

k 错线性复杂度具有第二下降点的 2^n 周期序列

戴小平, 毕松松, 王喜凤, 周建钦

(安徽工业大学计算机科学与技术学院, 安徽 马鞍山 243002)

摘 要: k 错线性复杂度度量伪随机序列的稳定性, 而关键错误线性复杂度分布能够对 k 错线性复杂度下降点进行描述。使用方体理论和筛选法研究 k 错线性复杂度具有第二下降点(关键点)的周期序列。通过分析错线性复杂度第一下降点 $k=4$ 且第二下降点 $k'=6$ 的 2^n 周期序列, 给出序列线性复杂度和第一下降点线性复杂度之间的约束条件, 得到第二下降点线性复杂度所有可能的取值形式。推导出在已知序列第一下降点线性复杂度和第二下降点线性复杂度情况下二元序列的计数公式。分析结果表明, 该方法可研究具有第三下降点(关键点)的周期序列。

关键词: k 错线性复杂度; 关键错误线性复杂度分布; 第二下降点; 方体理论; 筛选法

中文引用格式: 戴小平, 毕松松, 王喜凤, 等. k 错线性复杂度具有第二下降点的 2^n 周期序列[J]. 计算机工程, 2016, 42(1): 156-162.

英文引用格式: Dai Xiaoping, Bi Songsong, Wang Xifeng, et al. 2^n -periodic Sequences with Second Descent Point of k -error Linear Complexity[J]. Computer Engineering, 2016, 42(1): 156-162.

2^n -periodic Sequences with Second Descent Point of k -error Linear Complexity

DAI Xiaoping, BI Songsong, WANG Xifeng, ZHOU Jianqin

(School of Computer Science and Technology, Anhui University of Technology, Ma' anshan, Anhui 243002, China)

[Abstract] The k -error linear complexity is used as an important stability index of pseudorandom sequences, and the critical error linear complexity distribution characterize the descent point of k -error linear complexity. This paper studies the 2^n -periodic binary sequences that k -error linear complexity with second descent point (critical point) via cube theory and sieve method. By analyzing the k -error linear complexity with first descent point $k=4$ and second descent point $k'=6$, the relationship between linear complexity of sequences and linear complexity of the first descent point is established, being given the possible value forms of the first descent point linear complexity. It obtains the counting functions of periodic binary sequences when being given first descent point linear complexity and second descent point linear complexity. Analysis result shows that periodic binary sequences can be studied with third descent point (critical point) of k -error linear complexity by the same methods.

[Key words] k -error linear complexity; critical error linear complexity distribution; second descent point; cube theory; sieve method

DOI: 10.3969/j.issn.1000-3428.2016.01.028

1 概述

序列密码是现代密码学的一个重要分支, 研究高安全性的密码序列一直是密码学的核心工作之一。高安全性的序列 s 要求序列具有较大的线性复杂度 $L(s)$ 和稳定的 k 错线性复杂度 $L_k(s)$ 。 k 错线

性复杂度^[1]是指当序列改变一个周期中至多 k bit 时, 得到的所有序列中最小的线性复杂度。在对 k 错线性复杂度下降点的研究中, 文献[2]提出关键错误线性复杂度分布 CELCS 的概念, CELCS 是由有序的关键点 $(k, L_k(s))$ 组成的, 当 $k' > k$ 时, 会有 $L_k(s) < L_{k'}(s)$ 。也就是说, 线性复杂度只在关键点上

基金项目: 安徽省自然科学基金资助项目(1208085MF106); 安徽省教育厅自然科学基金资助项目(KY2013Z025); 安徽工业大学青年基金资助项目(QZ201412)。

作者简介: 戴小平(1958-), 男, 教授, 主研方向为信息安全、密码学; 毕松松, 硕士研究生; 王喜凤, 讲师、硕士; 周建钦, 教授。

收稿日期: 2014-12-15 **修回日期:** 2015-03-03 **E-mail:** xpdai@ahut.edu.cn

下降。

目前,国内外对关键错误线性复杂度分布的研究主要在 k 错线性复杂度具有第一下降点的情况。文献[3]引入最小误差:使得序列 s 的 k 错线性复杂度严格小于其线性复杂度的最小整数 k ,并给出了这样的 k 值。文献[4]研究了序列 k 错线性复杂度具有第一下降点 $k=4$ 的特征。针对 k 错线性复杂度分布领域的研究一般是使用离散傅里叶变换和用 Games-Chan 算法^[5]推导等一些纯数学的方法,而使用纯数学研究方法会使得研究非常受限^[6]。

