 的序列，并且 $v_{s+1} = \bar{v}_{s-1} = v_s = v_{s+3}$，$v_{s+2} = v_{s-1}$。

如果 $k \equiv s+t \pmod 3$,则 $k-t+1 \equiv s+1 \pmod 3$。于是根据序列 $v_{s+1} \cdots v_{l-t+1}$ 的周期性我们得出 $v_{k-t+1} = v_{s+1} = v_s$ 和 $v_{k-t+2} = v_{s+2} = v_{s-1} \neq v_{k-t+1}$。其中最后一个等式由式子 (3.5) 得出。

如果 $k \equiv s + t + 1 \pmod 3$，则 $k - t + 1 \equiv (s + 1) + 1 \pmod 3$。所以 $v_{k-t+1} = v_{s+2} = v_{s-1}$ 并且 $v_{k-t+2} = v_{s+3} = v_s \neq v_{k-t+1}$。

如果 $k \equiv s+t+2 \pmod 3$，则 $k-t+1 \equiv (s+1)+2 \pmod 3$。所以 $v_{k-t+1} = v_{s+3} = v_s$ 并且 $v_{k-t+2} = \overline{v_{k-t}} = \overline{v_{s+2}} = \overline{v_{s-1}} = v_s$，其中最后一个等式根据式子 (3.5) 得到。这与 $v_{k-t+2} \neq v_{k-t+1}$ 矛盾。

由以上讨论，我们得出

$$v_{s+1}\cdots v_{l-t} = \begin{cases} (v_s v_{s-1} v_s)^{\frac{l-s-t}{3}}, & \text{如果} l \equiv s+t \pmod 3, \\ (v_s v_{s-1} v_s)^{\frac{l-s-t-1}{3}} v_s, & \text{如果} l \equiv s+t+1 \pmod 3. \end{cases} \tag{3.14}$$

现在,结合式子 (3.5),(3.9),(3.14),对于所有的 $s,t,\geqslant 0$ 以及所有的 $k \geqslant s+t+2$，我们得到 $\boldsymbol{v}$ 的八个取值，并将其列在表3.2中。注意，在表3.2的第三行和第七行中，t 的取值不能为 0。否则的话，我们将得到 $v_l = v_{l-1}$，这与式子 (3.13) 的第二个等式矛盾。

根据式子 (3.12) 和表3.2，我们得到表3.1中的结果。容易验证当 $\boldsymbol{v}$ 取这些值的时候，$a\bar{a}\boldsymbol{v}$ 和 $\boldsymbol{v}b\bar{b}$ 是 B 类易混淆的。再将表3.1和 (i) 中的结果比较可知，$a\bar{a}\boldsymbol{v}$ 和 $\boldsymbol{v}b\bar{b}$ 不是 A 类易混淆的。至此，我们完成了（ii）的证明。 ∎

表 3.2　式子 (3.7) 推出的 $\boldsymbol{v}$ 的八个取值

$\boldsymbol{v}$	参数 k,s,t 的条件	$a=b$
$(a\bar{a})^{\frac{s}{2}}(\bar{a}a\bar{a})^{\frac{k-s-t}{3}}(\bar{a}a)^{\frac{t}{2}}$	s 偶, t 奇, $k \equiv s+t \pmod 3$	否
$(a\bar{a})^{\frac{s}{2}}(\bar{a}a\bar{a})^{\frac{k-s-t}{3}}(\bar{a}a)^{\frac{t-1}{2}}\bar{a}$	s 偶, t 奇, $k \equiv s+t \pmod 3$	是
$(a\bar{a})^{\frac{s}{2}}(\bar{a}a\bar{a})^{\frac{k-s-t-1}{3}}(\bar{a}a)^{\frac{t}{2}}\bar{a}$	s 偶, $t \geqslant 2$ 偶 $k \equiv s+t+1 \pmod 3$	是
$(a\bar{a})^{\frac{s}{2}}(\bar{a}a\bar{a})^{\frac{k-s-t-1}{3}}(\bar{a}a)^{\frac{t+1}{2}}$	s 偶, t 奇 $k \equiv s+t+1 \pmod 3$	否
$(a\bar{a})^{\frac{s-1}{2}}a(a\bar{a}a)^{\frac{k-s-t}{3}}(a\bar{a})^{\frac{t}{2}}$	s 奇, t 偶 $k \equiv s+t \pmod 3$	是
$(a\bar{a})^{\frac{s-1}{2}}a(a\bar{a}a)^{\frac{k-s-t}{3}}(a\bar{a})^{\frac{t-1}{2}}a$	s 奇, t 奇 $k \equiv s+t \pmod 3$	否
$(a\bar{a})^{\frac{s-1}{2}}a(a\bar{a}a)^{\frac{k-s-t-1}{3}}(a\bar{a})^{\frac{t}{2}}a$	s 奇, $t \geqslant 2$ 偶 $k \equiv s+t+1 \pmod 3$	否
$(a\bar{a})^{\frac{s-1}{2}}a(a\bar{a}a)^{\frac{k-s-t-1}{3}}(a\bar{a})^{\frac{t+1}{2}}$	s 奇, t 奇 $k \equiv s+t+1 \pmod 3$	是

有了这些结果后，我们就可以构造相应的码了。我们先给出一些将会用得到的结论。

定义 3.5　对任何的 $\boldsymbol{x} \in \Sigma_2^n$，我们定义

$$\mathrm{Inv}(\boldsymbol{x}) = \left|\{(i,j) \mid 1 \leqslant i < j \leqslant n \text{ 并且} x_i > x_j\}\right|.$$

注　根据这个定义，我们有以下两个简单的观察。

(*i*) 对任何的 $a \in \Sigma_2$ 以及任何的 $\boldsymbol{u},\boldsymbol{v},\boldsymbol{w} \in \Sigma_2^*$，容易验证 $\mathrm{Inv}(\boldsymbol{u}a\bar{a}\boldsymbol{v}\bar{a}\boldsymbol{w}) - \mathrm{Inv}(\boldsymbol{u}\bar{a}\boldsymbol{v}\bar{a}a\boldsymbol{w}) = \mathrm{Inv}(a\bar{a}\boldsymbol{v}\bar{a}) - \mathrm{Inv}(\bar{a}\boldsymbol{v}\bar{a}a)$。

(*ii*) 对任何的 $a \in \Sigma_2$ 和 $\boldsymbol{v} \in \Sigma_2^*$，容易验证 $|\mathrm{Inv}(a\bar{a}\boldsymbol{v}\bar{a}) - \mathrm{Inv}(\bar{a}\boldsymbol{v}\bar{a}a)| = N_{\boldsymbol{v}}(\bar{a}) + 2$，其中 $N_{\boldsymbol{v}}(\bar{a})$ 表示 $\boldsymbol{v}$ 中 $\bar{a}$ 的个数。

定义 3.6　设 ℓ 和 t 是两个满足 $\ell < t$ 的正整数。如果对所有的 $1 \leqslant i \leqslant t-\ell$ 都成立 $x_i = x_{i+l}$，则我们称序列 $\boldsymbol{x} = x_1 \cdots x_t \in \Sigma_2^t$ 具有周期 ℓ。我们用 $R(n,\ell,t)$ 来表示 Σ_2^n 中满足以下性质的序列 $\boldsymbol{x}$ 全体：$\boldsymbol{x}$ 的任何周期小于等于 ℓ 的子字的长度都不超过 t。

引理 3.15　[78] 对所有的正整数 ℓ，如果 $t \geqslant \lceil \log_2(n) \rceil + \ell + 1$，则我们有 $|R(n,\ell,t)| \geqslant 2^{n-1}$。

定理 3.16 ($N = n+5$)　对任何的 $n \geqslant 3, P \geqslant 12$，其中 $6 \mid P$，令 $c \in \mathbb{Z}_{1+\frac{P}{2}}$ 以及 $d \in \mathbb{Z}_2$，我们将 $C(n;c,d)$ 定义为满足下面所有条件的序列 $\boldsymbol{x} = x_1 \cdots x_n \in \Sigma_2^n$ 的全体构成的集合：

- $\mathrm{Inv}(\boldsymbol{x}) \equiv c \pmod{1+\frac{P}{2}}$.
- $\sum_{i=1}^{n} x_i \equiv d \pmod 2$.
- $\boldsymbol{x} \in R(n,2,\frac{P}{3})$.

则 $C(n;c,d)$ 是一个 $(n, n+5; B_2^{I(2)})$-重构码。进一步地，如果 $\frac{P}{3} = \lceil \log_2(n) \rceil + 3$，则可以取到 c 和 d，使得 $C(n;c,d)$ 的冗余至多为 $1+\log_2(P+2) = \log_2\log_2(n) + O(1)$。

证明　在 [35] 定理 17 中，该文作者对于 $(n,2;B_2^{I(1)})$-重构码给出了一个类似的构造。我们的构造和他们的构造的唯一差别在于第三个条件：在第三个条件中，我们要求任何一个 ℓ-周期 ($\ell \leqslant 2$) 子字的长度都小于等于 $\frac{P}{3}$，而它们的要求是长度不超过 P。因此，我们构造的码是他们构造的码的一个子码。所以，$\left|I_1(\boldsymbol{x}) \cap I_1(\boldsymbol{y})\right| \leqslant 1$，即 $\left|I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})\right| \leqslant n+5$ 对任何不同的 $\boldsymbol{x},\boldsymbol{y} \in C(n;c,d)$ 都成立。这样一来，我们只需要证明 $C(n;c,d)$ 中不存在两个不同的码字 $\boldsymbol{x}$ 和 $\boldsymbol{y}$，使得 $\left|I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})\right| = n+5$。

我们用反证法证明。如果存在这样不同的 $\boldsymbol{x},\boldsymbol{y}$，则不失一般性，我们可以假设

$$\begin{cases} \boldsymbol{x} = \boldsymbol{u}a\bar{a}\boldsymbol{v}b\boldsymbol{w}, \\ \boldsymbol{y} = \boldsymbol{u}\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}, \end{cases}$$

其中 $\boldsymbol{v}$ 满足定理3.14的第 (i) 条。因为 $C(n;c,d)$ 所有码字的汉明重量的奇偶性相同，所以 $a=\bar{b}$。于是由注3.4.1我们可知存在 $i,j\geqslant 0$ 满足 $2i,2j\leqslant\frac{P}{3}$，使得 $|\mathrm{Inv}(\boldsymbol{x})-\mathrm{Inv}(\boldsymbol{y})|=|\mathrm{Inv}(a\bar{a}\boldsymbol{v}\bar{a})-\mathrm{Inv}(\bar{a}\boldsymbol{v}\bar{a}a)|=i+j+2$，所以 $2i+2j+4\leqslant\frac{2P}{3}+4$。另一方面，因为 $(1+\frac{P}{2})\mid(i+j+2)$，所以 $2+P\leqslant 2i+2j+4$。因此 $\frac{P}{3}\leqslant 2$，矛盾。

根据引理3.15，当 $\frac{P}{3}=\lceil\log_2(n)\rceil+3$ 时，$\left|R(n,2,\frac{P}{3})\right|\geqslant 2^{n-1}$。所以根据鸽笼原理，一定存在 c 和 d 使得 $|C(n;c,d)|\geqslant\frac{2^{n-1}}{2(1+\frac{P}{2})}$。对于这样的 c 和 d，$C(n;c,d)$ 的冗余至多为 $1+\log_2(P+2)=\log_2\log_2(n)+O(1)$（当 n 充分大的时候）。 ∎

注　在上面的定理中，如果 $\frac{P}{3}=\lceil\log_2(n)\rceil+3$ 且 n 充分大，则 $\log_2\log_2(n)+\log_2 3+1<1+\log_2(P+2)<\log_2\log_2(n)+3$。

定理 3.17 ($N=n+4$)　对任何的 $n\geqslant 3, P\geqslant 12$，其中 $6\mid P$，令 $c\in\mathbb{Z}_{1+\frac{P}{2}}$ 以及 $d\in\mathbb{Z}_2$。我们将 $D(n;c,d)$ 定义为满足下面所有条件的序列 $\boldsymbol{x}=x_1\cdots x_n\in\Sigma_2^n$ 的全体构成的集合：

- $\mathrm{Inv}(\boldsymbol{x})\equiv c\pmod{1+\frac{P}{2}}$.
- $\sum_{i=1}^{n}x_i\equiv d\pmod 2$.
- $\boldsymbol{x}\in R(n,3,\frac{P}{6})$.

