arXiv:2302.01487v1 [math.NT] 3 Feb 2023

素数长度的冲突避免码与分圆数

LIANG-CHUNG HSIA、HUA-CHIEH LI 和 WEI-LIANG SUN

摘要。关于构造偶数长度、汉明重量为 3 的最优冲突避免码的问题，现已得到彻底解决。相反，对于奇长度的情形，这个问题仍未解决。事实证明，素数长度是需要构造的基本情形。本文研究素数长度的冲突避免码，并揭示其与所谓分圆数之间的联系。借助某些非零分圆数，一种广为人知的构造最优冲突避免码的算法可适用于某些素数长度。因此，我们得以确定一类新的素数长度下最优冲突避免码的大小。

关键词：二进制协议序列、无反馈多址碰撞信道、最优冲突避免码、分圆数、分圆矩阵、平方数。

1. 引言

在信息论中，将用于在无反馈的多址碰撞信道上传输数据包的二进制协议序列集合称为冲突避免码（CAC）；Mat90、NGM92、GV93、TR02、LT05 和 Lev 曾在数十年前对其进行研究。长度为 n、（汉明）重量为 w 的冲突避免码的数学模型如下。令 $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ 为模 n 的加法群。对于 $\mathbb{Z}_n$ 的一个 w 元子集 $x = \{x1, \ldots, x_w\}$，将 x 的差集记为 $\Delta(x) = \{x_i - x_j \mid i \neq j\}$。长度为 n、重量为 w 的冲突避免码是 $\mathbb{Z}_n$ 的 w 元子集的一个集合 $\mathscr{C}$，满足对于 $\mathscr{C}$ 中任意不同的 x、y，均有 $\Delta(x) \cap \Delta(y) = \varnothing$。每个 x 称为一个码字。如果冲突避免码在所有长度和重量相同的冲突避免码中具有最大大小，则称其为最优冲突避免码。当重量为 1 或 2 时，确定最优大小并不困难。然而，对于大于 2 的重量，寻找最优冲突避免码并确定其大小仍是一个开放问题。首先遇到的挑战是重量 3，我们将在下文介绍其进展。

假设重量 $w = 3$。许多作者已完全解决任意偶数长度的最优冲突避免码构造问题 [LT05, JMJ+07, MFU09, FLM10]。然而，关于奇长度的已知结果仍远未完善。当长度 n 为奇数时，n 的素因子 p 所对应的单位元乘法群中 2 的乘法阶，在构造最优冲突避免码时起着关键作用。为方便起见，对于奇素数 p，我们用 $\mathbb{Z}_p^\times$ 表示 $\mathbb{Z}_p$ 的乘法群，用 $o_p(2)$ 表示 2 在 $\mathbb{Z}_p^\times$ 中的乘法阶。文献 [LT05] 给出了满足 $4 \mid o_p(2)$ 的素数长度 p 的最优冲突避免码构造。之后，文献 [Lev07] 改进了这一构造，将其推广到合数长度，且该长度的每个素因子 p 均满足 $4 \mid o_p(2)$。

剩下的情况是，长度存在一个素因子 p，使得 $4 \nmid o_p(2)$。文献 [FLS14], 证明，这类长度的问题可以归约为长度 n 的问题，其中 n 的每个素因子 p 均满足 $4 \nmid o_p(2)$。他们还证明，长度为 $n = p^k$ 的最优冲突避免码可以由长度为 p 的最优冲突避免码构造出来，其中 p 是非 Wieferich 素数（即 $2^{p-1} \not\equiv 1 \pmod{p^2}$）。然而，素数长度 p 的构造尚未完全解决。关于其他奇长度的构造，可参见 [Mom07, WF13, LMSJ14, MM17, HLS] 。事实证明，素数长度是亟待解决的基础对象。这促使我们研究素数长度、重量 3 的冲突避免码。

对于奇素数长度 $p > 3$，3-子集 x 的差集 $\Delta(x)$ 的大小为 4 或 6，其中 x 属于 $\mathbb{Z}_p$。不失一般性，我们可以假设码字 x 为 $\{0, \alpha, \beta\}$，其中 α、 $\beta \in \mathbb{Z}_p^\times$。于是，$|\Delta(x)| = 4$ 当且仅当 $x = \{0, \alpha, 2\alpha\}$，其中 α。在这种情况下，x 称为等差码字。为了获得最优冲突避免码，尽可能多地使用等差码字是很自然的。若 $M^e(p)$ 表示所有仅由等差码字组成的冲突避免码中的最大大小，则有

$$M^e(p) = \frac{p - 1 - 2O(p)}{4}$$

其中，当 4 整除 $|\langle -1$ 时，$O(p) = 0$ $2\rangle|$，否则 $O(p) = (p - 1)/|\langle -12\rangle|$。此外，[FLS14，引理 3] 给出

$$M^e(p) \le M(p) \le M^e(p) + \left\lfloor \frac{O(p)}{3} \right\rfloor \tag{1}$$

其中，M(p) 表示所有冲突避免码中的最大大小。因此，若 $O(p) < 3$，则仅由等差码字组成的冲突避免码必定是最优的。剩下的情形是 $O(p) \ge 3$。 [FLS14] 的作者提出了一种构造非等差码字的算法。他们猜想，对于素数长度 p，该算法总能构造出 $\left\lfloor \frac{O(p)}{3} \right\rfloor$ 非等差码字。随后还可进一步得到 $\frac{p-1-2O(p)}{4}$ 个等差码字，根据式 (1) 中的上界，这个冲突避免码将是最优的。为此，我们将他们的猜想改写为关于乘法群 $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ 中由 -1 和 2 生成的子群 $\langle -1, 2\rangle$ 的陪集的表述。

猜想 A（[FLS14，猜想 1]）。设 p 为非 Wieferich 素数。那么，子群 $\langle -1, 2\rangle$ 在 $\mathbb{Z}_p^\times$ 中有 $3\left\lfloor \frac{O(p)}{3} \right\rfloor$ 个陪集 $A_1, B_1, C_1, \ldots, A_{\left\lfloor \frac{O(p)}{3} \right\rfloor}, B_{\left\lfloor \frac{O(p)}{3} \right\rfloor}, C_{\left\lfloor \frac{O(p)}{3} \right\rfloor}$，使得对于每个 i，都存在 $(a_i, b_i, c_i) \in A_i \times B_i \times C_i$ 满足

$$a_i + b_i = c_i \quad \text{in } \mathbb{Z}_p.$$

我们注意到，每个 (a_i, b_i, c_i) 都对应一个非等差码字 $x_i = \{0, a_i, c_i\}$ where $\Delta(x_i) = \{\pm a_i, \pm b_i, \pm c_i\}$。上述三元组 (a_i, b_i, c_i) 在他们的术语中对应于辅助超图中的一个超图匹配。我们举例说明猜想 A 和他们的算法如何用于构造一个最优冲突避免码。

考虑长度为 $p = 73$ 且重量为 3、其中 $O(p) = 4$ 的冲突避免码。首先，$\mathbb{Z}_{73}^{\times}$ 中有 $\langle -1,2\rangle$ 的四个陪集：

$$\langle -1,2\rangle, \quad 3\langle -1,2\rangle, \quad 5\langle -1,2\rangle, \quad 11\langle -1,2\rangle.$$

我们分别从三个不同的陪集中选取元素 a、b、c，使得 $a + b = c$。例如，我们从前三个陪集中分别选择 $a = 2$、$b = 3$ 和 $c = 5$。令 $x = \{0,2,5\}$。则 x 是一个非等差码字，并且 $\Delta(x) = \{\pm 2, \pm 3, \pm 5\}$。$\langle -1$中的元素、$2\rangle \setminus \Delta(x)$导出四个等差码字

$$\mathbf{x}_1 = \{0, 2^2, 2^3\}, \quad \mathbf{x}_2 = \{0, 2^4, 2^5\}, \quad \mathbf{x}_3 = \{0, 2^6, 2^7\}, \quad \mathbf{x}_4 = \{0, 2^8, 2^9\}.$$