本文进一步研究 k 错线性复杂度具有第二下降点的情况。通过使用方体理论和非纯数学的研究方法:筛选法,对 k 错线性复杂度具有第一下降点 $k=4$ 且第二下降点 $k'=6$ 的序列进行分析。本文主要工作如下:(1)给出序列线性复杂度与第一下降点线性复杂度的关系,并指出约束条件;(2)给出第二下降点线性复杂度所有可能的取值形式;(3)推导出给定第一下降点线性复杂度和第二下降点线性复杂度的时二元序列的精确计数公式。

2 预备知识

下文主要介绍方体理论和给出筛选法:

(1)方体理论基本内容,详细内容可参考文献[7-8]。

定义 1 周期为 2^n 的二元序列 s ,若 s 的两非零元素下标之差可表示为 $(2x+1)2^y$, ($x, y \in \mathbb{Z}^+$),则这两元素的距离为 2^y 且这两元素形成边的长度也为 2^y 。

定义 2 周期为 2^n 的二元序列 s ,设 s 有 2^m 个非零元素, $0 \leq i_1 < i_2 < \dots < i_m < n$,若 $m=1$,则序列 s 有 2 个非零元素且这 2 个非零元素形成一条边,边长为 2^{i_1} ,构成一个 1 方体。若 $m=2$,则 s 有 4 个非零元素且形成一个矩形,边长为 $2^{i_1}, 2^{i_2}$,构成一个 2 方体。一般而言,若 s 中有 2^{m-1} 个非零元素构成一个 $(m-1)$ 方体, s 中另外 2^{m-1} 个非零元素也构成一个 $(m-1)$ 方体,假设这 2^{m-1} 对元素之间的距离均为 2^{i_m} ,则这 2 个 $(m-1)$ 方体构成一个 m 方体, 2^{i_m} 为这 2 个 $(m-1)$ 方体的距离,并且序列 s 的线性复杂度为方体的线性复杂度。

引理 1 周期为 2^n 的二元序列 s ,若 s 的非零元素组成一个 m 方体,且其边长为 $2^{i_1}, 2^{i_2}, \dots, 2^{i_m}$, $0 \leq i_1 < i_2 < \dots < i_m < n$,则序列 s 的线性复杂度 $L(s) = 2^n - (2^{i_1} + 2^{i_2} + \dots + 2^{i_m})$ 。

如图 1 所示为一个 3 方体,其边长为 1, 2, 4, 其线性复杂度为 $2^n - (1 + 2 + 4)$ 。这个 3 方体可分解成 2 个边长为 1, 4 的 2 方体,且这 2 个 2 方体之间的距离为 2。

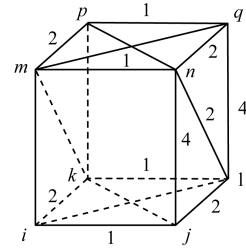


图 1 3 方体示意图

(2)筛选法的内容。

引理 2 周期为 2^n 的二元序列 s , s 的线性复杂度 $L(s) = 2^n$,当且仅当序列 s 的一个周期的非零元素的个数为奇数^[7-10]。

引理 3 周期为 2^n 线性复杂度为 L 的二元序列的个数^[7-8, 11-12]:

$$N(L) = \begin{cases} 1 & L=0 \\ 2^{L-1} & 1 \leq L \leq 2^n \end{cases}$$

引理 4 周期为 2^n 的二元序列 s , s 的线性复杂度 $L(s) = 2^n - (2^{i_1} + 2^{i_2} + \dots + 2^{i_m})$, $0 \leq i_1 < i_2 < \dots < i_m < n$ 线性复杂度第一下降点的 k 最小值 $k_{\min} = 2^m$ ^[3, 8]。

假设在二元有限域上有序列 $x = (x_1, x_2, \dots, x_n)$ 和 $y = (y_1, y_2, \dots, y_n)$, 定义 $x + y = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$, 其中, $+$ 为异或运算。

引理 5 周期为 2^n 的二元序列 s_1, s_2 , 若 $L(s_1) \neq L(s_2)$, 则 $L(s_1 + s_2) = \max\{L(s_1), L(s_2)\}$ 。若 $L(s_1) = L(s_2)$, 则 $L(s_1 + s_2) < L(s_1)$ ^[8, 12-13]。