则 $D(n;c,d)$ 是一个 $(n,n+4;B_2^{I(2)})$-重构码。进一步地，如果 $\frac{P}{6}=\lceil\log_2(n)\rceil+4$，则可以取到 c 和 d，使得 $D(n;c,d)$ 的冗余至多为 $1+\log_2(P+2)=\log_2\log_2(n)+O(1)$。这个值要比定理3.16中构造的码的冗余大 1 个左右的比特。

证明　和定理3.16证明中的理由一样，我们可得出 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|\leqslant 1$ 对任何两个不同的码字 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 都成立。注意到定理3.17和定理3.16之间唯一的区别是：在定理3.17中我们要求 $\boldsymbol{x}\in R(n,3,\frac{P}{6})$，但在定理3.16中我们要求 $\boldsymbol{x}\in R(n,2,\frac{P}{3})$。这说明 $D(n;c,d)$ 是定理3.16构造的码的一个子码。因此，$\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|\leqslant n+4$ 对任何不同的 $\boldsymbol{x},\boldsymbol{y}\in C(n;c,d)$ 都成立。现在我们只需要证明不存在两个不同的码字 $\boldsymbol{x},\boldsymbol{y}\in C(n;c,d)$ 使得 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=n+4$。

我们用反证法证明。如果存在这样不同的 $\boldsymbol{x},\boldsymbol{y}$，则不失一般性，我们可以假设

$$\begin{cases}\boldsymbol{x}=\boldsymbol{u}a\bar{a}\boldsymbol{v}b\boldsymbol{w}\\ \boldsymbol{y}=\boldsymbol{u}\bar{a}\boldsymbol{v}b\bar{b}\boldsymbol{w}\end{cases},$$

其中 $\boldsymbol{v}$ 满足定理3.14的第 (ii) 条。因为 $D(n;c,d)$ 所有码字的汉明重量的奇偶性相同，所以我们得出 $a=\bar{b}$。用和定理3.16的证明中相同的过程，我们得到 $\frac{P}{3}\leqslant 2$，$\frac{2P}{9}\leqslant 1$，$\frac{11P}{18}\leqslant 4$，$\frac{13P}{18}\leqslant 2$，$\frac{5P}{9}\leqslant 2$ 以及 $\frac{2P}{3}\leqslant 2$，矛盾。

根据引理3.15，当 $\frac{P}{6}=\lceil\log_2(n)\rceil+4$ 时，$\left|R(n,2,\frac{P}{3})\right|\geqslant 2^{n-1}$。此时一定存在 c 和 d 使得 $|D(n;c,d)|\geqslant\frac{2^{n-1}}{2(1+\frac{P}{2})}$。对于这样的 c 和 d，$D(n;c,d)$ 的冗余至多为

$1+\log_2(P+2)=\log_2\log_2(n)+O(1)$（当 n 充分大时）。这个值要比定理3.16中构造的码的冗余大 1 个左右的比特。 ∎

注　在上述定理中，如果 $\frac{P}{6}=\lceil\log_2(n)\rceil+4$ 且 n 充分大，则 $\log_2\log_2(n)+\log_2 3+2<1+\log_2(P+2)<\log_2\log_2(n)+\log_2 7+1$。

3.4.2　$N=6$ 的情形

此时，若 C 是一个 $(n,N;B_2^{I_2(2)})$-重构码，则对任何不同的 $\boldsymbol{x},\boldsymbol{y}\in C$，$I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})=\varnothing$ 均成立。此外，我们有下面的引理。

引理 3.18　设 $\boldsymbol{x},\boldsymbol{y}\in\Sigma_2^n$，其中 $n\geqslant 2$，则 $I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})=\varnothing$ 当且仅当存在满足条件 $a\boldsymbol{d}\neq\boldsymbol{e}\bar{b}$ 和 $\boldsymbol{d}b\neq\bar{a}\boldsymbol{e}$ 的 $\boldsymbol{u},\boldsymbol{w},\boldsymbol{d},\boldsymbol{e}\in\Sigma_2^*$ 以及 $a,b\in\Sigma_2$，使得

$$\begin{cases}\boldsymbol{x}=\boldsymbol{u}a\boldsymbol{d}b\boldsymbol{w},\\ \boldsymbol{y}=\boldsymbol{u}\bar{a}\boldsymbol{e}\bar{b}\boldsymbol{w}.\end{cases}$$

证明　首先，对任何的 $\boldsymbol{u},\boldsymbol{w},\boldsymbol{d},\boldsymbol{e}\in\Sigma_2^*$ 和任何的 $a,b\in\Sigma_2$，容易验证

$$I_1(\boldsymbol{u}a\boldsymbol{d}b\boldsymbol{w})\cap I_1(\boldsymbol{u}\bar{a}\boldsymbol{e}\bar{b}\boldsymbol{w})=\boldsymbol{u}\left(I_1(a\boldsymbol{d}b)\cap I_1(\bar{a}\boldsymbol{e}\bar{b})\right)\boldsymbol{w},$$

以及 $I_1(a\boldsymbol{d}b)\cap I_1(\bar{a}\boldsymbol{e}\bar{b})=\varnothing$ 成立当且仅当 $a\boldsymbol{d}\neq\boldsymbol{e}\bar{b}$ 和 $\boldsymbol{d}b\neq\bar{a}\boldsymbol{e}$ 同时成立。于是，充分性得证。

另一方面，如果 $I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})=\varnothing$，则 $d_H(\boldsymbol{x},\boldsymbol{y})\geqslant 2$。因此，存在 $\boldsymbol{u},\boldsymbol{w},\boldsymbol{d},\boldsymbol{e}\in\Sigma_2^*$ 和 $a,b\in\Sigma_2$ 使得

$$\begin{cases}\boldsymbol{x}=\boldsymbol{u}a\boldsymbol{d}b\boldsymbol{w},\\ \boldsymbol{y}=\boldsymbol{u}\bar{a}\boldsymbol{e}\bar{b}\boldsymbol{w}.\end{cases}$$

于是必要性得证。 ∎

引理 3.19　沿用上面的记号，如果 $I_1(\boldsymbol{u}a\boldsymbol{d}b\boldsymbol{w})\cap I_1(\boldsymbol{u}\bar{a}\boldsymbol{e}\bar{b}\boldsymbol{w})=\varnothing$，则

$$I_2(\boldsymbol{u}a\boldsymbol{d}b\boldsymbol{w})\cap I_2(\boldsymbol{u}\bar{a}\boldsymbol{e}\bar{b}\boldsymbol{w})=\boldsymbol{u}\left(I_2(a\boldsymbol{d}b)\cap I_2(\bar{a}\boldsymbol{e}\bar{b})\right)\boldsymbol{w}.$$

特别地，$\left|I_2(\boldsymbol{u}a\boldsymbol{d}b\boldsymbol{w})\cap I_2(\boldsymbol{u}\bar{a}\boldsymbol{e}\bar{b}\boldsymbol{w})\right|=\left|I_2(a\boldsymbol{d}b)\cap I_2(\bar{a}\boldsymbol{e}\bar{b})\right|$。

证明　与引理3.13的证明类似，因此我们不再赘述。 ∎

引理 3.20　令 $n\geqslant 2$，设 $\boldsymbol{x},\boldsymbol{y}\in\Sigma_2^n$ 是两个不相同的序列。则 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|\leqslant 6$ 当且仅当 $I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})=\varnothing$.

证明　充分性由引理3.1（取 $t=\ell=2$）可得到。下面我们用反证法来证明必要性。首先，如果 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=2$，则引理3.11表明 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=2n+4>6$，矛盾。其次，如果 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=1$，则根据引理3.6我们有 $n\geqslant 3$。另一方面，当

$n=3$ 且 $\left|I_1(\boldsymbol{x})\cap I_1(\boldsymbol{y})\right|=1$ 时，定理3.14表明 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=n+5>6$，矛盾。当 $n\geqslant 4$ 时，$\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|\geqslant n+3>6$，矛盾。

综上，必要性成立。 ∎

有了上面的三个引理之后, 我们现在可以完全地刻画 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=6$ 的条件了。令 $S\triangleq I_2(a\boldsymbol{d}b)\cap I_2(\bar{a}\boldsymbol{e}\bar{b})$, 其中 $a\boldsymbol{d}\neq\boldsymbol{e}\bar{b}$ 并且 $\boldsymbol{d}b\neq\bar{a}\boldsymbol{e}$。则 $S=S_b^a\cup S_{\bar{b}}^a\cup S_b^{\bar{a}}\cup S_{\bar{b}}^{\bar{a}}$, 其中

$$\begin{aligned}
S_b^a &= a\left(I_2(\boldsymbol{d})\cap\{\bar{a}\boldsymbol{e}\bar{b}\}\right)b,\\
S_{\bar{b}}^a &= a\left(I_1(\boldsymbol{d}b)\cap I_1(\bar{a}\boldsymbol{e})\right)\bar{b},\\
S_b^{\bar{a}} &= \bar{a}\left(I_1(a\boldsymbol{d})\cap I_1(\boldsymbol{e}\bar{b})\right)b,\\
S_{\bar{b}}^{\bar{a}} &= \bar{a}\left(\{a\boldsymbol{d}b\}\cap I_2(\boldsymbol{e})\right)\bar{b}.
\end{aligned}$$

很显然，$S_b^a, S_{\bar{b}}^a$ $S_b^{\bar{a}}$ 和 $S_{\bar{b}}^{\bar{a}}$ 两两不相交。

定理 3.21　令 $n\geqslant 2$, 设 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 是 Σ_2^n 中两个不同的序列。则 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=6$ 当且仅当存在满足条件 $a\boldsymbol{d}\neq\boldsymbol{e}\bar{b}$ 和 $\boldsymbol{d}b\neq\bar{a}\boldsymbol{e}$ 的 $\boldsymbol{u},\boldsymbol{w},\boldsymbol{d},\boldsymbol{e}\in\Sigma_2^*$ 以及 $a,b\in\Sigma_2$，使得

$$\begin{cases}\boldsymbol{x}=\boldsymbol{u}a\boldsymbol{d}b\boldsymbol{w}\\ \boldsymbol{y}=\boldsymbol{u}\bar{a}\boldsymbol{e}\bar{b}\boldsymbol{w}\end{cases},$$

这里 $\boldsymbol{d}$ 和 $\boldsymbol{e}$ 满足下面的条件:

(i) 当 $a=b$ 时，$\boldsymbol{d}$ 和 $\boldsymbol{e}$ 必须满足表A.1中某一行的条件（见附录A）。

(ii) 当 $a=\bar{b}$ 时，$\boldsymbol{d}$ 和 $\boldsymbol{e}$ 必须满足表A.2中某一行的条件（见附录A）。

证明　从引理3.18，引理3.19和引理3.20，我们可以看出 $\left|I_2(\boldsymbol{x})\cap I_2(\boldsymbol{y})\right|=6$ 当且仅当存在 $\boldsymbol{u},\boldsymbol{w},\boldsymbol{d},\boldsymbol{e}\in\Sigma_2^*$ 和 $a,b\in\Sigma_2$，满足 $a\boldsymbol{d}\neq\boldsymbol{e}\bar{b}$ 和 $\boldsymbol{d}b\neq\bar{a}\boldsymbol{e}$，使得

$$\begin{cases}\boldsymbol{x}=\boldsymbol{u}a\boldsymbol{d}b\boldsymbol{w}\\ \boldsymbol{y}=\boldsymbol{u}\bar{a}\boldsymbol{e}\bar{b}\boldsymbol{w}\end{cases},$$

并且 $|S|=6$。另一方面，因为 $a\boldsymbol{d}\neq\boldsymbol{e}\bar{b}$ 以及 $\boldsymbol{d}b\neq\bar{a}\boldsymbol{e}$，所以 $|S|=6$ 当且仅当

$$\begin{aligned}
&\boldsymbol{d}b\text{和}\bar{a}\boldsymbol{e}\text{是 A 类易混淆的}\\
&a\boldsymbol{d}\text{和}\boldsymbol{e}\bar{b}\text{是 A 类易混淆的}\\
&\bar{a}\boldsymbol{e}\bar{b}\in I_2(\boldsymbol{d})\\
&a\boldsymbol{d}b\in I_2(\boldsymbol{e})
\end{aligned}\tag{3.15}$$

我们的思路就是利用上面的四个条件找出 $\boldsymbol{d}$ 和 $\boldsymbol{e}$ 的具体值。

设 $\boldsymbol{d}=d_1\cdots d_k$，$\boldsymbol{e}=e_1\cdots e_k$，其中 $k\geqslant 0$。记住当 $k=0$ 时，$\boldsymbol{d}$ 和 $\boldsymbol{e}$ 都是空序列。和之前一样，我们可以拓展 $\boldsymbol{d}$ 和 $\boldsymbol{e}$ 的下标至 $d_{k+1}=b$，$e_{-1}=a$，$e_0=\bar{a}$ 以及 $e_{k+1}=\bar{b}$。从式子 (3.15) 的第一个等式我们可以看出存在 $\tilde{\boldsymbol{u}},\tilde{\boldsymbol{u}},\boldsymbol{c}\in\Sigma_2^*$ 使得 $\boldsymbol{c}$ 是交

错序列，并且

$$\begin{cases} \boldsymbol{d}b = \tilde{\boldsymbol{u}}\boldsymbol{c}\tilde{\boldsymbol{u}}, \\ \bar{a}\boldsymbol{e} = \tilde{\boldsymbol{u}}\bar{\boldsymbol{c}}\tilde{\boldsymbol{u}}, \end{cases} \tag{3.16}$$

令 $|\boldsymbol{u}| = s$，$|\boldsymbol{w}| = t$，其中 $s, t \geqslant 0$。则因为 $\boldsymbol{d}b \neq \bar{a}\boldsymbol{e}$，所以 $k \geqslant s + t$。此时，式子 (3.16) 就等价于

$$\begin{aligned} &d_1 \cdots d_s = e_0 \cdots e_{s-1}, \\ &d_{s+1} \cdots d_{k+1-t} = \overline{e_s \cdots e_{k-t}}, \\ &d_{k+2-t} \cdots d_{k+1} = e_{k+1-t} \cdots e_k, \\ &e_s \cdots e_{k-t}\text{是交错序列.} \end{aligned} \tag{3.17}$$

我们将证明分成两种情形：（i）$t = 0$ 和（ii）$t \geqslant 1$。正如下面的推导所表明的一样，我们这样做的理由是当 $t = 0$ 时，我们有 $b = \bar{e}_k$；当 $t \geqslant 1$ 时，我们有 $b = e_k$。

情形 (i): $s \geqslant 0$ 并且 $t = 0$

在这种情况下，式子 (3.17) 等价于

$$\begin{aligned} &d_1 \cdots d_s = e_0 \cdots e_{s-1}, \\ &d_{s+1} \cdots d_{k+1} = \overline{e_s \cdots e_k}, \\ &e_s \cdots e_k\text{是交错序列.} \end{aligned} \tag{3.18}$$

因此 $\boldsymbol{d} = e_0 \cdots e_{s-1}\overline{e_s \cdots e_{k-1}}$ 并且 $e_k = \bar{d}_{k+1} = \bar{b}$。

- 首先，假设 $k = s$，则 $a\boldsymbol{d} = e_{-1} \cdots e_{s-1}$ 并且 $\boldsymbol{e}\bar{b} = e_1 \cdots e_{s+1}$。令 $1 \leqslant i \leqslant s+1$ 是最大的使得 $e_i \neq e_{i-2}$ 的整数。因为 $a\boldsymbol{d} \neq \boldsymbol{e}\bar{b}$，所以这样的 i 一定存在。由 i 的选取可知 $e_{i-1} \cdots e_{s-1} = e_{i+1} \cdots e_{s+1}$。现在，因为 $e_s = e_{s+1} = \bar{b}$，所以可以得到 $e_{i-1} = \cdots = e_{s+1}$。特别地，$e_{i-1} = e_i$。这样一来，$a\boldsymbol{d}$ 和 $\boldsymbol{e}\bar{b}$ 的 A 类易混淆性表明 $e_{-1} \cdots e_{i-3} = e_1 \cdots e_{i-1}$。另一方面我们有 $e_{-1} = a$ 且 $e_0 = \bar{a}$，所以 $e_{-1} \cdots e_{i-1}$ 是一个交错序列。因此，对任何的 $s \geqslant 0$ 以及任何的 $1 \leqslant i \leqslant s+1$，$\boldsymbol{e}$ 和 $\boldsymbol{d}$ 有下面的几种取值：