这与 $3\langle -1$、$2\rangle \setminus \Delta(x)$、$5\langle -1$、$2\rangle \setminus \Delta(x)$ 以及 $11\langle -1$、$2\rangle \setminus \Delta(x)$ 类似，即

$$\mathbf{x}_{i+4} = \{0, 3\cdot 2^{2i}, 3\cdot 2^{2i+1}\}, \quad \mathbf{x}_{i+8} = \{0, 5\cdot 2^{2i}, 5\cdot 2^{2i+1}\}, \quad \mathbf{x}_{i+12} = \{0, 11\cdot 2^{2i}, 11\cdot 2^{2i+1}\},$$

分别对于 $i = 1$、2、3、4。所有码字 x、x1、.....、x_{16}的差集两两不相交。根据式 (1) 中 M(p) 的上界，集合 $\mathscr{C} = \{x$、x1、.....、$x_{16}\}$构成一个最优冲突避免码，其中包含 1 个非等差码字和 16 个等差码字。如果我们选择 $a = 6$、$b = 5$ 和 $c = 11$，使得 $a + b = c$，那么 $x = \{0,6,11\}$ 且 $\Delta(x) = \{\pm 6, \pm 5, \pm 11\}$。采用相同的步骤将得到另外 16 个等差码字。a、b、c 的不同选择将产生不同的最优冲突避免码。

[MZS14] 的作者独立地从商群$\mathbb{Z}_p^{\times}/\langle -1,2\rangle$的群结构角度，对猜想 A 中三元组 (A_i, B_i, C_i) 的存在性提出了类似的想法。他们注意到，由于 $\mathbb{Z}_p^{\times}$是循环群，因此 $\mathbb{Z}_p^{\times}/\langle -1,2\rangle$ 也是循环群。

猜想 B（[MZS14，猜想]）。设 p 为奇素数。若 $\left[\mathbb{Z}_p^{\times}: \langle -1,2\rangle\right] \geq 3$，则存在循环群 $\mathbb{Z}_p^{\times}/\langle -1,2\rangle$ 的生成元 $t\langle -1,2\rangle$，其中某个 $t \in \mathbb{Z}_p^{\times}$满足

$$1 + b = c$$

其中某个 $b \in t\langle -1,2\rangle$，以及某个 $c \in t^2\langle -1,2\rangle$。

注意，$\left[\mathbb{Z}_p^{\times}: \langle -1,2\rangle\right] \geq 3$ 意味着 $O(p) = 0$ 或 $O(p) \geq 3$。此外，若猜想 B 对素数 p 成立，则可依次取 $A_1 = t^0\langle -1,2\rangle$、$B_1 = t^1\langle -1,2\rangle$、$C_1 = t^2\langle -1,2\rangle$、$A_2 = t^3\langle -1,2\rangle$、$B_2 = t^4\langle -1,2\rangle$、$C_2 = t^5\langle -1,2\rangle$，以此类推，从而对每个 i 得到 $t^{3i} + t^{3i}b = t^{3i}c$，其中 $(t^{3i}, t^{3i}b, t^{3i}c) \in A_i \times B_i \times C_i$。因此，猜想 B 蕴含猜想 A。对于前面的例子，$p = 73$，t 可取 5。于是 $b = 5$，$c = 6 \in 5^2\langle -1,2\rangle$ 且$1 + 5 = 6$ 在 $\mathbb{Z}_p$中。此外，这里并未假设 p 是非 Wieferich 素数。在 [MZS14], 中，作者通过计算机验证了猜想 B 对素数 $p \leq 2^{30}$成立。

本文旨在研究猜想 B。全文中，我们用以下符号表示

$$\ell = \left[\mathbb{Z}_p^{\times} : \langle -1,2\rangle\right] = \left|\mathbb{Z}_p^{\times}/\langle -1,2\rangle\right|$$

对于给定的素数 p。猜想 B 中 b 和 c 的存在性与所谓的关于某个原根、阶为 ℓ 的分圆数 A(i, j) 密切相关，其中 i、j

是整数。特别地，当且仅当对某些 i，A(i, 2i) $\neq 0$ 时，b 和 c 都存在。更准确地说，猜想 B 等价于以下陈述。详情见第2节。

猜想。设 p 为奇素数，且 $\ell = \left[\mathbb{Z}_p^\times : \langle -1, 2\rangle\right]$。若 $\ell \geq 3$，则对于某个 $1 \leq$ i $\leq \ell - 1$，有 A(i, 2i) $\neq 0$，且 (i ℓ) $= 1$。

C.F. Gauss [Gau01] 曾研究分圆数，后来 L.E. Dickson[Dic35b, Dic35a, Dic35c] 在华林问题的背景下研究了这些数。一个核心问题是用某个丢番图方程组的解来确定这些数。另见综述 [Raj80, Kat02, AT20]。然而，A(i, 2i) $\neq 0$ 是否成立仍不明显，因为当 ℓ 不断增大时，要么难以找到合适的丢番图方程组，要么难以写出分圆数的公式。最近，分圆数被应用于一种安全的公钥密码学模型[ATP21]。

本文研究上述猜想，并将证明以下结果 t.

定理A. 设 p 为奇素数，且 $\ell = [\mathbb{Z}_p^\times : \langle -1, 2\rangle]$。若 ℓ 为奇素数，则对于某个满足 (i ℓ) $= 1$ 的 $1 \leq$ i $\leq \ell - 1$，有 A(i, 2i) $\neq 0$。

这不仅回答了猜想 B，也回答了关于一类素数 p 的猜想 A。此外，最优冲突避免码的大小 M(p) 可确定如下；当 $4 \nmid o_p(2)$ 时，O(p) $= \ell$。

定理B. 设 p 为满足 $4 \nmid o_p(2)$ 的奇素数。若 $\ell = [\mathbb{Z}_p^\times : \langle -1, 2\rangle]$ 为奇素数，则长度为 p 、重量为 3 的最优冲突避免码的大小为

$$\frac{p-1-2\ell}{4} + \left\lfloor \frac{\ell}{3} \right\rfloor.$$

本文组织如下。第2节介绍分圆数，并探讨这些数与猜想 B 的联系。第 3 节将由分圆数引出一个有趣的矩阵。该矩阵可用于回答猜想 B，以及关于 ℓ 较小的素数的猜想 A。第4节将说明，某个 $\mathbb{Z}_p$ 子集中的平方数的数量可以表示为特定的分圆数之和。通过计数平方数，并利用 [BHKM13]，中给出的分圆数上界，我们将证明定理A。最后，我们将指出，对于具有合数 ℓ 的素数，会遇到一个障碍。

2. 预备知识

本文中，p 是一个奇素数，$\mathbb{Z}_p$ 是含有 p 个元素的有限域。全文中，我们记

$$L = \langle -1, 2\rangle$$

$\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ 由 -1 和 2 生成的子群，然后是 $\ell = \left[\mathbb{Z}_p^\times : \text{L}\right]$ 是 L 在 $\mathbb{Z}_p^\times$中的指数。我们始终假设

$$\ell \geq 3.$$

$\mathbb{Z}_p^\times$ 的生成元也称为 $\mathbb{Z}_p$ 的原根。固定一个原根 g。定义数

$$A(i,j)=\left|\left\{(m,n)\mid 0\le m,n\le\frac{p-1}{\ell}-1 \text{ and } 1+g^{i+m\ell}=g^{j+n\ell}\right\}\right|$$