下面给出筛选法^[11], 筛选法是第 3 节的证明采取的主要方法。

周期为 2^n 的二元序列 s , s 的 k 错线性复杂度 $L_k(s) = c$, 令 $s = t + e$, $L(t) = c$, e 是非零元素个数为 k 的序列。为研究满足 $L_k(s) = c$ 的序列, 构造如下框架: 设 $TE = \{t + e \mid t \in T, e \in E\}$, 其中, $t = \{t \mid L(t) = c\}$, $E = \{e \mid W_H(e) = k\}$ 。

为从 TE 中筛选出满足 $L_k(t + e) = c$ 的序列 $t + e$, 有 2 类序列需要从 TE 中排除, 第一类是 $t + e \in TE$, 但 $L_k(t + e) < c$ 。第二类是 $x + u, y + v \in TE$, 并且 $L_k(x + u) = L_k(y + v) = c$, $x \neq y, u \neq v, W_H(u) = W_H(v) = k$, 但是 $x + u = y + v$ 。

对第一类的情况, 相当于存在 $v, W_H(v) = k$, 使得 $L_k(t + u) = L(t + u + v) < c$ 。因为 $L(t) = c$, 根据引理 5, 有 $L(u + v) = c$ 。即第一类的序列可以转化成检查是否存在 v , 使得 $L(u + v) = c$ 。对第二类的情况, 因 $x + u = y + v$, 根据异或运算规则, 有 $x + y = u + v$ 。因为 $L(x) = c, L(y) = c$, 根据引理 5, 有 $L(x + y) = c$, 从而有 $L(u + v) < c$ 。即第二类的序列就可以转化为检查是否存在 v , 使得 $L(u + v) < c$, 如果存在这样的 v , 进一步讨论 v 的个数。

3 具有第二下降点的 2^n 周期序列计数

使用方体理论和筛选法研究 k 错线性复杂度具有第一下降点 $k=4$ 且第二下降点 $k'=6$ 的序列,并给出结论。定理 1 得出序列线性复杂度与第一下降点线性复杂度的关系,定理 2 给出第二下降点线性复杂度所有可能的取值形式,定理 3 推导出满足第一下降点和第二下降点线性复杂度的二元序列计数公式。

定理 1 设 $s^{(n)}$ 是以 2^n 为周期的二元序列,且 $s^{(n)}$ 的线性复杂度 $L(s^{(n)}) < 2^n$, 则:

(1) $L_6(s^{(n)}) < L_4(s^{(n)}) < L(s^{(n)})$, $L(s^{(n)}) = L_2(s^{(n)}) = L_3(s^{(n)})$, $L_4(s^{(n)}) = L_5(s^{(n)})$, 当且仅当 $s^{(n)}$ 可以分解为若干方体 $c_0, c_1, c_2, \dots$, $L(c_0) > L(c_1) > L(c_2) > \dots$, 其中, c_0 是 2 方体; c_1 是 2 方体, 且 c_0 和 c_1 有 1 个非零元素重合。

(2) $L_6(s^{(n)}) < L_4(s^{(n)}) < L(s^{(n)})$, $L(s^{(n)}) = L_2(s^{(n)}) = L_3(s^{(n)})$, $L_4(s^{(n)}) = L_5(s^{(n)})$, 当且仅当 $L(s^{(n)}) = 2^n - (2^i + 2^j)$, $L_4(s^{(n)}) = 2^n - (2^p + 2^q)$, $0 < p < q < n$, $j < q$, $p \neq i, j$ 。