$\boldsymbol{e}$	$\boldsymbol{d}$	i 的条件	$a = b$
$(a\bar{a})^{\frac{i-1}{2}}\bar{a}^{s-i+1}$	$(\bar{a}a)^{\frac{i-1}{2}}\bar{a}^{s-i+1}$	i 是奇数	是
$(a\bar{a})^{\frac{i-2}{2}}a^{s-i+2}$	$(\bar{a}a)^{\frac{i-2}{2}}\bar{a}a^{s-i+1}$	i 是偶数	否

  当 $k \geqslant s+1$（即 $k-1 \geqslant s$）时，因为 $e_s \cdots e_k$ 是交错序列，所以我们能推出 $\bar{e}_{k-1} = e_k = e_{k+1} = \bar{b}$ 以及 $e_s \cdots e_{k-2} = e_{s+2} \cdots e_k$（若 $k \geqslant s+2$）。
- 其次，假设 $k \geqslant s+2$，则 $a\boldsymbol{d} = e_{-1} \cdots e_{s-1}\bar{e}_s \cdots \bar{e}_{k-1}$ 并且 $\boldsymbol{e}\bar{b} = e_1 \cdots e_{k+1}$。下面，我们根据 s 的取值范围分成三种情况讨论。

  如果 $s = 0$，因为 $e_0 \cdots e_k$ 是一个交错序列，所以 $e_0 \neq e_1$。另一方面，$e_0 = \bar{a} \neq e_{-1} = a$，所以 $e_1 = e_{-1} = a$。这样一来，根据 $e_0 \cdots e_k$ 的交错性，我们得到（对所有的 $k \geqslant 2$）：

$\boldsymbol{e}$	$\boldsymbol{d}$	k 的条件	$a=b$
$(a\bar{a})^{\frac{k}{2}}$	$(a\bar{a})^{\frac{k}{2}}$	k 是偶数	是
$(a\bar{a})^{\frac{k-1}{2}}a$	$(a\bar{a})^{\frac{k-1}{2}}a$	k 是奇数	否

如果 $s=1$，由于 $e_1\neq e_2$，所以 $e_1\neq e_{-1}$ 并且 $e_2\neq e_0$，或者 $e_1=e_{-1}$ 并且 $e_2=e_0$。因此，对所有的 $k\geqslant 3$，我们得到（记住 $e_1\cdots e_k$ 是交错序列）：

$\boldsymbol{e}$	$\boldsymbol{d}$	k 的条件	$a=b$
$(\bar{a}a)^{\frac{k}{2}}$	$(\bar{a}a)^{\frac{k}{2}}$	k 是偶数	否
$(\bar{a}a)^{\frac{k-1}{2}}\bar{a}$	$(\bar{a}a)^{\frac{k-1}{2}}\bar{a}$	k 是奇数	是

或者

$\boldsymbol{e}$	$\boldsymbol{d}$	k 的条件	$a=b$
$(a\bar{a})^{\frac{k}{2}}$	$\bar{a}\bar{a}(a\bar{a})^{\frac{k-2}{2}}$	k 是偶数	是
$(a\bar{a})^{\frac{k-1}{2}}a$	$\bar{a}(\bar{a}a)^{\frac{k-1}{2}}$	k 是奇数	否

现在我们假设 $s\geqslant 2$，即 $s-1\geqslant 1$。如果存在 $1\leqslant j\leqslant s+1$ 使得 $e_j\neq e_{j-2}$，则令 i 是 j 的最大值。如果不存在这样的 j，则令 $i=0$。无论那种情况，i 的取值都是确定的。根据 i 的取法，可知 $e_{i-1}\cdots e_{s-1}=\overline{e_{i+1}\cdots e_{s+1}}$。此外，因为 $a\boldsymbol{d}$ 和 $\boldsymbol{e}\bar{b}$ 是 A 类易混淆的，所以 $e_{i-1}\cdots e_{s-1}=\overline{e_{i+1}\cdots e_{s+1}}$ 一定是交错序列。如前所述，当 $k\geqslant s+2$ 时，$e_s=e_{s+2}$，因此 $\bar{e}_s\neq e_{s+2}$。再根据 $a\boldsymbol{d}$ 和 $\boldsymbol{e}\bar{b}$ 的 A 类易混淆的性质，我们得到 $e_{-1}\cdots e_{i-2}=e_1\cdots e_i$。因此由于 $e_{-1}\neq e_0$，序列 $e_{-1}\cdots e_i$ 是一个交错序列。如果 $i\leqslant s-2$，由式子 $e_{i-1}\cdots e_{s-1}=\overline{e_{i+1}\cdots e_{s+1}}$ 我们可以得到 $e_{i+1}=\bar{e}_{i-1}=\bar{e}_{i+1}$，这不可能。于是 $i\in\{s-1,s,s+1\}$。如果 $i=s-1$，则 $e_{-1}\cdots e_{s-1}$ 是一个交错序列并且 $e_{s-1}=\bar{e}_{s+1}=e_s$。如果 $i=s$，则 $e_s=\bar{e}_{s-1}=e_{s+1}$，这与 $e_s\cdots e_k$ 是交错序列矛盾。如果 $i=s+1$，因为 $e_{-1}\cdots e_{s+1}$ 和 $e_s\cdots e_k$ 都是交错序列，所以 $e_{-1}\cdots e_k$ 是一个交错序列。因此对所有的 $s\geqslant 2$ 和所有的 $k\geqslant s+2$，我们得到表3.3中所列的 $\boldsymbol{e}$ 和 $\boldsymbol{d}$ 的值。这里前四行对应着 $i=s-1$ 的情形，而后面的四行对应着 $i=s+1$ 的情形。

- 最后，假设 $k=s+1$，则 $a\boldsymbol{d}=e_{-1}\cdots e_{s-1}\bar{e}_s$ 并且 $\boldsymbol{e}\bar{b}=e_1\cdots e_{s+2}$。在这种情况下，因为 $e_s\neq e_{s+1}$ 以及 $e_{s+1}=\bar{b}=e_{s+2}$，所以 $\bar{e}_s=e_{s+2}$。这时候，仅仅依靠式子 (3.15) 的前两个条件不足以让我们确定 $\boldsymbol{d}$ 和 $\boldsymbol{e}$ 的值。我们需要利用式子 (3.15) 的第四个等式。因为 $\bar{e}_s=e_{s+1}=e_k=\bar{b}$，所以 $a\boldsymbol{d}b\in I_2(\boldsymbol{e})$ 当且仅当 $e_{-1}\cdots e_{s-1}\in I_1(e_1\cdots e_s)$。如果 $s=0$，则 $e_1=d_1=a=\bar{b}$。但是此时一定成立 $a\boldsymbol{d}=\boldsymbol{e}\bar{b}$，矛盾。因此，$s\geqslant 1$ 一定成立。
  - 如果 $e_i=e_{i-1}$ 对所有的 $1\leqslant i\leqslant s$ 都成立，则 $e_0=\cdots=e_s$。这种情况下我们只能取 $s=1$，因此 $\boldsymbol{e}=\boldsymbol{d}=\bar{a}a$ 且 $a=\bar{b}$。事实上，若 $s\geqslant 2$，则 e_0 一定等于 e_2。另一方面，因为 $e_{s+1}\neq e_s$ 并且 $e_{s-1}=e_s$，所以 $e_{s+1}\neq e_{s-1}$。这样的话，$a\boldsymbol{d}$ 和 $\boldsymbol{e}\bar{b}$ 的易混淆性表明 $e_1=e_{-1}\neq e_0$，矛盾。

表 3.3　情形（i）中对应的 $s \geqslant 2, k \geqslant s+2$ 的情形

$\boldsymbol{e}$	$\boldsymbol{d}$	s 和 k 的条件	$a=b$
$(a\bar{a})^{\frac{s-1}{2}}(\bar{a}a)^{\frac{k-s+1}{2}}$	$(\bar{a}a)^{\frac{k}{2}}$	s 是奇数 k 是偶数	否
$(a\bar{a})^{\frac{s-1}{2}}\bar{a}(a\bar{a})^{\frac{k-s}{2}}$	$(\bar{a}a)^{\frac{k-1}{2}}\bar{a}$	s 是奇数 k 是奇数	是
$(a\bar{a})^{\frac{s-2}{2}}a(a\bar{a})^{\frac{k-s+1}{2}}$	$(\bar{a}a)^{\frac{k-1}{2}}\bar{a}$	s 是偶数 k 是奇数	是
$(a\bar{a})^{\frac{s-2}{2}}a(a\bar{a})^{\frac{k-s}{2}}a$	$(\bar{a}a)^{\frac{k}{2}}$	s 是偶数 k 是偶数	否
$(a\bar{a})^{\frac{k}{2}}$	$(\bar{a}a)^{\frac{s-1}{2}}\bar{a}(\bar{a}a)^{\frac{k-s-1}{2}}\bar{a}$	s 是奇数 k 是偶数	是
$(a\bar{a})^{\frac{k}{2}}$	$(\bar{a}a)^{\frac{s}{2}}(a\bar{a})^{\frac{k-s}{2}}$	s 是偶数 k 是偶数	是
$(a\bar{a})^{\frac{k-1}{2}}a$	$(\bar{a}a)^{\frac{s-1}{2}}\bar{a}(\bar{a}a)^{\frac{k-s}{2}}$	s 是奇数 k 是奇数	否
$(a\bar{a})^{\frac{k-1}{2}}a$	$(\bar{a}a)^{\frac{s}{2}}a(\bar{a}a)^{\frac{k-s-1}{2}}$	s 是偶数 k 是奇数	否

– 如果存在 $1 \leqslant j \leqslant s$ 使得 $e_j \neq e_{j-1}$，令 i 表示其中最大的 j。此时 $a\boldsymbol{d}b \in I_2(\boldsymbol{e})$ 当且仅当 $e_{-1}\cdots e_{i-2} = e_1 \cdots e_i$。因此 $e_{-1}\cdots e_i$ 是交错序列，并且 $e_i = \cdots = e_s$。所以对所有的 $s \geqslant 1$ 以及所有的 $1 \leqslant i \leqslant s$，我们得到

$\boldsymbol{e}$	$\boldsymbol{d}$	i 的条件	$a=b$
$(a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}a$	$(\bar{a}a)^{\frac{i}{2}}\bar{a}^{s-i}a$	i 是偶数	否
$(a\bar{a})^{\frac{i-1}{2}}a^{s-i+1}\bar{a}$	$(\bar{a}a)^{\frac{i-1}{2}}\bar{a}a^{s-i}\bar{a}$	i 是奇数	是

无论 i 是奇数还是偶数，为了保证 $a\boldsymbol{d}$ 和 $\boldsymbol{e}\bar{b}$ 是 A 类易混淆的，必须取 $i = s-1$。很显然，此时 $s \geqslant 2$。因此 $\boldsymbol{e}$ 和 $\boldsymbol{d}$ 的取值如下（其中 $s \geqslant 2$）：

$\boldsymbol{e}$	$\boldsymbol{d}$	s 的条件	$a=b$
$(a\bar{a})^{\frac{s-1}{2}}\bar{a}a$	$(\bar{a}a)^{\frac{s-1}{2}}\bar{a}a$	s 是奇数	否
$(a\bar{a})^{\frac{s-2}{2}}a^2\bar{a}$	$(\bar{a}a)^{\frac{s-2}{2}}\bar{a}a\bar{a}$	s 是偶数	是

现在我们将上述讨论的结果总结在表3.4中，这里 i, j 是新的参数。容易验证当 $\boldsymbol{d}$ 和 $\boldsymbol{e}$ 取表3.4中所列的值的时候，式子 (3.15) 中的所有条件均得到满足。

情形 (ii) $s \geqslant 0, t \geqslant 1$

这种情况下，由式子 (3.17) 可知 $\boldsymbol{d} = e_0 \cdots e_{s-1}\bar{e}_s \cdots \bar{e}_{k-t}e_{k-t+1}\cdots e_{k-1}$ 以及 $e_k =$

表 3.4　定理3.21证明中的情形（i）

	$\boldsymbol{e}$	$\boldsymbol{d}$	i,j 的条件
$a=b$	$(a\bar{a})^i\bar{a}^j$	$(\bar{a}a)^i\bar{a}^j$	$i,j\geqslant 0$
	$(a\bar{a})^i\bar{a}(a\bar{a})^j$	$(\bar{a}a)^{i+j}\bar{a}$	$i\geqslant 0, j\geqslant 1$
	$(a\bar{a})^i a(a\bar{a})^j$	$(\bar{a}a)^{i+j}\bar{a}$	$i\geqslant 0, j\geqslant 1$
	$(a\bar{a})^{i+j+1}$	$(\bar{a}a)^i\bar{a}(\bar{a}a)^j\bar{a}$	$i\geqslant 0, j\geqslant 1$
	$(a\bar{a})^{i+j}$	$(\bar{a}a)^i(a\bar{a})^j$	$i\geqslant 0, j\geqslant 1$
$a=\bar{b}$	$(a\bar{a})^i a^{j+1}$	$(\bar{a}a)^i\bar{a}a^j$	$i,j\geqslant 0$
	$(a\bar{a})^i(\bar{a}a)^j$	$(\bar{a}a)^{i+j}$	$i\geqslant 0, j\geqslant 1$
	$(a\bar{a})^i a(a\bar{a})^j a$	$(\bar{a}a)^{i+j+1}$	$i\geqslant 0, j\geqslant 1$
	$(a\bar{a})^{i+j}a$	$(\bar{a}a)^i\bar{a}(\bar{a}a)^j$	$i\geqslant 0, j\geqslant 1$
	$(a\bar{a})^{i+j}a$	$(\bar{a}a)^i a(\bar{a}a)^j$	$i\geqslant 0, j\geqslant 1$