对于 i、j $\in\mathbb{Z}$。这些数 A(i, j) 被称为关于 g 的 ℓ 阶分圆数。我们可以将 A(i, j) 重写如下。注意，$|L|=p_\ell^{-1}$，且 L 由 ℓ 次幂元素组成，~~其~~中元素取自 $\mathbb{Z}_p^\times$。因此，对于 $0\le$ m、n $\le|L|-1$，$g^{m\ell}$ 和 $g^{n\ell}\in$ L 均成立。由此可得

$$A(i,j)=\left|(1+g^iL)\cap g^jL\right|$$

对于 i、j $\in\mathbb{Z}$。如果 i′ 和 j′ 是满足 i′ ≡ i（模 ℓ）以及 j′ ≡ j（模 ℓ）的整数，那么 $g^{i'}L=g^iL$ 且 $g^{j'}L=g^jL$。我们有 A(i′, j′) = A(i, j)。因此，考虑模 ℓ意义下的 i、j 是方便的。

由于 g 是一个原根且 $\ell=[\mathbb{Z}_p^\times:\ L]$，商群 $\mathbb{Z}_p^\times/L$ 由元素 $g^0L=L$、g^1L.....、$g^{\ell-1}L$ 组成。特别地，集合

$$\left\{g^iL\mid 1\le i\le\ell \text{ and } (i,\ell)=1\right\}$$

是 $\mathbb{Z}_p^\times/L$ 的一组完整生成元，其中（·,·）表示给定两个整数的最大公约数。令 t $\in\mathbb{Z}_p^\times$。当且仅当对于某个 $1\le$ i $\le\ell$（满足 (i ℓ) = 1）有 tL $=g^iL$ 时，tL 生成 $\mathbb{Z}_p^\times/L$。此外，

$$\left|(1+tL)\cap t^2L\right|=\left|(1+g^iL)\cap g^{2i}L\right|=A(i,2i).$$

因此，对于 p，猜想 B 成立，当且仅当对于某个 $1\le$i $\le\ell$有 A(i, 2i) $\neq0$（满足 (i ℓ) = 1）。由于每个 A(i, 2i) 都是非负的，因此只需考虑以下和式

$$s(\ell)=\sum_{\substack{1\le i\le\ell,\\(i,\ell)=1}}A(i,2i).$$

上述论证实际上说明了以下引理。

引理 2.1。设 p 和 ℓ如上所述。则 s(ℓ) $\neq0$，当且仅当猜想 B 对此 p 成立。

和式 s(ℓ) 是相对于给定原根 g 定义的。事实上，选取任意原根时，我们都可以自由计算 s(ℓ)。这在实践中非常有帮助。由于我们没有找到关于这一事实的任何参考文献，因此将证明留在下文，供读者参考。

命题 2.2。和 s(ℓ) 与原根的选择无关。

证明。设 h 是 $\mathbb{Z}_p$ 的原根。记 A′(i, j) = $|(1+h^iL)\cap h^jL|$，并记 s′(ℓ) 为当 i = 1, . . . ,ℓ 且 (i ℓ) = 1 时，A′(i, 2i) 的和。由于 hL 也生成 $\mathbb{Z}_p^\times/L$，故对某个满足 (k ℓ) = 1 的 $1\le$k $\le\ell$，有 hL $=g^kL$。于是 $h^iL=g^{ki}L$，因此对 i, j $\in\mathbb{Z}$，A′(i, j) = A(ki, k j)。回顾一下，$\{1\le$i $\le\ell\mid$(i ℓ) = 1$\}$ 是模 ℓ 的既约剩余系。由于 (k ℓ) = 1，可知 $\{$ki $\mid 1\le$i $\le\ell$，且 (i ℓ) = 1$\}$ 也是模 ℓ 的既约剩余系。

因此,

$$s'(\ell)=\sum_{\substack{1\le i\le \ell,\\ (i,\ell)=1}} A'(i,2i)=\sum_{\substack{1\le i\le \ell,\\ (i,\ell)=1}} A\left(ki,k(2i)\right)=\sum_{\substack{1\le i\le \ell,\\ (i,\ell)=1}} A(i,2i)=s(\ell).$$

□

正如我们所提到的，分圆数理论中的主要问题之一，是用某些丢番图方程组的解来找出所有 A(i, j) 的显式公式。例如，考虑满足 $\ell=3$ 的 $p\equiv 1 \pmod 3$。众所周知，丢番图方程组

$$\begin{cases} 4p=X^2+27Y^2,\\ X\equiv 1 \pmod 3 \end{cases}$$

has 有一个关于唯一的 a 的解 (a, b)，其中 $-p<a<p$。[Gau01，第 358] 节给出

$$A(0,0)=\frac{1}{9}(p-8+a),$$

$$A(0,1)=A(1,0)=A(2,2)=\frac{1}{18}(2p-4-a+9b),$$

$$A(0,2)=A(1,1)=A(2,0)=\frac{1}{18}(2p-4-a-9b),$$

$$A(1,2)=A(2,1)=\frac{1}{9}(p+1+a)$$

其中，b 的符号取决于原根的选择。在这种情况下，A(1, 2) =A(2, 1) >0，因此

$$s(3)=A(1,2)+A(2,4)=A(1,2)+A(2,1)>0,$$

而 A(2, 4) = A(2, 1)，因为 $4\equiv 1 \pmod{\ell}$。然而，对于较大的 ℓ，公式将极其复杂且难以求出。例如，$\ell=11$ 的公式发表于 [LW75] 中。但对于 $p\equiv 1 \pmod{11}$，并不明显 s(11) $\neq 0$ 是否成立。另见例 4.5。

我们推导出以下有用性质。

引理 2.3. 对于模 ℓ 的 i、j,

$$A(i,j)=A(-i,j-i) \quad and \quad A(i,j)=A(j,i).$$

证明。对于 $\alpha\in(1+g^iL)\cap g^jL$，设 $\alpha=1+g^ia=gjb$，其中 a、b $\in L$。可得$1+(\alpha-1)^{-1}=1+g^{-i}a^{-1}\in 1+g^{-i}L$。此外，$1+(\alpha-1)^{-1}=(g^ia+1)g^{-i}a^{-1}=(g^jb)(g^{-i}a^{-1})=g^{j-i}(ba^{-1})\in g^{j-i}L$。因此，存在一个从 $(1+g^iL)\cap gjL$ 到 $(1+g^{-i}L)\cap gj{-}iL$ 的映射 φ，其定义为 $\varphi(\alpha)=1+(\alpha-1)^{-1}$。由此可推得 φ 是一个双射。因此，第一个等式成立。

对于第二个等式，注意到当 $-1\in L$ 时，$1-\alpha=1+g_j(-b)=g^i(-a)\in(1+g_jL)\cap g^iL$。于是，$\alpha\mapsto 1-\alpha$ 给出了从 $(1+g^iL)\cap g_jL$ 到 $(1+g^jL)\cap g^iL$ 的一个双射。□

3. 扩展分圆矩阵

模关系和分圆数的性质引出了一个有趣的矩阵。这将为冲突避免码问题带来新的见解。在本节中，我们将能够轻松回答关于较小 ℓ 的猜想 B。

给定 $\mathbb{Z}_p$ 的一个原根，分圆矩阵是一个 $\ell\times\ell$ 矩阵，定义如下

$$(A(i,j))_{\ell\times\ell} \quad \text{for } i,j=0,1,\ldots,\ell-1.$$

给出分圆矩阵的一种变体很方便。我们将扩展分圆矩阵 $B=(b_{i,j})_{\ell\times\ell}$ 定义如下

$$b_{i,j}=\begin{cases} A(0,0)+1 & \text{if } i=j=0;\\ A(i,j) & \text{otherwise.}\end{cases}$$