证明: (1) (必要性) 根据引理 4 知, 若 $s^{(n)}$ 是周期为 2^n 的二元序列, 其线性复杂度为 $L(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2} + \dots + 2^{i_m})$, $0 \leq i_1 < i_2 < \dots < i_m$, 使得 $L_k(s^{(n)}) < L(s^{(n)})$ 的最小 k 值 $k_{\min} = 2^m$ 。因为 c_0 是 2 方体, $L(s^{(n)}) = 2^n - (2^i + 2^j)$, 所以 $s^{(n)}$ 线性复杂度的第一下降点 $k=4$ 。 c_1 也是 2 方体, 设 c_0 的 4 个非零元素分别为 e_1, e_2, e_3, e_4 ; c_1 的 4 个非零元素分别为 e_5, e_6, e_7, e_8 。由于 c_0, c_1 存在 1 个元素重合, 不妨设重合元素为 e_4 和 e_8 , 此时 $e_4(e_8)$ 的位置是 0。当发生 4 错时, 去掉 c_0 的 e_1, e_2, e_3 , 在 e_4 位置添加 1, 此时 $e_5, e_6, e_7, e_8(e_4)$ 构成的方体 c_1 为当前最大的方体, 线性复杂度下降。当发生 6 错时, 若序列 $s^{(n)}$ 仅有 6 个非零元素, 只要消去这 6 个非零元素, 线性复杂度变为 0, 线性复杂度下降; 否则, 令 2^d 是集合 $\{D(e_i, e_j) \mid 5 \leq i, j \leq 8\}$ 中的最大值, $D(e_i, e_j)$ 是定义 1 中所定义的 e_i 与 e_j 的距离。不妨设 $D(e_5, e_8) = 2^d$, 在 e_8 位置添加 1, 消去 e_6, e_7 , 再添加 e_9, e_{10}, e_{11} , 可以使得 e_5, e_1, e_2, e_3 和 e_8, e_9, e_{10}, e_{11} 组成一个 3 方体 c , $L(c) = 2^n - (2^x + 2^y + 2^z)$, 且 $d \in (x, y, z)$ 。那么 c_3 至少是一个 3 方体, 线性复杂度下降。

充分性: 假设 c_0 是 2 方体且 c_1 是 0 方体, 当线性复杂度发生第二次下降最多只需要改变 5 个元素, 与第二下降点 $k=6$ 矛盾, 故该情况不存在。

假设 c_0 是 2 方体且 c_1 是 1 方体, 当 c_0, c_1 存在非零元素重合时, 发生第二次下降最多只需要改变 4 个元素, 与第二下降点 $k=6$ 矛盾; 当 c_0, c_1 不存在非零元素重合时, 该情况等价于 c_0 是 2 方体, c_1 是 2 方体, 且 c_0 和 c_1 有 1 个非零元素重合。但是当序

列 $s^{(n)}$ 的非零元素个数多于 6 个, 序列发生 4 错时, 仅仅消去 c_0 并不会使得此时的线性复杂度最小。设 $L(c_0) = 2^n - (2^i + 2^j)$, $L(c_1) = 2^n - 2^k$, $k > j > i$ 。下面构造当发生 4 错时, 更大的方体。设 c_0 的 4 个非零元素分别为 e_1, e_2, e_3, e_4 , c_1 的 2 个非零元素分别为 e_5, e_6 。在 c_0 的 4 个非零元素中, 不妨设 e_1 与 c_1 的距离最大, 即 $2^d = D(e_1, e_5) = D(e_1, e_6)$ 。消去 e_2, e_3, e_4 , 添加一个非零元素 e , 使得 e_5, e_6, e_1, e 构成一个 2 方体 c , 那么 $L(c) = 2^n - (2^k + 2^d) > 2^n - 2^k$ 。所以 c_1 必然是一个 2 方体。故 c_0 是 2 方体且 c_1 是 1 方体这种情况不存在。

假设 c_0 是 2 方体且 c_1 是 3 方体, 当 c_0, c_1 不存在非零元素重合时, 发生第二次下降最少需要改变 12 个元素, 与第二下降点 $k=6$ 矛盾; 当 c_0, c_1 存在非零元素重合时, 因第二下降点 $k=6$, 所以 c_0 和 c_1 有 3 个非零元素重合。由定义 2 知, c_1 可以由 2 个相同的 2 方体构成, 设这 2 个 2 方体为 c_2, c_3 , $L(c_2) = L(c_3) = 2^n - (2^x + 2^y)$, $0 \leq x < y$, 且 c_2, c_3 的距离为 2^z , $x < y < z$, 那么 $L(c_1) = 2^n - (2^x + 2^y + 2^z)$ 。令 c_2 的非零元素为 e_1, e_2, e_3, e_4 和 c_3 的非零元素为 e_5, e_6, e_7, e_8 , 如图 2 所示。下面讨论 c_0 和 c_1 中哪 3 个非零元素可以重合。因为 $L(c_0) > L(c_1)$, 那么 c_0 中有 2 个非零元素的距离 $2^d \geq 2^z$ 。不妨设重合的 3 个点为 e_2, e_7, e_8 , 如果 c_0 中的另外一个不与 c_1 重合的元素为 e , 根据方体理论有 $D(e_2, e_1) = D(e_3, e_1)$, $D(e_2, e_6) = D(e_3, e_6)$, $D(e_i, e_j)$ 是定义 1 中所定义的 e_i 与 e_j 的距离。那么 e_1, e_3, e_5, e_6 构成一个 2 方体; e_4, e 构成一个 1 方体, 即 c_0 是 2 方体且 c_1 是 3 方体, c_0 和 c_1 有 3 个非零元素重合的情况等价于 c_0 是 2 方体且 c_1 是 1 方体, c_0, c_1 不存在非零元素重合的情况。但是若序列 $s^{(n)}$ 的非零元素个数多于 6 个时, $s^{(n)}$ 的线性复杂度发生第二次下降, 需要改变的元素个数至少为 2^3 , 与第二下降点 $k=6$ 矛盾。故该情况不存在。