$d_{k+1}=b$。此外，考虑到序列 $e_s\cdots e_{k-t}$ 的交错性质，我们很容易看出 $a\boldsymbol{d}b\in I_2(\boldsymbol{e})$ 当且仅当 $e_{-1}\cdots e_{s-1}\in I_1(e_1\cdots e_s)$，以及 $\bar{a}\boldsymbol{e}\bar{b}\in I_2(\boldsymbol{d})$ 当且仅当 $e_{k-t+1}\cdots e_{k+1}\in I_1(\bar{e}_{k-t}e_{k-t+1}\cdots e_{k-1})$。

- 我们首先确定 $\boldsymbol{e}$ 的前 $k-t$ 项。为了达到这个目的，我们只需要条件 $a\boldsymbol{d}b\in I_2(\boldsymbol{e})$。

  如果 $s=0$，或者 $s\geqslant 1$ 且 $e_i=e_{i-1}$ 对所有的 $1\leqslant i\leqslant s$ 都成立，则 $e_0=\cdots=e_s$。此时序列 $e_s\cdots e_{k-t}$ 的交错性质表明

$$e_1\cdots e_{k-t}=\begin{cases}\bar{a}^s(a\bar{a})^{\frac{k-t-s}{2}}, & \text{若}k\equiv s+t \pmod 2, \quad (3.19)\\ \bar{a}^s(a\bar{a})^{\frac{k-t-s-1}{2}}a, & \text{若}k\equiv s+t+1 \pmod 2. \quad (3.20)\end{cases}$$

  对所有的 $s\geqslant 0$ 和所有的 $k\geqslant s+t$ 都成立。

  如果 $s\geqslant 1$ 且存在 $1\leqslant j\leqslant s$ 使得 $e_j\neq e_{j-1}$，令 i 是 j 的最大值。此时 $e_i=\cdots=e_s$。于是条件 $a\boldsymbol{d}b\in I_2(\boldsymbol{e})$ 等价于 $e_{-1}\cdots e_{i-1}\in I_1(e_1\cdots e_i)$，这意味着 $e_{-1}\cdots e_i$ 是交错序列。再一次地，根据序列 $e_s\cdots e_{k-t}$ 的交错性质，我们得到

$$e_1\cdots e_{k-t}=\begin{cases}(a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s}{2}}, & i,k-s-t\text{ 都是偶数}, \quad (3.21)\\ (a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s-1}{2}}a, & i\text{ 是偶数}, k-s-t\text{ 是奇数}, \quad (3.22)\\ (a\bar{a})^{\frac{i-1}{2}}a^{s+1-i}(\bar{a}a)^{\frac{k-t-s}{2}}, & i\text{ 是奇数}, k-s-t\text{ 是偶数}, \quad (3.23)\\ (a\bar{a})^{\frac{i-1}{2}}a^{s+1-i}(\bar{a}a)^{\frac{k-t-s-1}{2}}\bar{a}, & i\text{ 是奇数}, k-s-t\text{ 是奇数}. \quad (3.24)\end{cases}$$

  对所有的 $s\geqslant 1$，$1\leqslant i\leqslant s$ 以及 $k\geqslant s+t$ 都成立。

- 现在我们需要确定 $\boldsymbol{e}$ 的最后 t 项，此时我们只需要条件 $\bar{a}\boldsymbol{e}\bar{b}\in I_2(\boldsymbol{d})$。

如果 $e_{k-t} = e_{k-t+1}$，则

$$e_{k-t+1} \cdots e_k \text{是交错序列.} \tag{3.25}$$

现在设 $e_{k-t+1} = \bar{e}_{k-t}$。如果 $t = 1$，或者 $t \geqslant 2$ 但是 $e_j = e_{j-1}$ 对所有的 $k-t+2 \leqslant j \leqslant k$ 都成立，则条件 $\bar{a}\boldsymbol{e}\bar{b} \in \boldsymbol{I}_2(\boldsymbol{d})$ 自然成立。此时，

$$e_{k-t+1} = \cdots = e_k \tag{3.26}$$

如果 $e_{k-t+1} = \bar{e}_{k-t}$，$t \geqslant 2$，并且且存在 $k-t+2 \leqslant j_1 \leqslant k$ 使得 $e_{j_1} \neq e_{j_1-1}$，令 j 是 j_1 的最小值。此时 $\bar{a}\boldsymbol{e}\bar{b} \in \boldsymbol{I}_2(\boldsymbol{d})$ 当且仅当 $e_j \cdots e_{k+1} \in \boldsymbol{I}_1(e_{j-1} \cdots e_{k-1})$，并且

$$\begin{aligned} e_{k-t+1} &= \cdots = e_{j-1}, \\ e_{j-1} \cdots e_{k-1} &= e_{j+1} \cdots e_{k+1}. \end{aligned} \tag{3.27}$$

因为 $e_j \neq e_{j-1}$，所以式子（3.27）中的第二个等式表明 $e_{j-1} \cdots e_k$ 是一个交错序列。

注意到式子 (3.19)–(3.24) 唯一确定 $\boldsymbol{e}$ 的前 $k-t$ 项，而式子 (3.25)–(3.27) 唯一确定了 $\boldsymbol{e}$ 的最后 t 项。所以结合式子 (3.19)–(3.27)，我们能够唯一确定出 $\boldsymbol{e}$ 和 $\boldsymbol{d}$ 的值。比如，如果 $k-s-t$ 和 t 都是偶数，则根据式子 (3.19) 和式子 (3.25) 我们得到 $\boldsymbol{e} = \bar{a}^s(a\bar{a})^{\frac{k-t-s}{2}}(\bar{a}a)^{\frac{t}{2}}$ 以及 $\boldsymbol{d} = \bar{a}^s(a\bar{a})^{\frac{k-s}{2}}$。运用类似的思路，对于所有的 $s \geqslant 0$，$t \geqslant 1$，$k \geqslant s+t$，$1 \leqslant i \leqslant s$ 和 $k-t+2 \leqslant j \leqslant k$，我们得到了 $\boldsymbol{d}$ 和 $\boldsymbol{e}$ 所有可能的取值，并将它们列在了表B.1中（这个表格比较长，我们将其放在附录B中）。表B.1的最后一列指出了我们应用了式子 (3.19)–(3.27) 中的哪些来确定 $\boldsymbol{e}$ 的值。

注意，到目前为止我们只是利用了式子 (3.15) 中的第一个和最后两个条件。然而仅仅凭借这三个条件，我们并不能保证式子 (3.15) 中的第二个条件成立。为了保证 $a\boldsymbol{d}$ 和 $\boldsymbol{e}\bar{b}$ 是 A 类易混淆的，我们需要对参数 i, j, k, s, t 加上额外的约束条件。我们将这些额外的约束条件列在下面，它们的正确性均可直接地被验证。

- 在第 1，2 行，当 $s \geqslant 2$ 时，取 $k = s+t$；当 $s = 0, 1$ 时，取 $k \geqslant s+t$。
- 在第 3，4 行，我们只能够取 $s = 0$ 和 1。当 $s = 0$ 时，取 $k > s+t+1$；当 $s = 1$ 时，取 $k \geqslant s+t+1$。
- 在第 5 行，我们只能够取 $s = 0, 1$。当 $s = 0$ 时，取 $k = s+t$ 和 $t \geqslant 1$，或者取 $k > s+t$ 和 $t = 1$；当 $s = 1$ 时，我们只能够取 $t = 1$。
- 在第 6 行，我们只能够取 $s = 0, 1$ 和 $t = 1$。
- 在第 7, 8 行, 我们只能取 $s = 0, 1$。当 $s = 0$ 时, 取 $k = s+t$ 和 $k-t+2 \leqslant j \leqslant k$, 或者取 $k > s+t$ 和 $j = k-t+2$；当 $s = 1$ 时，取 $j = k-t+2$。
- 在第 9，10 行，我们只能够取 $s = 0, 1$ 以及 $j = k-t+2$。
- 在第 11，12，21，22 行，当 $s-i \geqslant 2$ 时，取 $k = s+t$；当 $s-i = 0, 1$ 时，取 $k \geqslant s+t$。

- 在第 13，23 行，我们只能取 $s-i=0,1$。当 $s-i=0$ 时，取 $k=s+t$ 和 $t\geqslant 1$，或者取 $k>s+t$ 和 $t=1$；当 $s-i=1$ 时，我们只能取 $t=1$。
- 在第 14，15，24，25 行，$s-i$ 只能取 0 和 1。当 $s-i=0$ 时，取 $k=s+t$ 和 $k-t+2\leqslant j\leqslant k$，或者取 $k>s+t$ 和 $j=k-t+2$；当 $s-i=1$ 时，我们只能够取 $j=k-t+2$。
- 在第 18，28 行，我们只能够取 $s-i=0,1$ 和 $t=1$。
- 在第 19，20，29，30 行，我们只能够取 $s-i=0,1$ 和 $j=k-t+2$。
- 在第 16, 17, 26, 27, 我们只能够取 $s-i=0,1$。当 $s-i=0$ 时, 取 $k>s+t+1$；当 $s-i=1$ 时，取 $k\geqslant s+t+1$。

有了这些额外的约束条件以后，很容易验证表B.1的任一行都满足式子 (3.15) 中所有的条件。

现在，结合表3.4和表B.1，我们就能够得到定理3.21中的结论。在定理3.21中，i,j 是新的参数，而不是证明中出现的。我们有必要指出表3.4的第三行和第四行分别是表A.1的第 24 和 23 行的特殊情形，而表3.4的第八行和第九行分别是表A.2的第 18 行和第 17 行的特殊情形。

至此，我们完成了定理3.21的证明。 ∎

接下来我们将给出 $(n,6;B_2^{I(2)})$-重构码的构造。在这之前，我们先给出一个作用在所有有限长的序列上的函数的定义，这个函数非常有用。对任何的序列 $\boldsymbol{x}\in\Sigma_2^*$，令 $f(\boldsymbol{x})\triangleq\sum\limits_{i=1}^{L}i^2x_i$，其中 L 指的是 $\boldsymbol{x}$ 的长度。如果 $L=0$，则我们规定 $f(\boldsymbol{x})\triangleq 0$。设 $s=|\boldsymbol{u}|$，$t=|\boldsymbol{w}|$。下面这个简单的等式将会帮我们节省很多计算。

$$f(\boldsymbol{u}a\boldsymbol{d}b\boldsymbol{w})-f(\boldsymbol{u}\bar{a}e\bar{b}\boldsymbol{w})=\sum_{i=0}^{L+1}(i+s+1)^2(d_i-e_i),\tag{3.28}$$

其中 L 是 $\boldsymbol{d}$ 的长度；此外，令 $d_0=a$，$d_{L+1}=b$，$e_0=\bar{a}$，$d_{L+1}=\bar{b}$。作为文献 [74] 中命题 1 的推论，下面的这个引理给出了一个单个插入纠错码，即一个 $(n,1;B_2^{I(1)})$-重构码。虽然这个码不是最优的，但它在我们的 $(n,6;B_2^{I(2)})$-重构码的构造中起到了至关重要的作用，而 VT 码则起不到类似的作用。

引理 3.22　对任何大于等于 2 的整数 n 以及任何的 $d\in\mathbb{Z}_{n^2+1}$，码 $\left\{\boldsymbol{x}\in\Sigma_2^n\mid f(\boldsymbol{x})\equiv d\pmod{n^2+1}\right\}$ 是一个单个插入纠错码。

证明　在 [74] 的命题 1 中取 $\boldsymbol{v}=(1,2^2,\cdots,n^2)$，则可得到引理的结论。 ∎

定理 3.23　设 $n,P\geqslant 2$ 是整数,并且 P 是偶数。对任何的 $c\in\mathbb{Z}_{1+2P}$, $d\in\mathbb{Z}_{n^2+1}$ 以及 $e\in\mathbb{Z}_4$，我们将 $E(n;c,d,e)$ 定义为所有满足下面条件的序列 $\boldsymbol{x}=x_1\cdots x_n\in\Sigma_2^n$ 构成的集合：

- $\mathrm{Inv}\,(\boldsymbol{x})\equiv c\pmod{1+2P}$.

- $\sum_{i=1}^{n} i^2 x_i \equiv d \pmod{n^2+1}$.
- $\sum_{i=1}^{n} x_i \equiv e \pmod 4$.
- $\boldsymbol{x} \in R(n, 2, \frac{P}{2})$.