对于模 ℓ 的 i、j，引理 2.3 给出了矩阵元素之间的关系：

$$b_{i,j}=b_{-i,j-i}=b_{j-i,-i}=b_{i-j,-j}=b_{-j,i-j}=b_{j,i}. \tag{2}$$

为方便起见，称 B 的第 $(b_{i,0},b_{i,1},\ldots,b_{i,\ell-1})$ 行以 i 为指数，其中 $i=0,\ldots,\ell-1$。矩阵 B 具有以下良好性质。

引理 3.1. 设 B 为上述扩展分圆矩阵。

(i) B 是对称矩阵，且其项为非负整数，$b_{0,0}>0$. (ii) $b_{0,0}$ 之后的对角项是以 0 为指数的行的逆序：

$$(b_{1,1},b_{2,2},\ldots,b_{\ell-1,\ell-1})=(b_{0,\ell-1},b_{0,\ell-2},\ldots,b_{0,1}).$$

(iii) 对于 $1\le i\le\ell-1$，以 $\ell-i$ 为指数的行相对于以 i 为指数的行向左循环移位 i 次：

$$(b_{\ell-i,0},b_{\ell-i,1},\ldots,b_{\ell-i,\ell-1})=(b_{i,i},b_{i,i+1},\ldots,b_{i,\ell-1},b_{i,0},\ldots,b_{i,i-1})$$

(iv) 迹、每行之和以及每列之和均为 $|L|=\frac{p-1}{\ell}$ ——.

证明。(i)、(ii) 和 (iii) 可由 (2) 显然得出：$b_{i,j}=b_{j,i}$, $b_{i,i}=b_{0,\ell-i}$ 以及 $b_{\ell-i,j}=b_{i,j+i}$。对于 (iv)，设 g 为给定的原根。于是群 $\mathbb{Z}_p^\times$ 是 g^0L、g^1L.....、$g^{\ell-1}L$ 的不交并。由于 $1\notin 1+L$，以 0 为指数的行之和为

$$\sum_{j=0}^{\ell-1}b_{0,j}=1+\sum_{j=0}^{\ell-1}A(0,j)=1+\sum_{j=0}^{\ell-1}\left|(1+L)\cap g^jL\right|=1+\left|(1+L)\cap\mathbb{Z}_p^\times\right|=|L|.$$

此外，指数为 i 的行之和为

$$\sum_{j=0}^{\ell-1}b_{i,j}=\sum_{j=0}^{\ell-1}A(i,j)=\sum_{j=0}^{\ell-1}\left|(1+g^iL)\cap g^jL\right|=\left|(1+g^iL)\cap\mathbb{Z}_p^\times\right|=|L|.$$

由 (ii)，B 的迹也为 $|L|$。最后，由 (i)，每一列的和为 $|L|$。 □

回顾和 s(ℓ)，我们有

$$s(\ell)=\sum_{\substack{1\le i\le \ell,\\ (i,\ell)=1}} b_{i,2i}.$$

由关系式 (2) 和引理 3.1 可知，对于较小的 ℓ，$s(\ell)>0$。

命题 3.2. 对于 $\ell=3,4,5$，有 $s(\ell)>0$。

证明。利用 (2) 以及引理 3.1 的 (i)、(ii)、(iii)，我们将矩阵 B 化简。为方便起见，我们用 r_i 表示由 i 编号的行。

对于 $\ell=3$,

$$B=\begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2}\\ b_{1,0} & b_{1,1} & b_{1,2}\\ b_{2,0} & b_{2,1} & b_{2,2}\end{pmatrix}.$$

由对称性，$b1_{,0}=b^{0,1}$，$b2_{,0}=b^{0,2}$，且 $b2_{,1}=b^{1,2}$。由引理 3.1(ii)，$(b^{1,1},b^{2,2})=(b^{0,2},b^{0,1})$。因此,

$$B=\begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2}\\ b_{0,1} & b_{0,2} & b_{1,2}\\ b_{0,2} & b_{1,2} & b_{0,1}\end{pmatrix}.$$

根据引理 3.1(iv)，r_0 与 r_1 的和相等。我们有 $b_{0,0}=b^{1,2}$。由此得到 $s(3)=b_{1,2}+b_{2,4}\ge b_{1,2}=b_{0,0}>0.$

对于 $\ell=4$,

$$B=\begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3}\\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3}\\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3}\\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3}\end{pmatrix}.$$

根据引理 3.1(ii)，$b1_{,1}=b^{0,3}$。由 (2)，我们可以推得 $b1_{,3}=b^{1,2}$。因此 r_1 变为 $(b^{1,0},b^{0,3},b^{1,2},b^{1,2})$。根据引理 3.1(iii)，$r_2$ 满足 $(b^{2,0},b^{2,1},b^{2,2},b^{2,3})=(b^{2,2},b^{2,3},b^{2,0},b^{2,1})$，进而可得 $(b^{2,0},b^{2,1},b^{2,0},b^{2,1})$。此外，通过对 r_1 进行移位，$r_3=(b^{0,3},b^{1,2},b^{1,2},b^{1,0})$。因此，根据对称性，我们有

$$B=\begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3}\\ b_{0,1} & b_{0,3} & b_{1,2} & b_{1,2}\\ b_{0,2} & b_{1,2} & b_{0,2} & b_{1,2}\\ b_{0,3} & b_{1,2} & b_{1,2} & b_{0,1}\end{pmatrix}.$$

设 $s(4)=b1_{,2}+b3_{,2}=0$。那么 $b1_{,2}=0$ 和

$$B=\begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3}\\ b_{0,1} & b_{0,3} & 0 & 0\\ b_{0,2} & 0 & b_{0,2} & 0\\ b_{0,3} & 0 & 0 & b_{0,1}\end{pmatrix}.$$

根据引理 3.1(iv)，r_0 与 r_1 的和相等。我们得到 $b0_{,0}=0$。这与 $b0_{,0}>0$ 矛盾。因此，$s(4)\neq 0$。

对于 $\ell = 5$,

$$B = \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} & b_{0,4} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} & b_{1,4} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} & b_{2,4} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} & b_{3,4} \\ b_{4,0} & b_{4,1} & b_{4,2} & b_{4,3} & b_{4,4} \end{pmatrix}.$$

根据引理 3.1(ii)，b1，$_1$ =b$_{0,4}$ 和 b2，$_2$ = b$_{0,3}$。由 (2) 可推得 b1，$_4$ = b$_{1,2}$ 和 b2，$_3$ =b2，$_4$ =b$_{1,3}$。因此，r$_1$ =(b$_{1,0}$,b$_{0,4}$,b$_{1,2}$,b$_{1,3}$,b$_{1,2}$) 和 r$_2$ =(b$_{2,0}$,b$_{2,1}$,b$_{0,3}$,b$_{1,3}$,b$_{1,3}$)。根据引理 3.1(iii)，通过分别平移 r$_2$ 和 r$_1$,，可得 r$_3$ =(b$_{0,3}$, b$_{1,3}$,b$_{1,3}$,b$_{2,0}$,b$_{2,1}$和 r $_4$ =(b$_{0,4}$,b$_{1,2}$,b$_{1,3}$,b$_{1,2}$,b$_{1,0}$)。因此，根据对称性，我们有

$$B = \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} & b_{0,4} \\ b_{0,1} & b_{0,4} & b_{1,2} & b_{1,3} & b_{1,2} \\ b_{0,2} & b_{1,2} & b_{0,3} & b_{1,3} & b_{1,3} \\ b_{0,3} & b_{1,3} & b_{1,3} & b_{0,2} & b_{1,2} \\ b_{0,4} & b_{1,2} & b_{1,3} & b_{1,2} & b_{0,1} \end{pmatrix}.$$