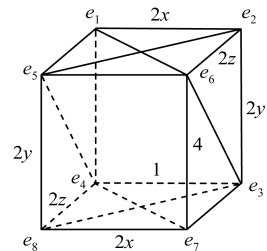


图 2 方体 c_2, c_3 的构成示意图

同理, 其他情况也不存在。

(2) 根据 (1) 的证明可知, $L_6(s^{(n)}) < L_4(s^{(n)}) < L(s^{(n)})$, $L(s^{(n)}) = L_2(s^{(n)}) = L_3(s^{(n)})$, $L_4(s^{(n)}) = L_5(s^{(n)})$, 当且仅当 $L(s^{(n)}) = 2^n - (2^i + 2^j)$, $L_4(s^{(n)}) = 2^n - (2^p + 2^q)$, $0 < p < q < n$ 。

证明 $j < q, p \neq i, j$ 的思想源自筛选法的第一类

的情况, 并构造如下框架: 设 $TE = \{t + e \mid t \in T, e \in E\}$, 其中 $T = \{t \mid L(t) = L = L_4(s^{(n)})\}$, $E = \{e \mid W_H(e) = 4\}$, 使用筛选法, 从 TE 中筛选出满足 $L_4(t + e) = L$ 的序列 $t + e$ 。现研究 $t + u \in TE$, 但 $L_4(t + u) < L = L_4(s^{(n)})$ 的情况。这种情况等价于检查是否存在 $v, v \in E$, 使得 $L(u + v) = L$ 。对于 $\forall u \in E$, 使得 $L_4(u) = L_4(s^{(n)})$ 。

(1) 证明 $j < q$ 。因为 c_0 是 2 方体, c_1 是 2 方体, $L(s^{(n)}) = 2^n - (2^i + 2^j)$, $L_4(s^{(n)}) = 2^n - (2^p + 2^q)$, 若要 $L_4(s^{(n)}) < L(s^{(n)})$, 则有 $j \leq q$ 。现在证明 $j \neq q$ 。假设 $n = 5, i = 0, j = 2, p = 1$ 时, 有 $u^{(4)} = \{1100 \ 1100 \ 0000 \ 0000\}$, 存在 $v^{(4)} = \{0000 \ 0000 \ 0110 \ 0110\}$, 使得 $L(u + v) = 2^4 - (2^1 + 2^2)$, 所以有 $L_4(t + u) < 2^4 - (2^1 + 2^2)$ 。因此 $j \neq q$, 进而 $j < q$ 。

(2) 证明 $p \neq i$ 。假设 $n = 4, i = 0, j = 2, q = 3$ 时有 $u^{(4)} = \{1100 \ 1100 \ 0000 \ 0000\}$, 存在 $v^{(4)} = \{0000 \ 1100 \ 1100 \ 0000\}$, 使得 $L(u + v) = 2^4 - (2^0 + 2^3)$, 所以有 $L_4(t + u) < 2^4 - (2^0 + 2^3)$ 。因此 $p \neq i$ 。

同理可证, $p \neq j$ 。

定理 2 设 $s^{(n)}$ 是以 2^n 为周期的二元序列, 若 $L_6(s^{(n)}) < L_4(s^{(n)}) < L(s^{(n)})$, $L(s^{(n)}) = L_2(s^{(n)}) = L_3(s^{(n)})$, $L_4(s^{(n)}) = L_5(s^{(n)})$ 且有 $L(s^{(n)}) = 2^n - (2^i + 2^j)$, $L_4(s^{(n)}) = 2^n - (2^p + 2^q)$, $0 < p < q < n$, $j < q, p \neq i, j$, 那么:

$$L_6(s^{(n)}) = \begin{cases} 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) & 0 \leq i_1 < i_2 < \cdots < i_m, m > 4 \\ 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3}) & \{i_1, i_2, i_3\} \neq \{i, p, q\} \\ \{i_1, i_2, i_3\} \neq \{j, p, q\}; \{i_1, i_2\} \neq \{i, j\} \end{cases}$$