则 $E(n;c,d,e)$ 是一个 $(n, 6; B_2^{I(2)})$-重构码。进一步地，若 $\frac{P}{2} = \lceil \log_2(n) \rceil + 3$，则存在 c,d,e，使得 $E(n;c,d,e)$ 的冗余至多为 $3 + \log_2(n^2+1) + \log_2(2P+1) = 2\log_2(n) + \log_2\log_2(n) + O(1)$。

证明　第二个条件和引理3.22表明 $E(n;c,d,e)$ 是一个 $(n, 1; B^{I_1(1)})$-重构码。因此对任何两个不同的序列 $\boldsymbol{x}, \boldsymbol{y} \in C(n;c,d,e)$，我们有 $\left|I_1(\boldsymbol{x}) \cap I_1(\boldsymbol{y})\right| = 0$，即 $\left|I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})\right| \leqslant 6$。假设 $E(n;c,d,e)$ 中存在两个不同的序列 $\boldsymbol{x}, \boldsymbol{y}$ 使得 $\left|I_2(\boldsymbol{x}) \cap I_2(\boldsymbol{y})\right| = 6$, 则不失一般性, 我们可设存在 $\boldsymbol{u} \in \Sigma_2^s, \boldsymbol{w} \in \Sigma_2^t$ 以及 $\boldsymbol{d}, \boldsymbol{e} \in \Sigma_2^L$，使得

$$\begin{cases} \boldsymbol{x} = \boldsymbol{u}a\boldsymbol{d}b\boldsymbol{w}, \\ \boldsymbol{y} = \boldsymbol{u}\bar{a}\boldsymbol{e}\bar{b}\boldsymbol{w}, \end{cases}$$

其中 $s+t+L+2=n$，且 $\boldsymbol{d}, \boldsymbol{e}$ 由定理3.21给出。由观察可知

$$wt_H(\boldsymbol{x}) - wt_H(\boldsymbol{y}) = \begin{cases} wt_H(\boldsymbol{d}) - wt_H(\boldsymbol{e}) + 2(a-\bar{a}), & \text{若} a = b, \\ wt_H(\boldsymbol{d}) - wt_H(\boldsymbol{e}) & \text{若} a = \bar{b}. \end{cases}$$

因为 $wt_H(\boldsymbol{d}) = N_{\boldsymbol{d}}(a)$（如果 $a=1$）或 $wt_H(\boldsymbol{d}) = |\boldsymbol{d}| - N_{\boldsymbol{d}}(a)$（如果 $a=0$），所以第三个条件表明

$$\begin{cases} N_{\boldsymbol{d}}(a) - N_{\boldsymbol{e}}(a) \equiv 2 \pmod 4, & \text{若} a = b, \\ N_{\boldsymbol{d}}(a) - N_{\boldsymbol{e}}(a) \equiv 0 \pmod 4 & \text{若} a = \bar{b}. \end{cases} \tag{3.29}$$

当式子 (3.29) 成立的时候，容易验证 $\mathrm{Inv}(\boldsymbol{x}) - \mathrm{Inv}(\boldsymbol{y}) = \mathrm{Inv}(a\boldsymbol{d}b) - \mathrm{Inv}\left(\bar{a}\boldsymbol{e}\bar{b}\right)$。

因此，当 $a=b$ 时，我们只需要考虑下面六种情形:

表A.1 中对应的行	$\boldsymbol{e},\boldsymbol{d}$	$\lvert\mathrm{Inv}(\boldsymbol{x})-\mathrm{Inv}(\boldsymbol{y})\rvert$
17	$\boldsymbol{e}=(a\bar{a})^{i+j}a(a\bar{a})^{l}a$ $\boldsymbol{d}=(\bar{a}a)^{i}\bar{a}(\bar{a}a)^{j+l}\bar{a}$	$\lvert i-l\rvert$
18	$\boldsymbol{e}=(a\bar{a})^{i}a^{j}(\bar{a}a)^{l}$ $\boldsymbol{d}=(\bar{a}a)^{i+1}a^{j-4}(a\bar{a})^{l+1}$	$\lvert i-l\rvert$
19	$\boldsymbol{e}=(a\bar{a})^{i}a(a\bar{a})^{j}a(a\bar{a})^{l}a$ $\boldsymbol{d}=(\bar{a}a)^{i+j+l+1}\bar{a}$	$\lvert i-l\rvert$
20	$\boldsymbol{e}=(a\bar{a})^{i+j+l+1}a$ $\boldsymbol{d}=(\bar{a}a)^{i}\bar{a}(\bar{a}a)^{j}\bar{a}(\bar{a}a)^{l}\bar{a}$	$\lvert i-l\rvert$
21	$\boldsymbol{e}=(a\bar{a})^{i}a(a\bar{a})^{j+l}a$ $\boldsymbol{d}=(\bar{a}a)^{i}\bar{a}(a\bar{a})^{j}(\bar{a}a)^{l}\bar{a}$	$\lvert i-l\rvert$
22	$\boldsymbol{e}=(a\bar{a})^{i+1}\bar{a}^{j}(a\bar{a})^{l}a$ $\boldsymbol{d}=(\bar{a}a)^{i}\bar{a}^{j+2}(\bar{a}a)^{l}\bar{a}$	$\lvert i-l\rvert$

令 $\Delta=|f(\boldsymbol{x})-f(\boldsymbol{y})|$。如果 $i=l$，则根据式子（3.28），我们可算出这六种情形对应的 Δ 的值分别为：$2(2i+j)(i+1)$，$4(i+j+1)(i+1)$，$2(2i+2j+3)(i+1)$，$2(2i+2j+3)(i+1)$，$4(i+j+2)(i+1)$,$2(2i+j+3)(i+1)$。因为 $\boldsymbol{x}$ 的长度 n 等于 $s+t+L+2$，所以 $n^2+1>\Delta>0$ 总是成立的。但这与第二个条件矛盾，因此，$i\neq l$ 一定成立。这样一来，$0<|\mathrm{Inv}(\boldsymbol{x})-\mathrm{Inv}(\boldsymbol{y})|\leqslant i+l$ 在上述六种条件下都成立。

当 $a=\bar{b}$ 时, 我们只需要考虑表3.5中所列的十二中情形。根据定理3.23的第一个和第三个条件, 再经过和定理3.16以及定理3.17的证明中相同的过程, 我们可以证明上述十八种情形都不可能发生。因此，$E(n;c,d,e)$ 的确是一个 $(n,6;B_2^{I(2)})$-重构码。

证明完成。 ∎

3.5　小节

本章中，我们研究了 2-插入信道重构码。设 N 是信道的数目，n 是序列的长度，则非平凡的情形是 $1\leqslant N\leqslant 6$ 和 $N\in\{n+4,n+5\}$。当两个不同序列的 2-插入球相交大小分别是 $6,n+4$ 和 $n+5$ 时，我们完全确定了它们的结构。然后，我们给出了相应的码的构造。特别地，当 $N=n+4$ 和 $n+5$ 时，我们构造的码有渐近最优的冗余；当 $N=6$ 时，我们不清楚码的冗余是否最优。

对于未来的研究，我们提出下面几个问题。

(1) 在定理3.23，我们构造了 $(n,6;B_2^{I(2)})$-重构码，其冗余的主项和第二项分别是

$2\log_2(n)$ 和 $\log_2\log_2(n)$。它们是不是最优的？若不是，我们能否构造出冗余更小的码？

(2) 当 $1 \leqslant N \leqslant 5$ 时，本章的方法不适用。因此我们需要新的方法来研究 $1 \leqslant N \leqslant 5$ 的情形。

表 3.5　定理3.23证明中 $a = \bar{b}$ 的情形

表A.2 中对应的行	$\boldsymbol{e}, \boldsymbol{d}$	$\lvert\mathrm{Inv}(\boldsymbol{x}) - \mathrm{Inv}(\boldsymbol{y})\rvert$
2	$\boldsymbol{e} = (a\bar{a})^i(\bar{a}a)^j$ $\boldsymbol{d} = (\bar{a}a)^{i+j}$	$i + 2j + 1$
3	$\boldsymbol{e} = (a\bar{a})^{i+j}a$ $\boldsymbol{d} = (a\bar{a})^i a(a\bar{a})^j$	$2i + 3j + 2$
4	$\boldsymbol{e} = (a\bar{a})^{i+j}$ $\boldsymbol{d} = (a\bar{a})^i(\bar{a}a)^j$	$2i + j + 1$
5	$\boldsymbol{e} = (\bar{a}a)^{i+j}\bar{a}$ $\boldsymbol{d} = (\bar{a}a)^i\bar{a}(\bar{a}a)^j$	$2i + j + 2$
12	$\boldsymbol{e} = (a\bar{a})^{i+j}a(a\bar{a})^l$ $\boldsymbol{d} = (\bar{a}a)^i(a\bar{a})^{j+l}a$	$i + 2j + l + 2$
13	$\boldsymbol{e} = (a\bar{a})^i(\bar{a}a)^j(a\bar{a})^l$ $\boldsymbol{d} = (\bar{a}a)^{i+j+l}$	$i + 2j + l + 1$
14	$\boldsymbol{e} = (a\bar{a})^{i+j+l}$ $\boldsymbol{d} = (\bar{a}a)^i(a\bar{a})^j(\bar{a}a)^l$	$i + 2j + l + 1$
15	$\boldsymbol{e} = (a\bar{a})^i(\bar{a}a)^{j+l}\bar{a}$ $\boldsymbol{d} = (\bar{a}a)^{i+j}\bar{a}(\bar{a}a)^j$	$i + 2j + l + 2$
22	$\boldsymbol{e} = (a\bar{a})^{i+j}(\bar{a}a)^l\bar{a}$ $\boldsymbol{d} = (\bar{a}a)^i\bar{a}(\bar{a}a)^{j+l}$	$i + l + 2$
23	$\boldsymbol{e} = (a\bar{a})^i a(a\bar{a})^j(\bar{a}a)^l\bar{a}$ $\boldsymbol{d} = (\bar{a}a)^{i+j+l+1}$	$i + l + 2$
24	$\boldsymbol{e} = (a\bar{a})^{i+j+l+1}$ $\boldsymbol{d} = (\bar{a}a)^i\bar{a}(\bar{a}a)^j(a\bar{a})^l a$	$i + l + 2$
25	$\boldsymbol{e} = (a\bar{a})^i a(a\bar{a})^{j+l+1}$ $\boldsymbol{d} = (\bar{a}a)^{i+j+1}(a\bar{a})^l a$	$i + l + 2$

第 4 章　其 他 工 作

本章补充了本人在攻读博士学位期间的其他研究工作。这里我们只对这些工作做简要介绍而不展开论述。

4.1　自对偶极大距离可分码

极大距离可分码是编码领域里面一个非常重要的码类，因为在给定码长和码的维数时，其具有最大的纠错能力。极大距离可分码在卫星通讯、量子码的构造、分布式存储系统等实际场景中有着广泛的应用。此外极大距离可分码与很多其他的领域，比如密码学中的理想门限方案（ideal threshold schemes）、组合学中的正交阵列，都有密切联系。自正交码本身具有良好的代数结构以及在构造量子码上面的应用，而一直受到研究人员的关注。极大距离可分自正交码因为同时具有极大距离可分和自正交的性质，近些年吸引了很多人的研究兴趣[79-82]。作为一类特殊的极大距离可分自正交码，极大距离可分自对偶码本身也得到了广泛的研究[83-89]。人们关心当给定域的大小 q 的时候，极大距离可分自对偶码的长度 n 能取到的值有哪些。自从 2017 年金玲飞和邢超平[88] 第一次使用广义 Reed-Solomon 码构造极大距离可分码后，这个问题的研究就得到飞速发展。设 $q = r^2$，其中 r 是奇数幂，则我们对此问题的主要贡献为：

- 对任意的 $2r \leqslant n \leqslant 3r - 3$ 且 n 是偶数，域 $\mathbb{F}_q$ 上均存在长度为 n 的极大距离可分自对偶码。此前被完整覆盖的区间只有 $[2, 2r]$。
- 对任意的 $3r - 1 \leqslant n \leqslant 4r$ 且 n 模 4 余 2，域 $\mathbb{F}_q$ 上均存在长度为 n 的极大距离可分自对偶码。

4.2　纠错码上的码字重构问题

码字重构问题有几个要素，一是传输的码字或者序列集合 V，另一个是信道的错误集合 H，即可以发生什么样的错误。给定 V 和 H，码字重构问题可以看成是以 V 中任意两个序列为中心的等半径球的交的大小的确定。记 N 是这些相交中最大的值，那么 $N + 1$ 个信道或失真信息就可以保证准确地恢复出传输的码字。

从已有的成功的 DNA 存储实验来看，在存储技术中加入纠错机制可以显著降低信息的读取错误率。所研究当 V 是某类纠错码时的码字重构问题是很自然并有意义的。由于重构问题要和 V 的具体结构有关，但有些纠错码的构造是很稀少的。因此研究这类问题时，我们考虑任意两个序列满足一定距离时的球相交

大小，这个值可以作为相应纠错码的码字重构参数 N 的上界。目前已有学者研究了当 V 是纠删码，H 是插入错误或删除错误的码字重构问题。当 H 为删除错误时，现有的工作只考虑了两个序列之间的 Levenshtein 距离至少为 2 时的球相交问题[28]。因此我们考虑 Levenshtein 距离至少为 t（≥ 3）时的球相交问题。

这部分研究正在进行当中。

4.3　多重集码

2018 年，Mladen 和 Vincent 在研究传输序列服从随机排列的通信信道和某些 DNA 存储系统的时候，考虑了以下问题模型：信息以给定的有限字母表上的多重集的形式被存储或传输[90]。在文献 [90] 中，作者把问题转换成了度量空间 $(\mathbb{Z}^m, d_a)$ 中码的构造问题，其中 d_a 是一个度量。设 $C \subseteq \mathbb{Z}^m$ 是一个码。如果以 C 中的码字为中心的半径等于 r 的球两两不交，并且所有的球恰好填充整个空间 $\mathbb{Z}^m$，则我们称 C 是一个 r-完美码。Mladen 和 Vincent 证明了当 $m \in \{1, 2\}$, r 任意，或者 $m \geqslant 3$ 且 $r = 1$ 的时候，r-完美码是存在的。此外他们还证明了当 $m \geqslant 3$ 且 r 充分大时，r-完美码是不存在的。

我们猜想当 $m \geqslant 3$ 且 $r \geqslant 2$ 的时候，r-完美码都是不存在的，并且考虑了 $r = 2$ 并且码是线性的情形。利用群环的知识，我们将线性 2-完美码的存在性问题转换成了群环上面的某个方程成立与否的问题，并进一步将这个问题转换成了整系数方程组非负整数解的存在性问题。借助计算机编程，我们得到以下初步结论：当 $16 \leqslant m \leqslant 2000$ 且 $m \equiv 1 \pmod 5$，或者 $13 \leqslant m \leqslant 2000$ 且 $m \equiv 3 \pmod 5$ 的时候，线性 2-完美码是不存在的。

这个问题目前还在研究当中。

参 考 文 献

[1] The Digitization of the World from Edge to Core[C]//IDC Report. 2018.

[2] Church G M, Gao Y, Kosuri S. Next-Generation Digital Information Storage in DNA[J]. Science, 2012, 337(6102): 1628-1628.

[3] Goldman N, Bertone P, Chen S, et al. Towards Practical, High-capacity, Low-Maintenance Information Storage in Synthesized DNA[J]. Nature, 2013, 494(7435): 77-80.

[4] Bornholt J, Lopez R, Carmean D M, et al. A DNA-Based Archival Storage System[C]// Proceedings of the Twenty-First International Conference on Architectural Support for Programming Languages and Operating Systems. 2016: 637-649.

[5] Kiah H M, Puleo G J, Milenkovic O. Codes for DNA Sequence Profiles[J]. IEEE Transactions on Information Theory, 2016, 62(6): 3125-3146.

[6] Jain S, Farnoud Hassanzadeh F, Schwartz M, et al. Duplication-Correcting Codes for Data Storage in the DNA of Living Organisms[J]. IEEE Transactions on Information Theory, 2017, 63(8): 4996-5010.