假设 s(5) =b1，$_2$+b2，$_4$+b3，$_1$+b4，$_3$ = 0。那么 b1，$_2$ =b1，$_3$ = 0，于是我们有

$$B = \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} & b_{0,4} \\ b_{0,1} & b_{0,4} & 0 & 0 & 0 \\ b_{0,2} & 0 & b_{0,3} & 0 & 0 \\ b_{0,3} & 0 & 0 & b_{0,2} & 0 \\ b_{0,4} & 0 & 0 & 0 & b_{01} \end{pmatrix}.$$

根据引理 3.1(iv)，r$_0$ 和 r$_1$ 的和相等。我们得到 b0，$_0$ = 0，矛盾。因此，s(5) $\neq 0$。□

根据引理 2.1，若 s(ℓ) $\neq 0$，则素数 p 满足猜想 B 和猜想 A。因此，我们得到关于最优冲突避免码大小的以下结论。

推论 3.3。设 p 是一个满足 4 ∤ o$_p$(2) 的奇素数。若 $\ell = \left[\mathbb{Z}_p^{\times} : \langle -1, 2\rangle\right] = 3,4,5$，则长度为 p、重量为 3 的最优冲突避免码的大小为 $p^{\frac{-1-2\ell}{4}} + 1$。

推论 3.3 也以不同的方法见于 [MZS14，推论 4.8] 。当$\ell \geq 6$时，上述方法不足以检验 s(ℓ) $\neq 0$ 是否成立。在下一节中，我们将探讨 s(ℓ) 的更多性质。

4. 平方数的数量

在上一节中，我们看到，某些分圆数之和 s(ℓ) 实际上回答了关于某些 ℓ 的猜想 A 和猜想 B。本节将探讨 s(ℓ) 如何与 $\mathbb{Z}_p$ 的平方数相联系，并回答关于更多 ℓ的这两个猜想。首先，回到猜想 B 中的方程 1 +b = c，其中 b $\in$tL，c $\in$t^{2}L，且 t $\in \mathbb{Z}_p^{\times}$ 满足 $\mathbb{Z}_p^{\times}$/L = ⟨tL⟩。在这种情况下，(1 +tL) ∩t^{2}L 非空。令 b = tβ，c = t^{2}γ，其中β, γ $\in$L。由此得到 t^{2}γ − tβ − 1 = 0。将该方程视为关于 t 的二次多项式,

判别式表明 $\beta^2+4\gamma$ 是一个平方数。等价地， $1+4\beta^{-2}\gamma$ 是一个平方数。由于 $2\in L$，可知 $1+4\beta^{-2}\gamma$ 是 L 中的平方数。这使我们开始考虑$1+L$ 中的平方数。一般来说，如果对于 $\alpha\in L$， $1+\alpha$ 是一个平方数，即 $1+\alpha=(s-1)^2$，其中某个 $s\in\mathbb{Z}_p^\times$ 满足该条件，那么我们有 $1+s(2\alpha^{-1})=s^2\alpha^{-1}$，它给出了 $(1+sL)\cap s^2L$ 中的一个元素，因为$2\alpha^{-1},\alpha^{-1}\in L$。注意，对于某个 $0\le i\le \ell-1$，有 $sL=g^iL$，其中 g 是给定的原根。因此 A(i, 2i) $\neq 0$。于是， $1+L$ 中的每个平方数（如果存在）都会使某个 $0\le i\le \ell-1$ 对应一个非零分圆数 A(i, 2i)。我们将看到，对于某个 $i\neq 0$， A(i, 2i) $\neq 0$。由此可知，当 ℓ 是素数时， $s(\ell)\neq 0$。

给定 $\mathbb{Z}_p$ 的一个原根 g，我们通常考虑 $1+g^kL$ 中的平方数，其中 $0\le k\le \ell-1$。固定 k，并令 $r\in\mathbb{Z}_p$ 使得 $r^2\in 1+g^kL$。于是 $r^2-1\in g^kL$。注意， $r^2-1=(r-1)(r+1)$，且 $r\neq\pm1$，因为 $0\notin g^kL$。因此，对某些满足 $i+j\equiv k\pmod{\ell}$ 的 i、j，有 $r-1\in g^iL$ 且 $r+1\in g^jL$，因为 $(g^iL)(g^jL)=g^kL$。特别地， $r\in(1+g^iL)\cap(-1+g^jL)$。反过来，如果 $r'\in(1+g^iL)\cap(-1+gjL)$，且 $i+j\equiv k\pmod{\ell}$，那么我们有 $r'^2\in 1+g^kL$。令

$$R(i,j)=(1+g^iL)\cap(-1+g^jL)$$

对于整数 i、j，令 S_k 为 $1+g^kL$ 的平方数集合。上述讨论给出了一个满射

$$\begin{aligned} f_k:\ \bigcup_{\substack{0\le i,j\le \ell-1,\\ i+j\equiv k\,(\mathrm{mod}\,\ell)}} R(i,j) &\to S_k\\ r &\mapsto r^2. \end{aligned}$$

引理 4.1。令 R(i, j) 如上所述。

(i) 对于 $0\le i, i', j, j'\le \ell-1$，如果 $i\neq i'$或 $j\neq j'$，则 $R(i,j)\cap R(i',j')=\varnothing$。因此， f_k 的定义域是各个 R(i, j) 的不交并。(ii) 对于模 ℓ, | 的 i、j，有 R(i, j) | = A(i, j)。

证明。对于 (i)，当 $i\neq i'$ 时，有 $(1+g^iL)\cap(1+g^{i'}L)=\varnothing$，因为 $g^iL\cap g^{i'}L=\varnothing$。类似地，当 $j\neq j'$ 时，也有 $(-1+g^jL)\cap(-1+g^{j'}L)=\varnothing$。结论得证。

对于 (ii)，考虑映射

$$\begin{aligned} \psi:\ R(i,j) &\to (1+g^iL)\cap g^jL\\ r &\mapsto 2^{-1}(1+r). \end{aligned}$$

容易看出， ψ 是单射。对于每个 $s\in(1+g^iL)\cap g^jL$， $-1+2s\in T(i,j)$，因为 $2\in L$。此外， $\psi(-1+2s)=s$。因此， ψ 是双射，结论由 A(i, j) 的定义即可得出。□

下面的引理建立了某个分圆数之和与平方数个数之间的联系。

引理 4.2. $1+L$ 的平方数的数量为

$$\frac{1}{2}+\frac{1}{2}\sum_{i=0}^{\ell-1}A(i,-i).$$

对于 $1 \le k \le \ell-1$，$1+g^k L$ 的平方数的数量为

$$\frac{1}{2}\sum_{i=0}^{\ell-1} A(i,k-i).$$

证明。令 R(i, j)、S_k 和 f_k 如上。注意，若 $0 \in R(i,j)$，则 $0 \in 1+g^i L$ 且 $0 \in -1+g^j L$。由于 $1,-1 \in L$，我们推得 $0 \in R(i,j)$ 当且仅当 $i = j = 0$。回顾引理 4.1(i)，f_k 的定义域是不交并 R(i, j)，其中 $0 \le i, j \le \ell-1$ 且 $i+j \equiv k \pmod{\ell}$。我们分两种情形讨论：$i = j$ 和 $i \ne j$。