证明: 证明思想源自筛选法中的第一类的情况, 并构造如下框架: 设 $TE = \{t + e \mid t \in T, e \in E\}$, 其中, $T = \{t \mid L(t) = L = L_6(s^{(n)})\}$, $E = \{e \mid W_H(e) = 6\}$, 使用筛选法, 从 TE 中筛选出满足 $L_6(t + e) = L$ 的序列 $t + e$ 。现研究 $t + u \in TE$, 但 $L_6(t + u) < L = L_6(s^{(n)})$ 的情况。这种情况等价于检查是否存在 $v, v \in E$, 使得 $L(u + v) = L$ 。对于 $\forall u \in E$, 有 $L_4(u) = L_4(s^{(n)})$, $L_6(u) = L_6(s^{(n)})$ 。

当 $L_6(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m})$, $0 \leq i_1 < i_2 < \cdots < i_m, m > 4$, $s^{(n)}$ 的 6 错线性复杂度序列有 2^m 个非零元素。关于 $L_k(t + u) < L$ 的情况, 相当于存在 v , 使得 $L(u + v) = L$, 因 $W_H(u) = 6, W_H(v) = 6$, 序列 $u + v$ 的非零元素最多为 12 个, 小于 2^m , 所以 $L(u + v) \neq L_6(s^{(n)})$, 即不存在这样的 v 。

当 $L_6(s^{(n)}) = 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3}) < 2^n - (2^p + 2^q)$ 时, 证明:

(1) $\{i_1, i_2, i_3\} \neq \{i, p, q\}$ 。假设 $n = 5, i = 1, j = 2, p = 3, q = 4$ 时, 有 $u^{(5)} = \{1010 \ 1010 \ 1000 \ 0000 \ 0000\}$, 存在 $v^{(5)} = \{0000 \ 1010 \ 0010 \ 0000$

$1010 \ 0000 \ 0010 \ 0000\}$, 使得 $L(u + v) = 2^5 - (2^1 + 2^3 + 2^4)$, 所以 $L_6(t + u) < 2^5 - (2^1 + 2^3 + 2^4)$, 因此 $\{i_1, i_2, i_3\} \neq \{i, p, q\}$ 。

(2) $\{i_1, i_2, i_3\} \neq \{j, p, q\}$ 。假设 $n = 5, i = 1, j = 2, p = 3, q = 4$ 时, $u^{(5)} = \{1010 \ 1010 \ 1000 \ 0000 \ 0000\}$, 存在 $v^{(5)} = \{0010 \ 00010 \ 0000 \ 1000 \ 1000 \ 1000 \ 0000 \ 1000\}$, 使得 $L(u + v) = 2^5 - (2^2 + 2^3 + 2^4)$, 所以 $L_6(t + u) < 2^5 - (2^2 + 2^3 + 2^4)$, 因此 $\{i_1, i_2, i_3\} \neq \{j, p, q\}$ 。

(3) $\{i_1, i_2\} \neq \{i, j\}$ 。假设 $n = 5, i = 1, j = 2, p = 3, q = 4$ 时, 有 $u^{(5)} = \{1010 \ 1010 \ 0100 \ 0000 \ 0000 \ 0000 \ 0100 \ 0000\}$, 存在 $v^{(5)} = \{0000 \ 0000 \ 1110 \ 1010 \ 0000 \ 0000 \ 0100 \ 0000\}$, 使得 $L(u + v) = 2^5 - (2^1 + 2^2 + 2^3)$, 所以有 $L_6(t + u) < 2^5 - (2^1 + 2^2 + 2^3)$, 因此 $\{i_1, i_2\} \neq \{i, j\}$ 。

定理 3 设 $s^{(n)}$ 是以 2^n 为周期的二元序列, 若:

(1) $L_6(s^{(n)}) < L_4(s^{(n)}) < L(s^{(n)})$, $L(s^{(n)}) = L_2(s^{(n)}) = L_3(s^{(n)})$, $L_4(s^{(n)}) = L_5(s^{(n)})$, 其中 $L(s^{(n)}) = 2^n - (2^i + 2^j)$, $L_4(s^{(n)}) = 2^n - (2^p + 2^q)$, $0 < p < q < n$, $j < q, p \neq i, j$, 且:

$$L_6(s^{(n)}) = \begin{cases} 2^n - (2^{i_1} + 2^{i_2} + \cdots + 2^{i_m}) & 0 \leq i_1 < i_2 < \cdots < i_m, m > 4 \\ 2^n - (2^{i_1} + 2^{i_2} + 2^{i_3}) & \{i_1, i_2, i_3\} \neq \{i, p, q\}; \\ \{i_1, i_2, i_3\} \neq \{j, p, q\}; \{i_1, i_2\} \neq \{i, j\} \end{cases}$$