[7] Raviv N, Schwartz M, Yaakobi E. Rank-Modulation Codes for DNA Storage with Shotgun Sequencing[J]. IEEE Transactions on Information Theory, 2018, 65(1): 50-64.

[8] Eitan B, Roy A. Binary and Multilevel Flash Cells[M]. Boston, MA: Springer US, 1999: 91-152.

[9] Chen B, Zhang X, Wang Z. Error Correction for Multi-level NAND Flash Memory Using Reed-Solomon Codes[C]//2008 IEEE Workshop on Signal Processing Systems. 2008: 94-99.

[10] Sun F, Rose K, Zhang T. On the Use of Strong BCH Codes for Improving Multilevel NAND Flash Memory Storage Capacity[C]//IEEE Workshop on Signal Processing Systems (SiPS): Design and Implementation. Citeseer, 2006: 5.

[11] Brewer J, Gill M. Nonvolatile Memory Technologies with Emphasis on Flash: a Comprehensive Guide to Understanding and Using Flash Memory Devices: volume 8[M]. John Wiley & Sons, 2008.

[12] Schwartz M. Quasi-Cross Lattice Tilings With Applications to Flash Memory[J]. IEEE Transactions on Information Theory, 2012, 58(4): 2397-2405.

[13] Levenshtein V I. Reconstruction of Objects from the Minimum Number of Distorted Patterns [J]. Dokl. Akad. Nauk, 1997, 354(5): 593-596.

[14] Levenshtein V I. Efficient Reconstruction of Sequences[J]. IEEE Transactions on Information Theory, 2001, 47(1): 2-22.

[15] Levenshtein V I. Efficient Reconstruction of Sequences from Their Subsequences or Supersequences[J]. Journal of Combinatorial Theory, Series A, 2001, 93(2): 310-332.

[16] Batu T, Kannan S, Khanna S, et al. Reconstructing Strings from Random Traces[C]//Proc. ACM-SIAM Symp. Discrete Algorithms (SODA). New Orleans, LA, USA, 2004: 910-918.

[17] Kannan S, McGregor A. More on Reconstructing Strings from Random Traces: Insertions and Deletions[C]//Proc. Int. Symp. Inf. Theory (ISIT). Adelaide, Australia, 2005: 297-301.

[18] Viswanathan K, Swaminathan R. Improved String Reconstruction Over Insertion-Deletion Channels[C]//Proc. ACM-SIAM Symp. Discrete Algorithms (SODA). San Francisco, CA, USA, 2008: 399-408.

[19] Holenstein T, Mitzenmacher M, Panigrahy R, et al. Trace reconstruction with Constant Deletion Probability and Related Results[C]//Proc. ACM-SIAM Symp. Discrete Algorithms (SODA). San Francisco, CA, USA, 2008: 389-398.

[20] Cheraghchi M, Gabrys R, Milenkovic O, et al. Coded Trace Reconstruction[J]. IEEE Transactions on Information Theory, 2020, 66(10): 6084-6103.

[21] Brakensiek J, Li R, Spang B. Coded Trace Reconstruction in a Constant Number of Traces [C]//Proc. Annu. Symp. Found. Comput. Sci. (FOCS). Durham, NC, USA, 2020: 482-493.

[22] Konstantinova E, Levenshtein V I, Siemons J. Reconstruction of Permutations Distorted by Single Transposition Errors[J]. arXiv: 0702191, 2007.

[23] Konstantinova E. On Reconstruction of Signed Permutations Distorted by Reversal Errors[J]. Discrete Mathematics, 2008, 308(5): 974-984.

[24] Konstantinova E. Reconstruction of Permutations Distorted by Reversal Errors[J]. Discrete Applied Mathematics, 2007, 155(18): 2426-2434.

[25] Levenshtein V I, Konstantinova E, Konstantinov E, et al. Reconstruction of a Graph from 2-Vicinities of Its Vertices[J]. Discrete Applied Mathematics, 2008, 156(9): 1399-1406.

[26] Levenshtein V I, Siemons J. Error Graphs and the Reconstruction of Elements in Groups[J]. Journal of Combinatorial Theory, Series A, 2009, 116(4): 795-815.

[27] Sala F, Gabrys R, Schoeny C, et al. Exact Reconstruction From Insertions in Synchronization Codes[J]. IEEE Transactions on Information Theory, 2017, 63(4): 2428-2445.

[28] Gabrys R, Yaakobi E. Sequence Reconstruction Over the Deletion Channel[J]. IEEE Transactions on Information Theory, 2018, 64(4): 2924-2931.

[29] Horovitz M, Yaakobi E. Reconstruction of Sequences Over Non-Identical Channels[J]. IEEE Transactions on Information Theory, 2019, 65(2): 1267-1286.

[30] Yaakobi E, Schwartz M, Langberg M, et al. Sequence Reconstruction for Grassmann Graphs and Permutations[C]//Proc. Int. Symp. Inf. Theory (ISIT). Istanbul, Turkey, 2013: 874-878.

[31] Gabrys R, Yaakobi E. Sequence Reconstruction Over the Deletion Channel[C]//Proc. Int. Symp. Inf. Theory (ISIT). Barcelona, Spain, 2016: 1596-1600.

[32] Mittu R, Segaria F. Common Operational Picture (COP) and Common Tactical Picture (CTP) Management via a Consistent Networked Information Stream (CNIS)[C]//Proc. Command Control Res. Technol. Symp. Monterey, CA, USA, 2000: 3-7.

[33] Yazdi S H T, Gabrys R, Milenkovic O. Portable and Error-Free DNA-Based Data Storage[J]. Sci. Rep., 2017, 7(1): 1-6.

[34] Kiah H M, Thanh Nguyen T, Yaakobi E. Coding for Sequence Reconstruction for Single Edits [C]//Proc. Int. Symp. Inf. Theory (ISIT). Los Angeles, CA, USA, 2020: 676-681.

[35] Cai K, Kiah H M, Nguyen T T, et al. Coding for Sequence Reconstruction for Single Edits [J/OL]. arXiv: 2001.01376, 2020. http://arxiv.org/abs/2001.01376.

[36] Chrisnata J, Kiah H M, Yaakobi E. Optimal Reconstruction Codes for Deletion Channels [J/OL]. arXiv: 2004.06032, 2020. https://arxiv.org/abs/2004.06032.

[37] Kløve T, Luo J, Naydenova I, et al. Some Codes Correcting Asymmetric Errors of Limited Magnitude[J]. IEEE Transactions on Information Theory, 2011, 57(11): 7459-7472.

[38] Cassuto Y, Schwartz M, Bohossian V, et al. Codes for Asymmetric Limited-Magnitude Errors With Application to Multilevel Flash Memories[J]. IEEE Transactions on Information Theory, 2010, 56(4): 1582-1595.

[39] Xie D, Luo J. Asymmetric Single Magnitude Four Error Correcting Codes[J]. IEEE Transactions on Information Theory, 2020, 66(9): 5322-5334.

[40] Hickerson D, Stein S. Abelian Groups and Packing by Semicrosses[J]. Pacific Journal of Mathematics, 1986, 122(1): 95-109.

[41] Stein S. Factoring by Subsets[J]. Pacific Journal of Mathematics, 1967, 22(3): 523-541.

[42] Stein S. Packings of $\mathbb{R}^n$ by Certain Error Spheres[J]. IEEE Transactions on Information Theory, 1984, 30(2): 356-363.

[43] Stein S, Szabó S. Carus mathematical monographs: volume 25 Algebra and Tiling: Homomorphisms in the Service of Geometry[M]. Mathematical Association of America, 1994.

[44] Szabó S. Some Problems on Splittings of Groups[J]. Aequationes Mathematicae, 1986, 30(1): 70-79.

[45] Szabó S. Some Problems on Splittings of Groups II[J]. Proceedings of the American Mathematical Society, 1987, 101(4): 585-591.

[46] Tamm U. Splittings of Cyclic Groups and Perfect Shift Codes[J]. IEEE Transactions on Information Theory, 1998, 44(5): 2003-2009.

[47] Yari S, Kløve T, Bose B. Some Codes Correcting Unbalanced Errors of Limited Magnitude for Flash Memories[J]. IEEE Transactions on Information Theory, 2013, 59(11): 7278-7287.

[48] Kløve T, Luo J, Yari S. Codes Correcting Single Errors of Limited Magnitude[J]. IEEE Transactions on Information Theory, 2012, 58(4): 2206-2219.

[49] Schwartz M. On the Non-existence of Lattice Tilings by Quasi-crosses[C]//2013 Information Theory and Applications Workshop (ITA). 2013: 1-2.

[50] Schwartz M. On the Non-existence of Lattice Tilings by Quasi-crosses[J]. European Journal of Combinatorics, 2014, 36: 130-142.

[51] Zhang T, Ge G. New Results on Codes Correcting Single Error of Limited Magnitude for Flash Memory[J]. IEEE Transactions on Information Theory, 2016, 62(8): 4494-4500.

[52] Zhang T, Zhang X, Ge G. Splitter Sets and k-Radius Sequences[J]. IEEE Transactions on Information Theory, 2017, 63(12): 7633-7645.

[53] Zhang T, Ge G. On the Nonexistence of Perfect Splitter Sets[J]. IEEE Transactions on Information Theory, 2018, 64(10): 6561-6566.

[54] Yuan P, Zhao K. On the Existence of Perfect Splitter Sets[J/OL]. Finite Fields and Their Applications, 2020, 61. DOI: https://doi.org/10.1016/j.ffa.2019.101603.

[55] Xie D, Luo J. New Results on Asymmetric Single Correcting Codes of Magnitude Four[J]. IEEE Transactions on Information Theory, 2021, 67(8): 5079-5087.

[56] Kløve T, Bose B, Elarief N. Systematic, Single Limited Magnitude Error Correcting Codes for Flash Memories[J]. IEEE Transactions on Information Theory, 2011, 57(7): 4477-4487.

[57] Szabó S, Sands A. Lecture Notes in Pure and Applied Mathematics": volume 257 Factoring Groups into Subsets[M]. Boca Raton, FL, USA: CRC Press, 2009.

[58] Munemasa A. On Perfect t-Shift Codes in Abelian Groups[J]. Des. Codes Cryptogr., 1995, 5 (3): 253-259.

[59] Ireland K, Rosen M. Graduate Texts in Mathematics: volume 84 A Classical Introduction to Modern Number Theory[M]. 2nd ed. Springer-Verlag New York, 1990.

[60] Wikipedia Contributors. Bunyakovsky Conjecture[EB/OL]. 2019. https://en.wikipedia.org/w/index.php?title=Bunyakovsky_conjecture&oldid=898182463.

[61] Godsil C, Royle G. Graduate texts in mathematics.: volume 207 Algebraic Graph Theory [M]. 1st ed. Springer-Verlag New York, 2001.

[62] Bondy A, Murty M. Graduate texts in mathematics.: volume 244 Graph Theory[M]. 1st ed. Springer-Verlag London, 2008.

[63] Imrich W. On the Connectivity of Cayley Graphs[J]. Journal of Combinatorial Theory. Series B, 1979, 26(3): 323-326.

[64] Babai L. Spectra of Cayley Graphs[J]. Journal of Combinatorial Theory. Series B, 1979, 27 (2): 180-189.

[65] Shahzamanian M, Shirmohammadi M, Davvaz B. Roughness in Cayley Graphs[J]. Information Sciences, 2010, 180(17): 3362-3372.

[66] Lovász L. Three Short Proofs in Graph Theory[J]. Journal of Combinatorial Theory, Series B, 1975, 19(3): 269-271.

[67] Woldar A J. A Reduction Theorem on Purely Singular Splittings of Cyclic Groups[J]. Proceedings of the American Mathematical Society, 1995, 123(10): 2955-2959.

[68] Levenshtein V I. Binary Codes Capable of Correcting Deletions, Insertions and Reversals[J]. Soviet Physics Doklady, 1966, 10(8): 707-710.

[69] Hirschberg D, Regnier M. Tight Bounds on the Number of String Subsequences[J]. Journal of Discrete Algorithms, 2000, 1(1): 123-132.

[70] Sloane N J A. On Single-Deletion-Correcting Codes[M]. Berlin, New York: De Gruyter, 2008: 273-292.

[71] Liron Y, Langberg M. A Characterization of the Number of Subsequences Obtained via the Deletion Channel[J]. IEEE Transactions on Information Theory, 2015, 61(5): 2300-2312.

[72] Brakensiek J, Guruswami V, Zbarsky S. Efficient Low-Redundancy Codes for Correcting Multiple Deletions[J]. IEEE Transactions on Information Theory, 2018, 64(5): 3403-3410.

[73] Gabrys R, Sala F. Codes Correcting Two Deletions[J]. IEEE Transactions on Information Theory, 2019, 65(2): 965-974.

[74] Sima J, Raviv N, Bruck J. Two Deletion Correcting Codes From Indicator Vectors[J]. IEEE Transactions on Information Theory, 2020, 66(4): 2375-2391.

[75] Sima J, Bruck J. On Optimal k-Deletion Correcting Codes[J]. IEEE Transactions on Information Theory, 2021, 67(6): 3360-3375.

[76] Guruswami V, Håstad J. Explicit Two-Deletion Codes with Redundancy Matching the Existential Bound[J/OL]. IEEE Transactions on Information Theory, 2021, Early Access. DOI: 10.1109/TIT.2021.3069446.

[77] R. R. Varshmov, G. M. Tenengolts. Codes Which Correct Single Asymmetric Errors[J]. Avtom. i Telemehk, 1965, 26(2): 288-292.

[78] Chee Y M, Kiah H M, Vardy A, et al. Coding for Racetrack Memories[J]. IEEE Transactions on Information Theory, 2018, 64(11): 7094-7112.

[79] Grassl M, Beth T, Rotteler M. On Optimal Quantum Codes[J]. International Journal of Quantum Information, 2004, 2(1): 55-64.

[80] Luo G, Cao X, Chen X. MDS Codes With Hulls of Arbitrary Dimensions and Their Quantum Error Correction[J]. IEEE Transactions on Information Theory, 2019, 65(5): 2944-2952.

[81] Fang W, Fu F W, Li L, et al. Euclidean and Hermitian Hulls of MDS Codes and Their Applications to EAQECCs[J]. IEEE Transactions on Information Theory, 2020, 66(6): 3527-3537.