情形 1：$i = j$。显然，$R(i,i) = -R(i,i)$。此外，$f_k(r) = r^2 = f_k(-r)$。因此，f_k 在 $R(i,i) \setminus \{0\}$ 上的限制是二对一的。若 $0 \in R(i,i)$，则 $i = 0$，且这仅在 $k = 0$ 时成立。因此，R(i, i) 在 f_0 下的像的大小为：当 $i = 0$ 时是 $A(0,0)\frac{1}{2} + \frac{1}{2}$，当 $i \ne 0$ 时是 $\frac{1}{2}A(i,i)$。对于 $k = 1, \ldots, \ell-1$，R(i, i) 在 f_k 下的像的大小为 $\frac{1}{2}A(i,i)$。

情形 2：$i \ne j$。在这种情形下，$R(i,j) \ne R(j,i)$，且 $R(j,i) = -R(i,j)$。因此，f_k 在 $R(i,j) \cup R(j,i)$ 上的限制也是二对一的。由此可知，$R(i,j) \cup R(j,i)$ 在 f_k 下的像大小为 $\frac{1}{2}(A(i,j) + A(j,i))$。

由于 f_k 是满射，情形 1 和情形 2 得出

$$|S_0| = \frac{1}{2} + \frac{1}{2}\sum_{\substack{0 \le i,j \le \ell-1,\\ i+j \equiv 0 \pmod{\ell}}} A(i,j) \quad \text{and} \quad |S_k| = \frac{1}{2}\sum_{\substack{0 \le i,j \le \ell-1,\\ i+j \equiv k \pmod{\ell}}} A(i,j)$$

对于 $k = 1, \ldots, \ell-1$。最后，每个 i 都对应唯一的 j，使得 $j \equiv k - i \pmod{\ell}$。证毕。□

例 4.3。设 $p = 31$。则 $L = \{\pm 1, \pm 2, \pm 2^2, \pm 2^3, \pm 2^4\}$ 和 $\ell = 3$。取 $g = 3$为一个原根。则 $1+g^k L$ 的平方数集合 S_k 如下：

$$S_0 = \{0,2,5,9,16,28\}, \quad S_1 = \{4,7,8,18,20,25\}, \quad S_2 = \{10,14,19\}.$$

另一方面，分圆矩阵（第 3 节）为

$$\begin{pmatrix} A(0,0) & A(0,1) & A(0,2) \\ A(1,0) & A(1,1) & A(1,2) \\ A(2,0) & A(2,1) & A(2,2) \end{pmatrix} = \begin{pmatrix} 3 & 4 & 2 \\ 4 & 2 & 4 \\ 2 & 4 & 4 \end{pmatrix}.$$

事实上，$|S_0| = \frac{1}{2} + \frac{1}{2}(A(0,0) + A(1,2) + A(2,1))$、$|S_1| = \frac{1}{2}(A(0,1) + A(1,0) + A(2,2))$ 以及 $|S_2| = \frac{1}{2}(A(0,2) + A(1,1) + A(2,0))$。

让我们聚焦于 $1+L$。根据引理 2.3，$A(i,-i) = A(-i,i) = A(i,2i)$。因此，$1+L$ 的平方数的数量也是

$$\frac{1}{2} + \frac{1}{2}\sum_{i=0}^{\ell-1} A(i,2i).$$

回顾一下，

$$s(\ell) = \sum_{\substack{1 \le i \le \ell,\\ (i,\ell)=1}} A(i,2i).$$

我们得出以下结论。

命题 4.4. 如果 ℓ 是奇素数，那么 $1+L$ 的平方数的数量为 $\frac{1}{2}(1+A(0,0)+s(\ell))$.

注意到 $1+L$ 至少包含一个平方数，即 0。当 ℓ 是奇素数时，命题 4.4 表明，如果相对于 $1+L$ 的平方数的数量而言，$A(0,0)$ 足够小，我们将有 $s(\ell)\neq 0$。下面来看一个例子。

例 4.5. 设 $p=331$。那么 $|L|=30$ 且 $\ell=11$。可以验证，$A(0,0)=|(1+L)\cap L|=5$。因此，根据命题 4.4，$1+L$ 有 $\frac{1}{2}+\frac{1}{2}s(11)$ 2 个平方数。注意到 $1+L$ 至少包含 4 个平方数，例如 0、$1+4=233^2$、$1-4=63^2$ 和 $1+8=3^2$。我们有 $s(11)\neq 0$。事实上，如果我们选取一个原根 $g=3$，就可以计算出 $A(1,2)=3$。这也说明了 $s(11)\neq 0$，因为根据引理 2.2，它与原根的选取无关。

现在我们关注 $A(0,0)$ 以及 $1+L$ 中平方数的数量。在 [BHKM13], 中，作者研究了分圆数的上界。他们通过计算某个元素属于 $\mathbb{Z}_p$ 的矩阵的秩来确定 $A(i,j)$。估计该秩可为一般的 ℓ 给出 $A(i,j)$ 的上界。下文将使用他们关于 $A(0,0)$ 的结果。

引理 4.6（[BHKM13，定理 1.1(iii)]）。若 $\ell\geq 3$，则

$$A(0,0)\leq\left\lceil\frac{p-1}{2\ell}\right\rceil-1$$

其中 $\lceil\cdot\rceil$ 表示大于或等于给定数的最小整数。

在我们的情形中，$\frac{p-1}{\ell}=|L|$，且 $|L|$ 为偶数，因为 $-1\in L$。因此，由引理 4.6 可得

$$A(0,0)\leq\frac{|L|}{2}-1.$$

我们采用与分圆数不同的方法研究 $1+L$ 中平方数的数量。记 $\left(\frac{\cdot}{p}\right)$ 的勒让德符号为

$$\left(\frac{x}{p}\right)=x^{\frac{p-1}{2}}=\begin{cases}0 & \text{if } x=0;\\ 1 & \text{if } x\neq 0 \text{ is a square;}\\ -1 & \text{if } x\neq 0 \text{ is not a square,}\end{cases}$$

对于 $x\in\mathbb{Z}_p$。那么，当且仅当 $\left(\frac{x}{p}\right)=0$，1 时，$x$ 是 $\mathbb{Z}_p$ 中的一个平方。因此，对于每个 x、$y\in\mathbb{Z}_p$，集合 $\{x,y,xy\}$ 中至少包含一个平方，这是由于乘法

$$\left(\frac{x}{p}\right)\cdot\left(\frac{y}{p}\right)=\left(\frac{xy}{p}\right)$$

成立（另见 [Bur11，第 9] 章）。我们得出以下结论。

引理 4.7. 若 $x,y\in\mathbb{Z}_p$ 且 $xy\neq 0$，则

$$\frac{1}{2}\left(1+\left(\frac{x}{p}\right)\right)+\frac{1}{2}\left(1+\left(\frac{y}{p}\right)\right)+\frac{1}{2}\left(1+\left(\frac{xy}{p}\right)\right)\geq 1.$$

我们得到 $1+\mathrm{L}$ 中平方数的数量下界如下。

引理 4.8。$1+\mathrm{L}$ 的平方数的数量大于 $\frac{1}{4}|\mathrm{L}|$。

证明。设 $\mathrm{m}=|1+\mathrm{L}|=|\mathrm{L}|$，并设 α 是 L 的一个生成元。整数 m 是偶数，因为 $-1\in\mathrm{L}$。此外，$\alpha^{\frac{m}{2}}=-1$。记 M 为 $1+\mathrm{L}$ 的平方数的数量。于是

$$M=1+\sum_{\substack{i=0,\\ i\neq\frac{m}{2}}}^{m-1}\frac{1}{2}\left(1+\left(\frac{1+\alpha^i}{p}\right)\right)$$