那么, 满足条件的二元序列 $s^{(n)}$ 的个数为:

$$\left(\frac{2^{6n - (i + 2j + p + q) - 7}}{\gamma} \right) \times 2^{L-1} / (\theta \times 2^\delta \times 2^\varepsilon \times 64n - i_m - 1)$$

如果存在 i_0 , 使得 $2^n - (2^{i_0} + 2^q) < L$, $i_0 < q < n$ 且 $i_0 = i_{m-1} + 1$, 那么 $\theta = 2^{q-i_0}$; 否则, $\theta = 1$ 。

当 $i < j < p < q$, 可得 $\gamma, \delta, \varepsilon$ 的取值。 $\gamma = 1$ 。若 $2^n - (2^j + 2^p + 2^q) > L$, $\delta = 0$; 若 $2^n - (2^j + 2^p + 2^q) < L$, $\delta = 1$; 若 $2^n - (2^i + 2^p + 2^q) < L$, $\delta = 2$; 若 $2^n - (2^i + 2^j + 2^q) < L$, $\delta = 3$ 。若 $q = i_m$ 或 $2^n - (2^q + 2^{i_m}) > L$, $\varepsilon = 0$; 若 $2^n - (2^q + 2^{i_m}) < L$, $\varepsilon = 1$; 若 $2^n - (2^p + 2^{i_m}) < L$, $\varepsilon = 2$; 若 $2^n - (2^i + 2^j + 2^{i_m}) < L$, $\varepsilon = 3$; 若 $2^n - (2^j + 2^{i_m}) < L$, $\varepsilon = 4$; 若 $2^n - (2^i + 2^{i_m}) < L < 2^n - 2^{i_m}$, $\varepsilon = 5$ 。

当 $i < p < j < q$ 时, 可得 $\gamma, \delta, \varepsilon$ 的取值。 $\gamma = 2$ 。若 $2^n - (2^j + 2^p + 2^q) > L$, $\delta = 0$; 若 $2^n - (2^j + 2^p + 2^q) < L$, $\delta = 1$; 若 $2^n - (2^i + 2^j + 2^q) < L$, $\delta = 2$; 若 $2^n - (2^i + 2^p + 2^q) < L$, $\delta = 3$ 。若 $q = i_m$ 或 $2^n - (2^q + 2^{i_m}) > L$, $\varepsilon = 0$; 若 $2^n - (2^q + 2^{i_m}) < L$, $\varepsilon = 1$; 若 $2^n - (2^i + 2^j + 2^{i_m}) < L$, $\varepsilon = 2$; 若 $2^n - (2^j + 2^{i_m}) < L$, $\varepsilon = 3$; 若 $2^n - (2^p + 2^{i_m}) < L$, $\varepsilon = 4$; 若 $2^n - (2^i + 2^{i_m}) < L < 2^n - 2^{i_m}$, $\varepsilon = 5$ 。

当 $p < i < j < q$ 时, 可得 $\gamma, \delta, \varepsilon$ 的取值。 $\gamma = 4$ 。若 $2^n - (2^i + 2^j + 2^q) > L$, $\delta = 0$; 若 $2^n - (2^i + 2^j + 2^q) < L$, $\delta = 1$; 若 $2^n - (2^j + 2^p + 2^q) < L$, $\delta = 2$; 若 $2^n - (2^i$

$+2^p + 2^q) < L, \delta = 3$ 。若 $q = i_m$ 或 $2^n - (2^q + 2^{i_m}) > L, \varepsilon = 0$; 若 $2^n - (2^q + 2^{i_m}) < L, \varepsilon = 1$; 若 $2^n - (2^i + 2^j + 2^{i_m}) < L, \varepsilon = 2$; 若 $2^n - (2^j + 2^{i_m}) < L, \varepsilon = 3$; 若 $2^n - (2^i + 2^{i_m}) < L, \varepsilon = 4$; 若 $2^n - (2^p + 2^{i_m}) < L < 2^n - 2^{i_m}, \varepsilon = 5$ 。