[82] Fang X, Liu M, Luo J. New MDS Euclidean Self-Orthogonal Codes[J]. IEEE Transactions on Information Theory, 2021, 67(1): 130-137.

[83] Georgiou S, Koukouvinos C. MDS Self-Dual Codes over Large Prime Fields[J]. Finite Fields and Their Applications, 2002, 8(4): 455-470.

[84] Harada M, Kharaghani H. Orthogonal Designs, Self-Dual Codes, and the Leech Lattice[J]. Journal of Combinatorial Designs, 2005, 13(3): 184-194.

[85] Haeada M, Khaeaghani H. Orthogonal Designs and MDS Self-Dual Codes[J]. Australasian Journal of Combinatorics, 2006, 35: 57-67.

[86] Grassl M, Gulliver T A. On Self-Dual MDS codes[C]//2008 IEEE International Symposium on Information Theory. 2008: 1954-1957.

[87] Guenda K. New MDS Self-Dual Codes over Finite Fields[J]. Designs, Codes and Cryptography, 2012, 62(1): 31-42.

[88] Jin L, Xing C. New MDS Self-Dual Codes From Generalized Reed-Solomon Codes[J]. IEEE Transactions on Information Theory, 2017, 63(3): 1434-1438.

[89] Yan H. A Note on the Constructions of MDS Self-Dual Codes[J]. Cryptography and Communications, 2019, 11(2): 259-268.

[90] Kovačević M, Tan V Y F. Codes in the Space of Multisets—Coding for Permutation Channels with Impairments[J]. IEEE Transactions on Information Theory, 2018, 64(7): 5156-5169.

附录 A　定理3.21中的两张表格

表 A.1　定理3.21中 $a=b$ 的情形

序号	$\boldsymbol{e}$	$\boldsymbol{d}$	条件
1	$\boldsymbol{e}=(a\bar{a})^i\bar{a}^j$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}^j$	$i,j\geqslant 0$
2	$\boldsymbol{e}=(a\bar{a})^{i+j}$	$\boldsymbol{d}=(\bar{a}a)^i(a\bar{a})^j$	$i\geqslant 0, j\geqslant 1$
3	$\boldsymbol{e}=(a\bar{a})^i\bar{a}(a\bar{a})^j$	$\boldsymbol{d}=(\bar{a}a)^{i+j}\bar{a}$	$i\geqslant 0, j\geqslant 1$
4	$\boldsymbol{e}=a^i(\bar{a}a)^j$	$\boldsymbol{d}=a^i(a\bar{a})^j$	$i\geqslant 1, j\geqslant 0$
5	$\boldsymbol{e}=(a\bar{a})^{i+j}a$	$\boldsymbol{d}=(a\bar{a})^ia(a\bar{a})^j$	$i\geqslant 1, j\geqslant 0$
6	$\boldsymbol{e}=(\bar{a}a)^{i+j}$	$\boldsymbol{d}=(\bar{a}a)^i(a\bar{a})^j$	$i\geqslant 1, j\geqslant 0$
7	$\boldsymbol{e}=(a\bar{a})^{i+j}(\bar{a}a)^l$	$\boldsymbol{d}=(\bar{a}a)^i(a\bar{a})^{j+l}$	$i,j\geqslant 0, l\geqslant 1$
8	$\boldsymbol{e}=(a\bar{a})^i(\bar{a}a)^j\bar{a}(\bar{a}a)^l$	$\boldsymbol{d}=(\bar{a}a)^{i+j+l}\bar{a}$	$i,j\geqslant 0, l\geqslant 1$
9	$\boldsymbol{e}=(a\bar{a})^i\bar{a}^j(\bar{a}a)^l$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}^j(a\bar{a})^l$	$i\geqslant 0, j\geqslant 2, l\geqslant 1$
10	$\boldsymbol{e}=(a\bar{a})^ia^j(\bar{a}a)^l$	$\boldsymbol{d}=(\bar{a}a)^ia^j(a\bar{a})^l$	$i,j\geqslant 1, l\geqslant 0$
11	$\boldsymbol{e}=(a\bar{a})^{i+j+l}a$	$\boldsymbol{d}=(\bar{a}a)^i(a\bar{a})^ja(a\bar{a})^l$	$i,j\geqslant 1, l\geqslant 0$
12	$\boldsymbol{e}=(a\bar{a})^i(\bar{a}a)^{j+l}$	$\boldsymbol{d}=(\bar{a}a)^{i+j}(a\bar{a})^l$	$i,j\geqslant 1, l\geqslant 0$
13	$\boldsymbol{e}=(a\bar{a})^{i+j}a(a\bar{a})^la$	$\boldsymbol{d}=(\bar{a}a)^i(a\bar{a})^{j+l+1}$	$i,l\geqslant 0, j\geqslant 1$
14	$\boldsymbol{e}=(a\bar{a})^i(\bar{a}a)^j(a\bar{a})^la$	$\boldsymbol{d}=(\bar{a}a)^{i+j+l}\bar{a}$	$i,l\geqslant 0, j\geqslant 1$
15	$\boldsymbol{e}=(a\bar{a})^{i+j+l}a$	$\boldsymbol{d}=(\bar{a}a)^i(a\bar{a})^j(\bar{a}a)^l\bar{a}$	$i,l\geqslant 0, j\geqslant 1$
16	$\boldsymbol{e}=(a\bar{a})^i(\bar{a}a)^{j+l+1}$	$\boldsymbol{d}=(\bar{a}a)^{i+j}\bar{a}\bar{a}(a\bar{a})^l$	$i,l\geqslant 0, j\geqslant 1$
17	$\boldsymbol{e}=(a\bar{a})^{i+j}a(a\bar{a})^la$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}(\bar{a}a)^{j+l}\bar{a}$	$i,j,l\geqslant 0$
18	$\boldsymbol{e}=(a\bar{a})^ia^j(\bar{a}a)^l$	$\boldsymbol{d}=(\bar{a}a)^{i+1}a^{j-4}(a\bar{a})^{l+1}$	$i,l\geqslant 0, j\geqslant 4$
19	$\boldsymbol{e}=(a\bar{a})^ia(a\bar{a})^ja(a\bar{a})^la$	$\boldsymbol{d}=(\bar{a}a)^{i+j+l+1}\bar{a}$	$i,j,l\geqslant 0$
20	$\boldsymbol{e}=(a\bar{a})^{i+j+l+1}a$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}(\bar{a}a)^j\bar{a}(\bar{a}a)^l\bar{a}$	$i,j,l\geqslant 0$
21	$\boldsymbol{e}=(a\bar{a})^ia(a\bar{a})^{j+l}a$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}(a\bar{a})^j(\bar{a}a)^l\bar{a}$	$i,l\geqslant 0, j\geqslant 1$
22	$\boldsymbol{e}=(a\bar{a})^{i+1}\bar{a}^j(a\bar{a})^la$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}^{j+2}(\bar{a}a)^l\bar{a}$	$i,j,l\geqslant 0$
23	$\boldsymbol{e}=(a\bar{a})^{i+j+1}(\bar{a}a)^l$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}(\bar{a}a)^{j+l}\bar{a}$	$i,l\geqslant 0, j\geqslant 1$
24	$\boldsymbol{e}=(a\bar{a})^ia(a\bar{a})^j(\bar{a}a)^l$	$\boldsymbol{d}=(\bar{a}a)^{i+j+l}\bar{a}$	$i,l\geqslant 0, j\geqslant 1$
25	$\boldsymbol{e}=(a\bar{a})^{i+j+l}a$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}(\bar{a}a)^j(a\bar{a})^l$	$i,l\geqslant 0, j\geqslant 1$
26	$\boldsymbol{e}=(a\bar{a})^ia(a\bar{a})^{j+l}a$	$\boldsymbol{d}=(\bar{a}a)^{i+j+1}(a\bar{a})^l$	$i,l\geqslant 0, j\geqslant 1$

表 A.2　定理3.21中 $a=\bar{b}$ 的情形

序号	$\boldsymbol{e}$	$\boldsymbol{d}$	条件
1	$\boldsymbol{e}=(a\bar{a})^i a^{j+1}$	$\boldsymbol{d}=(\bar{a}a)^i \bar{a}a^j$	$i,j\geqslant 0$
2	$\boldsymbol{e}=(a\bar{a})^i(\bar{a}a)^j$	$\boldsymbol{d}=(\bar{a}a)^{i+j}$	$i\geqslant 0, j\geqslant 1$
3	$\boldsymbol{e}=(a\bar{a})^{i+j}a$	$\boldsymbol{d}=(\bar{a}a)^i a(\bar{a}a)^j$	$i\geqslant 0, j\geqslant 1$
4	$\boldsymbol{e}=(a\bar{a})^{i+j}$	$\boldsymbol{d}=(a\bar{a})^i(\bar{a}a)^j$	$i\geqslant 1, j\geqslant 0$
5	$\boldsymbol{e}=(\bar{a}a)^{i+j}\bar{a}$	$\boldsymbol{d}=(\bar{a}a)^i \bar{a}(\bar{a}a)^j$	$i\geqslant 1, j\geqslant 0$
6	$\boldsymbol{e}=(a\bar{a})^i\bar{a}^j(\bar{a}a)^l\bar{a}$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}^j(a\bar{a})^l a$	$i,l\geqslant 0, j\geqslant 2$
7	$\boldsymbol{e}=(a\bar{a})^{i+j}(\bar{a}a)^l\bar{a}$	$\boldsymbol{d}=(\bar{a}a)^i(a\bar{a})^{j+l}a$	$i,j,l\geqslant 0$
8	$\boldsymbol{e}=(a\bar{a})^i(\bar{a}a)^j\bar{a}(\bar{a}a)^l\bar{a}$	$\boldsymbol{d}=(\bar{a}a)^{i+j+l+1}$	$i,j,l\geqslant 0$
9	$\boldsymbol{e}=(a\bar{a})^i a^j(\bar{a}a)^l\bar{a}$	$\boldsymbol{d}=(\bar{a}a)^i a^j(a\bar{a})^l a$	$i,l\geqslant 0, j\geqslant 1$
10	$\boldsymbol{e}=(a\bar{a})^{i+j+l+1}$	$\boldsymbol{d}=(\bar{a}a)^i(a\bar{a})^j a(a\bar{a})^l a$	$i,l\geqslant 0, j\geqslant 1$
11	$\boldsymbol{e}=(a\bar{a})^i(\bar{a}a)^{j+l}\bar{a}$	$\boldsymbol{d}=(\bar{a}a)^{i+j}(a\bar{a})^l a$	$i,l\geqslant 0, j\geqslant 1$
12	$\boldsymbol{e}=(a\bar{a})^{i+j}a(a\bar{a})^l$	$\boldsymbol{d}=(\bar{a}a)^i(a\bar{a})^{j+l}a$	$i\geqslant 0, j,l\geqslant 1$
13	$\boldsymbol{e}=(a\bar{a})^i(\bar{a}a)^j(a\bar{a})^l$	$\boldsymbol{d}=(\bar{a}a)^{i+j+l}$	$i\geqslant 0, j,l\geqslant 1$
14	$\boldsymbol{e}=(a\bar{a})^{i+j+l}$	$\boldsymbol{d}=(\bar{a}a)^i(a\bar{a})^j(\bar{a}a)^l$	$i,j\geqslant 1, l\geqslant 0$
15	$\boldsymbol{e}=(a\bar{a})^i(\bar{a}a)^{j+l}\bar{a}$	$\boldsymbol{d}=(\bar{a}a)^{i+j}\bar{a}(\bar{a}a)^l$	$i,j\geqslant 1, l\geqslant 0$
16	$\boldsymbol{e}=(a\bar{a})^i a^{j+1}(a\bar{a})^l$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}a^j(\bar{a}a)^l$	$i\geqslant 0, j\geqslant 2, l\geqslant 1$
17	$\boldsymbol{e}=(a\bar{a})^{i+j}a(a\bar{a})^l$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}(\bar{a}a)^{j+l}$	$i,j,l\geqslant 0$
18	$\boldsymbol{e}=(a\bar{a})^i a(a\bar{a})^j a(a\bar{a})^l$	$\boldsymbol{d}=(\bar{a}a)^{i+j+l+1}$	$i,j,l\geqslant 0$
19	$\boldsymbol{e}=(a\bar{a})^{i+1}\bar{a}^j(a\bar{a})^l$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}^{j+2}(\bar{a}a)^l$	$i,j,l\geqslant 0$
20	$\boldsymbol{e}=(a\bar{a})^{i+j+l+1}$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}(\bar{a}a)^j\bar{a}(\bar{a}a)^l$	$i,l\geqslant 0, j\geqslant 1$
21	$\boldsymbol{e}=(a\bar{a})^i a(a\bar{a})^{j+l}$	$\boldsymbol{d}=(\bar{a}a)^{i+j}\bar{a}(\bar{a}a)^l$	$i,l\geqslant 0, j\geqslant 1$
22	$\boldsymbol{e}=(a\bar{a})^{i+j}(\bar{a}a)^l\bar{a}$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}(\bar{a}a)^{j+l}$	$i,l\geqslant 0, j\geqslant 2$
23	$\boldsymbol{e}=(a\bar{a})^i a(a\bar{a})^j(\bar{a}a)^l\bar{a}$	$\boldsymbol{d}=(\bar{a}a)^{i+j+l+1}$	$i,l\geqslant 0, j\geqslant 1$
24	$\boldsymbol{e}=(a\bar{a})^{i+j+l+1}$	$\boldsymbol{d}=(\bar{a}a)^i\bar{a}(\bar{a}a)^j(a\bar{a})^l a$	$i,l\geqslant 0, j\geqslant 1$
25	$\boldsymbol{e}=(a\bar{a})^i a(a\bar{a})^{j+l+1}$	$\boldsymbol{d}=(\bar{a}a)^{i+j+1}(a\bar{a})^l a$	$i,l\geqslant 0, j\geqslant 1$

附录 B　定理3.21的证明中的表格

表 B.1　定理3.21证明中的情形 (ii)