其中开头的 1 对应于 $1+\alpha^{\frac{m}{2}}=0$。由于 $-1\in\mathrm{L}$，$1+\mathrm{L}=1-\mathrm{L}$，并且我们还有

$$M=1+\sum_{i=1}^{m-1}\frac{1}{2}\left(1+\left(\frac{1-\alpha^i}{p}\right)\right)$$

其中开头的 1 对应于 $1-\alpha^0=0$。

对于每个 $\mathrm{i}=0$、1、.....、$\mathrm{m}-1$，集合 $\{1+\alpha^i,1-\alpha^i,1-\alpha^{2i}\}$ 必须至少包含一个平方数，因为 $(1+\alpha^i)(1-\alpha^i)=1-\alpha^{2i}$。由引理 4.7，

$$\sum_{\substack{i=1,\\ i\neq\frac{m}{2}}}^{m-1}\frac{1}{2}\left(1+\left(\frac{1+\alpha^i}{p}\right)\right)+\frac{1}{2}\left(1+\left(\frac{1-\alpha^i}{p}\right)\right)+\frac{1}{2}\left(1+\left(\frac{1-\alpha^{2i}}{p}\right)\right)\geq m-2.$$

$\frac{1}{2}\left(1+\left(\frac{1+\alpha^i}{p}\right)\right)$和 $\frac{1}{2}\left(1+\left(\frac{1-\alpha^i}{p}\right)\right)$的前两个和是 $\mathrm{M}-1$的部分和，其项均为非负数。因此，$2(\mathrm{M}-1)+\mathrm{M}'\geq\mathrm{m}-2$其中

$$M'=\sum_{\substack{i=1,\\ i\neq\frac{m}{2}}}^{m-1}\frac{1}{2}\left(1+\left(\frac{1-\alpha^{2i}}{p}\right)\right).$$

注意，对于 $\mathrm{i}=1,\ldots,\frac{m}{2}-1$，都有 $\alpha^{2i}=\alpha^{2(\frac{m}{2}+i)}$。因此，

$$M'=2\sum_{i=1}^{\frac{m}{2}-1}\frac{1}{2}\left(1+\left(\frac{1-\alpha^{2i}}{p}\right)\right).$$

集合 $\{1-\alpha^{2i}\mid \mathrm{i}=1,\ldots,\frac{m}{2}-1\}$是 $1-\mathrm{L}$ 的子集，因此 M_2'是$\mathrm{M}-1$的部分和。我们得到 $\mathrm{M}'\leq 2(\mathrm{M}-1)$。因此，有 $4(\mathrm{M}-1)\geq\mathrm{m}-2$。于是，$\mathrm{M}\geq\frac{m}{4}+\frac{1}{2}$，如所需。□

现在我们可以证明下面的主定理。

定理 4.9. 设 p 为奇素数。若 $\ell=[\mathbb{Z}_p^\times:\langle-1,2\rangle]$ 是奇素数，则 $\mathrm{s}(\ell)\neq 0$。

证明。根据命题 4.4，$1+\mathrm{L}$ 的平方数的数量为 $12(1+\mathrm{A}(0,0)+\mathrm{s}(\ell))$。由引理 4.8，该数量大于 $\frac{1}{4}|\mathrm{L}|$，于是 $1+\mathrm{A}(0,0)+\mathrm{s}(\ell)>\frac{1}{2}|\mathrm{L}|$。根据引理 4.6 下方的内容，$1+\mathrm{A}(0,0)\leq\frac{1}{2}|\mathrm{L}|$。因此，$\mathrm{s}(\ell)>0$。□

定理 4.9 证明了当素数 p 满足 $[\mathbb{Z}_p^\times:\langle-1,2\rangle]$ 是素数时，猜想 B 成立。这也回答了关于此类素数的猜想 A。因此，我们得到以下推论。

推论 4.10. 设 p 是一个满足 $4 \nmid \mathrm{o}_p(2)$ 的奇素数。若 $\ell = [\mathbb{Z}_p^\times : \langle -1, 2\rangle]$ 是奇素数，则长度为 p、重量为 3 的最优冲突避免码的大小为

$$\frac{p-1-2\ell}{4} + \left\lfloor \frac{\ell}{3} \right\rfloor.$$

例如，若 $\mathrm{p} = 1229241823 > 2^{30}$，则 $\mathrm{o}_p(2)$ 为奇数，且 $\ell = 18307$ 是一个素数。因此，我们可以轻易得出，长度为 p、重量为 3 的最优冲突避免码的大小为 307307404。事实上，可以验证，$\mathrm{A}(1, 2) = 4$，其中原根为 3。$(1 + 3\mathrm{L}) \cap 9\mathrm{L}$ 的一个元素是 $1 + 3 \cdot 2^{1128543547} = 9 \cdot 2^{249779730}$。

长度为 p^k、$\mathrm{k} \geq 1$ 的最优冲突避免码可以由长度为 p 的最优冲突避免码通过 [FLS14，定理 8] 构造。将推论 4.10 应用于 [FLS14，定理 8]，，可得以下结论。

推论 4.11. 设 $\mathrm{p} > 3$ 是满足 $4 \nmid \mathrm{o}_p(2)$ 的非 Wieferich 素数。若 $\ell = [\mathbb{Z}_p^\times : \langle -1, 2\rangle]$ 是奇素数，则长度为 p^k、重量为 3 的最优冲突避免码的大小为

$$\frac{p^k - 1 - 2k\ell}{4} + k \left\lfloor \frac{\ell}{3} \right\rfloor$$

对每个 $\mathrm{k} \in \mathbb{N}$ 均成立。

5. 结论

根据推论 3.3 和 4.10，我们现在知道，当 $4 \nmid \mathrm{o}_p(2)$ 且 $\ell = \left[\mathbb{Z}_p^\times : \langle -1, 2\rangle\right] = 4$ 或 ℓ 是奇素数时，长度为素数 p、重量为 3 的最优冲突避免码的大小。对于合数 $\ell \geq 6$，确定 $\mathrm{s}(\ell) \neq 0$ 是否成立并不容易。例如，设 $\ell = 6$，利用第 3 节给出的性质，扩展分圆矩阵可简化如下：

$$B = \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} & b_{0,4} & b_{0,5} \\ b_{0,1} & b_{0,5} & b_{1,2} & b_{1,3} & b_{1,4} & b_{1,2} \\ b_{0,2} & b_{1,2} & b_{0,4} & b_{1,4} & b_{2,4} & b_{1,3} \\ b_{0,3} & b_{1,3} & b_{1,4} & b_{0,3} & b_{1,3} & b_{1,4} \\ b_{0,4} & b_{1,4} & b_{2,4} & b_{1,3} & b_{0,2} & b_{1,2} \\ b_{0,5} & b_{1,2} & b_{1,3} & b_{1,4} & b_{1,2} & b_{0,1} \end{pmatrix}.$$

假设 $\mathrm{s}(6) = \mathrm{b1}, {}_2 + \mathrm{b5}, {}_4 = 0$。那么

$$B = \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} & b_{0,4} & b_{0,5} \\ b_{0,1} & b_{0,5} & 0 & b_{1,3} & b_{1,4} & 0 \\ b_{0,2} & 0 & b_{0,4} & b_{1,4} & b_{2,4} & b_{1,3} \\ b_{0,3} & b_{1,3} & b_{1,4} & b_{0,3} & b_{1,3} & b_{1,4} \\ b_{0,4} & b_{1,4} & b_{2,4} & b_{1,3} & b_{0,2} & 0 \\ b_{0,5} & 0 & b_{1,3} & b_{1,4} & 0 & b_{0,1} \end{pmatrix}.$$