序号	$\boldsymbol{e}, \boldsymbol{d}$	参数 k,s,t,i,j 的约束条件	$a=b$	
1	$\boldsymbol{e}=\bar{a}^s(a\bar{a})^{\frac{k-t-s}{2}}(\bar{a}a)^{\frac{t}{2}}$ $\boldsymbol{d}=\bar{a}^s(a\bar{a})^{\frac{k-s}{2}}$	t 偶 $k-s-t$ 偶	是	(3.19), (3.25)
2	$\boldsymbol{e}=\bar{a}^s(a\bar{a})^{\frac{k-t-s}{2}}(\bar{a}a)^{\frac{t-1}{2}}\bar{a}$ $\boldsymbol{d}=\bar{a}^s(a\bar{a})^{\frac{k-s-1}{2}}a$	t 奇 $k-s-t$ 偶	否	
3	$\boldsymbol{e}=\bar{a}^s(a\bar{a})^{\frac{k-s-t-1}{2}}a(a\bar{a})^{\frac{t}{2}}$ $\boldsymbol{d}=\bar{a}^s(a\bar{a})^{\frac{k-s-1}{2}}a$	t 偶 $k-s-t$ 奇	否	(3.20), (3.25)
4	$\boldsymbol{e}=\bar{a}^s(a\bar{a})^{\frac{k-s-t-1}{2}}a(a\bar{a})^{\frac{t-1}{2}}a$ $\boldsymbol{d}=\bar{a}^s(a\bar{a})^{\frac{k-s}{2}}$	t 奇 $k-s-t$ 奇	是	
5	$\boldsymbol{e}=\bar{a}^s(a\bar{a})^{\frac{k-s-t}{2}}a^t$ $\boldsymbol{d}=\bar{a}^s(a\bar{a})^{\frac{k-s-t}{2}}a^t$	$k-s-t$ 偶	是	(3.19), (3.26)
6	$\boldsymbol{e}=\bar{a}^s(a\bar{a})^{\frac{k-s-t+1}{2}}\bar{a}^{t-1}$ $\boldsymbol{d}=\bar{a}^s(a\bar{a})^{\frac{k-s-t+1}{2}}\bar{a}^{t-1}$	$k-s-t$ 奇	否	(3.20), (3.26)
7	$\boldsymbol{e}=\bar{a}^s(a\bar{a})^{\frac{k-s-t}{2}}a^{j+t-k-1}(\bar{a}a)^{\frac{k-j+1}{2}}$ $\boldsymbol{d}=\bar{a}^s(a\bar{a})^{\frac{k-s-t}{2}}a^{j+t-k-1}(a\bar{a})^{\frac{k-j+1}{2}}$	$t\geqslant 2$ $k-s-t$ 偶 $k-j$ 奇	是	(3.19), (3.27)
8	$\boldsymbol{e}=\bar{a}^s(a\bar{a})^{\frac{k-s-t}{2}}a^{j+t-k-1}(\bar{a}a)^{\frac{k-j}{2}}\bar{a}$ $\boldsymbol{d}=\bar{a}^s(a\bar{a})^{\frac{k-s-t}{2}}a^{j+t-k-1}(a\bar{a})^{\frac{k-j}{2}}a$	$t\geqslant 2$ $k-s-t$ 偶 $k-j$ 偶	否	(3.19), (3.27)
9	$\boldsymbol{e}=\bar{a}^s(a\bar{a})^{\frac{k-s-t-1}{2}}a\bar{a}^{j+t-k-1}(a\bar{a})^{\frac{k-j+1}{2}}$ $\boldsymbol{d}=\bar{a}^s(a\bar{a})^{\frac{k-s-t+1}{2}}\bar{a}^{j+t-k-1}(a\bar{a})^{\frac{k-j-1}{2}}a$	$t\geqslant 2$ $k-s-t$ 奇 $k-j$ 奇	否	(3.20), (3.27)
10	$\boldsymbol{e}=\bar{a}^s(a\bar{a})^{\frac{k-s-t-1}{2}}a\bar{a}^{j+t-k-1}(a\bar{a})^{\frac{k-j}{2}}a$ $\boldsymbol{d}=\bar{a}^s(a\bar{a})^{\frac{k-s-t+1}{2}}\bar{a}^{j+t-k-1}(a\bar{a})^{\frac{k-j}{2}}$	$t\geqslant 2$ $k-s-t$ 奇 $k-j$ 偶	是	
11	$\boldsymbol{e}=(a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s}{2}}(\bar{a}a)^{\frac{t}{2}}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-s}{2}}$	t 偶, i 偶 $k-s-t$ 偶	是	(3.21), (3.25)

表格未完，下页继续

表 B.1　（续）

序号	$\boldsymbol{e}, \boldsymbol{d}$	参数 k,s,t,i,j 的约束条件	$a=b$	
12	$\boldsymbol{e}=(a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s}{2}}(\bar{a}a)^{\frac{t-1}{2}}\bar{a}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-s-1}{2}}a$	t 奇, i 偶 $k-s-t$ 偶	否	(3.21), (3.25)
13	$\boldsymbol{e}=(a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s}{2}}a^{t}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s}{2}}a^{t}$	i 偶 $k-s-t$ e 偶	是	(3.21), (3.26)
14	$\boldsymbol{e}=(a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s}{2}}a^{j+t-k-1}(\bar{a}a)^{\frac{k-j+1}{2}}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s}{2}}a^{j+t-k-1}(a\bar{a})^{\frac{k-j+1}{2}}$	i 偶, $t\geqslant 2$ $k-s-t$ 偶 $k-j$ 奇	是	(3.21), (3.27)
15	$\boldsymbol{e}=(a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s}{2}}a^{j+t-k-1}(\bar{a}a)^{\frac{k-j}{2}}\bar{a}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s}{2}}a^{j+t-k-1}(a\bar{a})^{\frac{k-j}{2}}a$	i 偶, $t\geqslant 2$ $k-s-t$ 偶 $k-j$ 偶	否	
16	$\boldsymbol{e}=(a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-s-t-1}{2}}a(a\bar{a})^{\frac{t}{2}}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-s-1}{2}}a$	t, i 偶 $k-s-t$ 奇	否	(3.22), (3.25)
17	$\boldsymbol{e}=(a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s-1}{2}}a(a\bar{a})^{\frac{t-1}{2}}a$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-s}{2}}$	t 奇, i 偶 $k-s-t$ 奇	是	
18	$\boldsymbol{e}=(a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s-1}{2}}a\bar{a}^{t}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s+1}{2}}\bar{a}^{t-1}$	i 偶 $k-s-t$ 奇	否	(3.22), (3.26)
19	$\boldsymbol{e}=(a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s-1}{2}}a\bar{a}^{j+t-k-1}(a\bar{a})^{\frac{k-j+1}{2}}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s-1}{2}}a\bar{a}^{j+t-k-1}(\bar{a}a)^{\frac{k-j+1}{2}}$	i 偶, $t\geqslant 2$ $k-s-t$ 奇 $k-j$ 奇	否	(3.22), (3.27)
20	$\boldsymbol{e}=(a\bar{a})^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s-1}{2}}a\bar{a}^{j+t-k-1}(a\bar{a})^{\frac{k-j}{2}}a$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i}{2}}\bar{a}^{s-i}(a\bar{a})^{\frac{k-t-s+1}{2}}\bar{a}^{j+t-k-1}(a\bar{a})^{\frac{k-j}{2}}$	i 偶, $t\geqslant 2$ $k-s-t$ 奇 $k-j$ 偶	是	
21	$\boldsymbol{e}=(a\bar{a})^{\frac{i-1}{2}}a^{s-i+1}(\bar{a}a)^{\frac{k-s-t}{2}}(a\bar{a})^{\frac{t}{2}}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i-1}{2}}\bar{a}a^{s-i}(\bar{a}a)^{\frac{k-s}{2}}$	t 偶, i 奇 $k-s-t$ 偶	否	
22	$\boldsymbol{e}=(a\bar{a})^{\frac{i-1}{2}}a^{s-i+1}(\bar{a}a)^{\frac{k-t-s}{2}}(a\bar{a})^{\frac{t-1}{2}}a$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i-1}{2}}\bar{a}a^{s-i}(\bar{a}a)^{\frac{k-s-1}{2}}\bar{a}$	t 奇数, i 奇 $k-s-t$ 偶	是	(3.23), (3.25)
23	$\boldsymbol{e}=(a\bar{a})^{\frac{i-1}{2}}a^{s-i}(a\bar{a})^{\frac{k-t-s+2}{2}}\bar{a}^{t-1}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i-1}{2}}\bar{a}a^{s-i}(\bar{a}a)^{\frac{k-t-s}{2}}\bar{a}^{t}$	i 奇 $k-s-t$ 偶	否	(3.23), (3.26)

表格未完，下页继续

表 B.1　（续）

序号	$\boldsymbol{e}, \boldsymbol{d}$	参数 k,s,t,i,j 的约束条件	$a=b$	
24	$\boldsymbol{e}=(a\bar{a})^{\frac{i-1}{2}}a^{s-i}(a\bar{a})^{\frac{k-t-s+2}{2}}\bar{a}^{j+t-k-2}(a\bar{a})^{\frac{k-j+1}{2}}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i-1}{2}}\bar{a}a^{s-i}(\bar{a}a)^{\frac{k-t-s}{2}}\bar{a}^{j+t-k-1}(\bar{a}a)^{\frac{k-j+1}{2}}$	i 奇, $t\geqslant 2$ $k-s-t$ 偶 $k-j$ 奇	否	(3.23), (3.27)
25	$\boldsymbol{e}=(a\bar{a})^{\frac{i-1}{2}}a^{s-i}(a\bar{a})^{\frac{k-t-s+2}{2}}\bar{a}^{j+t-k-2}(a\bar{a})^{\frac{k-j}{2}}a$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i-1}{2}}\bar{a}a^{s-i}(\bar{a}a)^{\frac{k-t-s}{2}}\bar{a}^{j+t-k}(a\bar{a})^{\frac{k-j}{2}}$	i 奇数, $t\geqslant 2$ $k-s-t$ 偶 $k-j$ 偶	是	(3.23), (3.27)
26	$\boldsymbol{e}=(a\bar{a})^{\frac{i-1}{2}}a^{s-i}(a\bar{a})^{\frac{k-s-t+1}{2}}(\bar{a}a)^{\frac{t}{2}}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i-1}{2}}\bar{a}a^{s-i}(\bar{a}a)^{\frac{k-s-1}{2}}\bar{a}$	t 偶, i 奇 $k-s-t$ 奇数	是	(3.24), (3.25)
27	$\boldsymbol{e}=(a\bar{a})^{\frac{i-1}{2}}a^{s-i}(a\bar{a})^{\frac{k-t-s+1}{2}}(\bar{a}a)^{\frac{t-1}{2}}\bar{a}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i-1}{2}}\bar{a}a^{s-i}(\bar{a}a)^{\frac{k-s}{2}}$	t, i 奇 $k-s-t$ 奇	否	
28	$\boldsymbol{e}=(a\bar{a})^{\frac{i-1}{2}}a^{s-i}(a\bar{a})^{\frac{k-t-s+1}{2}}a^{t}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i-1}{2}}\bar{a}a^{s-i}(\bar{a}a)^{\frac{k-t-s+1}{2}}a^{t-1}$	i 奇 $k-s-t$ 奇	是	(3.24), (3.26)
29	$\boldsymbol{e}=(a\bar{a})^{\frac{i-1}{2}}a^{s-i}(a\bar{a})^{\frac{k-t-s+1}{2}}a^{j+t-k-1}(\bar{a}a)^{\frac{k-j+1}{2}}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i-1}{2}}\bar{a}a^{s-i}(\bar{a}a)^{\frac{k-t-s+1}{2}}a^{j+t-k-2}(a\bar{a})^{\frac{k-j+1}{2}}$	i 奇, $t\geqslant 2$ $k-s-t$ 奇 $k-j$ 奇	是	(3.24),(3.27)
30	$\boldsymbol{e}=(a\bar{a})^{\frac{i-1}{2}}a^{s-i}(a\bar{a})^{\frac{k-t-s+1}{2}}a^{j+t-k-1}(\bar{a}a)^{\frac{k-j}{2}}\bar{a}$ $\boldsymbol{d}=(\bar{a}a)^{\frac{i-1}{2}}\bar{a}a^{s-i}(\bar{a}a)^{\frac{k-t-s+1}{2}}a^{j+t-k-1}(\bar{a}a)^{\frac{k-j}{2}}$	i 奇, $t\geqslant 2$ $k-s-t$ 奇 $k-j$ 偶	否	

致　谢

首先我要感谢我的导师张先得老师和葛根年老师。自我进入中国科学技术大学读博以来，两位老师在科研和生活上都给与了我很多的指导和建议。他们鼓励我去开阔视野，将研究主题扩展到更广的方向上，这极大地培养了我的独立科研能力。张老师和葛老师精深的理论知识，广阔的学科视野，严谨的治学态度更是为我树立了榜样，而这将使我终身受益。

其次我要感谢我的师兄——广州大学的张韬老师，他在科研上非常细心地给予了我很多指导和建议。和他讨论问题让我受益匪浅。

感谢和我一起学习的各位同门：孔祥梁、韩雪娇、徐民、兰昭君、余文俊、石飞、陈婷婷、徐子翔、谢城飞、钱昺辰、戚立波、奚元霄等。在 5 年的学习与生活的时光里，我们留下了很多美好的回忆。

感谢我在科大的朋友：郜东方、刘剑、程亦雨、杜家宾、戴涵，与他们一起成长令我的博士生活十分愉快。

感谢我的父母，他们是我强大的后盾。

由于作者水平有限，加之时间和篇幅所限，文中难免有谬误和不详之处，敬请各位专家学者不吝批评指正!

在读期间发表的学术论文与取得的研究成果

已发表论文

1. **Zuo Ye**, Tao Zhang, Xiande Zhang, and Gennian Ge, "Some New Results on Splitter Sets," IEEE Transactions on Information Theory, vol. 66, no. 5, pp. 2765-2776, May 2020.
2. Yu Ning, **Zuo Ye**, Gennian Ge, Fuyou Miao, Yan Xiong, and Xiande Zhang, "New Results on Self-Dual Generalized Reed-Solomon Codes", IEEE Transactions on Information Theory, July 2021, doi: 10.1109/TIT.2021.3096934.

待发表论文

1. **Zuo Ye**, Xiande Zhang, and Gennian Ge, "Reconstruction Codes for Two-Insertion Channels", submitted to IEEE Transactions on Information Theory.