由引理 3.1(iv)，我们将得到

$$\begin{cases} b_{0,0}+b_{0,2}+b_{0,3}+b_{0,4}=b_{1,3}+b_{1,4}, \\ b_{0,1}+b_{0,5}=b_{0,2}+b_{0,4}+b_{2,4}=2b_{0,3}+b_{1,3}+b_{1,4}, \\ b_{0,3}+b_{1,3}+b_{1,4}=\frac{|L|}{2}. \end{cases}$$

由此得到等式

$$b_{2,4}=b_{0,0}+3b_{0,3}.$$

另一方面，根据引理 4.2， $1+L$ 的平方数的数量为

$$\frac{1}{2}(b_{0,0}+b_{0,3}+2b_{2,4}).$$

由引理 4.8 可知，这个数量大于 $\frac{1}{4}|L|$，于是 $b_{0,0}+b_{0,3}+2b_{2,4}>\frac{1}{2}|L|$。利用上面的等式，我们得到 $3b_{0,0}+7b_{0,3}>\frac{1}{2}|L|$。然而，引理 4.7 中给出的 $b_{0,0}$ 上界（或 [BHKM13] 中给出的 $b_{0,3}$ 上界）在这种情况下无法提供更多信息。对于合数 $\ell\geq 6$，我们认为，寻找更小的分圆数上界或许能带来更好的方法。我们希望这些想法能为解决这个问题带来一些启发。

致谢

我们谨此感谢罗元勋教授向我们介绍 [FLS14] 。第一作者部分获得科技部补助金 110-2115-M-003-007-MY2 的资助。第二作者部分获得科技部补助金 111-2115-M-003-005 的资助。第三作者获得科技部补助金 111-2811-M-003-028 的资助。

参考文献

[AT20] M.H. Ahmed 和 J. Tanti。分圆数与雅可比和：综述。载于《数域类群及相关主题》，第 119–140 页。施普林格，新加坡，2020。doi:10.1007/978-981-15-1514-9_12.[ATP21] M.H. Ahmed、J. Tanti 和 S. Pushp。使用分圆矩阵的公钥密码系统。载于《编码理论——近期进展、新视角与应用》，第 86–132 页。IntechOpen，2021。doi:10.5772/intechopen.101105.[BHKM13]K. Betsumiya、M. Hirasaka、T. Komatsu 和 A. Munemasa。分圆数的上界。线性代数及其应用，438(1):111–120，2013。doi:10.1016/j.laa.2012.06.045.[Bur11] D.M. Burton。《初等数论》。麦格劳-希尔，纽约，2011.[Dic35a] L.E. Dickson。分圆理论与三项式同余。美国数学会会刊，37(3):363–380，1935。doi:10.1090/S0002-9947-1935-1501791-3.[Dic35b] L.E. Dickson。分圆理论、高次同余与华林问题。美国数学杂志，57(2):391–424，1935。doi:10.2307/2371217.[Dic35c] L.E. Dickson。当 e 为合数时的分圆理论。美国数学会会刊，38(2):187–200，1935。doi:10.1090/S0002-9947-1935-1501808-6.[FLM10] H.-L. Fu、Y.-H. Lin 和 M. Mishima。偶数长度、重量 3 的最优冲突避免码。IEEE 信息论汇刊，56(11):5747–5756，2010。doi:10.1109/TIT.2010.2069270。

[FLS14] H.-L. Fu、Y.-H. Lo 和 S.W. Shum。奇长度、重量三的最优冲突避免码。《设计、编码与密码学》，72(2):289–309，2014。doi:10.1007/s10623-012-9764-5.[Gau01] C.F. Gauss。《算术研究》。1801。Arthur A. Clarke 译并作序。William C. Waterhouse、Cornelius Greither 和 A. W. Grootendorst 修订，Waterhouse 作序。Springer-Verlag，纽约，1986。doi:10.1007/978-1-4939-7560-0.[GV93] L. Gy¨orfi 和 I. Vajda。无反馈多址碰撞信道协议序列的构造。IEEE 信息论汇刊，39(5):1762–1765，1993。doi:10.1109/18.259673.[HLS] L.-C. Hsia、H.-C. Li 和 W.-L. Sun。某些对角方程与素数长度冲突避免码。预印本。[JMJ+07] M. Jimbo、M. Mishima、S. Janiszewski、A.Y. Teymorian 和 V.D. Tonchev。关于长度为 n = 4 m、适用于三个活跃用户的冲突避免码。IEEE 信息论汇刊，53(8):2732–2742，2007。doi:10.1109/TIT.2007.901233.[Kat02] S.A. Katre。圆分问题。载于《数论研究新趋势》，第 59–72 页。Hindustan Book Agency，新德里，2002。doi:10.1007/978-93-86279-09-5_5.[Lev07] V.I. Levenshtein。冲突避免码与循环三元系。《信息传输问题》，43(3):199–212，2007。doi:10.1134/S0032946007030039.[LMSJ14] Y. Lin、M. Mishima、J. Satoh 和 M. Jimbo。奇长度、重量三的最优等差冲突避免码。《有限域及其应用》，26:49–68，2014。doi:10.1016/j.ffa.2013.11.001.[LT05] V.I. Levenshtein 和 V.D. Tonchev。适用于三个活跃用户的最优冲突避免码。IEEE 国际信息论研讨会论文集，第 535–537 页，2005。doi:10.1109/ISIT.2005.1523392.[LW75] P.A. Leonard 和 K.S. Williams。十一阶分圆数。《算术学报》，26(4):365–383，1975。doi:10.4064/aa-26-4-365-383.[Mat90] P. Mathys。适用于 n 个多址通信系统用户中的 t 个用户的一类码。IEEE 信息论汇刊，36(6):1206–1219，1990。doi:10.1109/18.59923.[MFU09] M. Mishima、H.-L. Fu 和 S. Uruno。长度 n ≡ 0 （模 16）、重量 3 的最优冲突避免码。《设计、编码与密码学》，52(3):275–291，2009。doi:10.1007/s10623-009-9282-2.[MM17] M. Mishima 和 K. Momihara。重量 3 的一类新型最优紧冲突避免码。《离散数学》，340(4):617–629，2017。doi:10.1016/j.disc.2016.12.003.[Mom07] K. Momihara。重量三的紧等差冲突避免码的充要条件。《设计、编码与密码学》，45(3):379–390，2007。doi:10.1007/s10623-007-9139-5.[MZS14] W. Ma、C. Zhao 和 D. Shen。奇长度、重量 3 的最优冲突避免码的新构造。《设计、编码与密码学》，73(3):791–804，2014。doi:10.1007/s10623-013-9827-2.[NGM92] Q.A. Nguyen、L. Gy¨orfi 和 J.L. Massey。二元恒重循环码与循环可置换码的构造。IEEE 信息论汇刊，38(3):940–949，1992。doi:10.1109/18.135636.[Raj80] A.R. Rajwade。分圆理论——综述文章。《数学学生》，48(1):70–115，1980。[TR02] B.S. Tsybakov 和 A.R. Rubinov。冲突避免码的若干构造。《信息传输问题》，38(4):268–279，2002。doi:10.1023/A:1022045812079.[WF13] S.-L. Wu 和 H.-L. Fu。长度为 n =$2^k \pm 1$、重量 3 的最优紧等差冲突避免码。《组合设计杂志》，21(6):223–231，2013。doi:10.1002/jcd.21332。

国立台湾师范大学数学系，台北 11677，台湾，中华民国

电子邮箱地址：hsia@math.ntnu.edu.tw

国立台湾师范大学数学系，台北 11677，台湾，中华民国

电子邮箱地址：li@math.ntnu.edu.tw

国立台湾师范大学数学系，台北 11677，台湾，中华民国

电子邮箱地址：wlsun@ntnu.edu.tw