(2) 如果 $L_6(s^{(n)}) = 0$, 以周期为 2^n 的二元序列 $s^{(n)}$ 的个数为: $2^{6n - (i+2j+p+q) - 7} / \gamma$ 。当 $i < j < p < q$ 时, $\gamma = 1$; 当 $i < p < j < q$ 时, $\gamma = 2$; 当 $p < i < j < q$ 时, $\gamma = 4$ 。

证明: 设 $TE = \{t + e | t \in T, e \in E\}, T = \{t | L(t) = L\}, E = \{e | W_H(e) = 6\}$, 其中 t 的线性复杂度为 $L(t) = 2^n - (2^{i_1} + 2^{i_2} + \dots + 2^{i_m})$, 并且 $L_4(e) = 2^n - (2^p + 2^q)$ 。使用筛选法, 从 TE 中筛选出 $L_6(t + e) = L$ 的序列 $t + e$ 。

1) 由引理 3 可知, 当 $L(t) = L$ 时, 若 $1 \leq L \leq 2^n$, 周期为 2^n 的二元序列的 t 个数为 2^{L-1} ; 否则, t 的个数为 1。

2) 下面求出 e 的个数, $W_H(e) = 6, L_4(e) = 2^n - (2^p + 2^q)$ 。

设 $s^{(i)}$ 是以 2^i 为周期的二元序列, 若 $L(s^{(i)}) = 2^i$ 且 $W_H(s^{(i)}) = 1$, 那么序列 $s^{(i)}$ 的个数是 2^i 。将周期翻倍变成 2^{i+1} , 若线性复杂度为 $2^{i+1} - 2^i = 2^i$, $W_H(s^{(i)}) = 2$, 那么 $s^{(i+1)}$ 的个数为 2^i 。若 $j > i$, 将周期变为 2^j , 序列 $s^{(j)}$ 的个数为 $(2^2)j - i - 1 \times 2^i = 2^{2j-i-2}$ 。若周期翻倍变为 2^{j+1} , 线性复杂度为 $2^{j+1} - (2^i + 2^j)$, $W_H(s^{(j+1)}) = 4$ 的个数也是 2^{2j-i-2} 。假设 $s^{(j+1)}$ 的 4 个非零元素分别为 p_1, p_2, p_3, p_4 , 并且这 4 个点构成一个 2 方体。

当 $i < j < p < q$ 时, 将周期变为 2^p 时, p_1, p_2, p_3, p_4 之间的距离不需要改变, $s^{(p)}$ 个数为 $(2^4)p - j - 1 \times (2^2)2j - i - 1 = 2^{4p-2j-i-6}$ 。此时将周期 2^p 翻倍变成 2^{p+1} , 并添加一个非零元素 p_5 , 由于 p_1, p_2, p_3, p_4 已经构成一个 2 方体, 那么有 4 种选择使得 p_5 与方体的距离为 2^p 。不妨选择 p_1 使得与 p_5 的距离为 2^p , 那么 p_2, p_3, p_4 的位置共有 2^3 种选择。 $s^{(p+1)}$ 的个数为 $4 \times 2^3 \times 2^{4p-2j-i-6} = 2^{4p-2j-i-1}$ 。将周期变为 2^q 时, 那么 p_1, p_2, p_3, p_4, p_5 的距离并不需要改变, $s^{(q)}$ 个数为 $(2^5)q - p - 1 \times 2^{4p-2j-i-1} = 2^{5q-p-2j-i-6}$ 。此时将周期 2^q 翻倍变成 2^{q+1} , 并添加一个非零元素 p_6, p_6 或与 p_1 , 或与 p_5 的距离为 q , 有 2 种选择, 其余元素有 2^4 种选择。 $s^{(q+1)}$ 的个数为 $2 \times 2^4 \times 2^{5q-p-2j-i-6} = 2^{5q-p-2j-i-1}$ 。

当 $i < p < j < q$ 时, 添加一个 $2^{p+1} - 2^p$ 的 1 方体。则 p_5, p_6 或与 p_2 , 或与 p_3 的距离为 2^p , 其余元素有 2^3 种选择, 则 $s^{(p+1)}$ 的个数为 $2 \times 2^3 \times 2^{4p-2j-i-6} = 2^{4p-2j-i-2}$ 。同理当周期变成 $q+1$ 时, $s^{(q+1)}$ 的个数 $2^{5q-p-2j-i-2}$ 。

当 $p < i < j < q$ 时, 添加一个 $2^{p+1} - 2^p$ 的 1 方体。

那么 $s^{(p+1)}$ 的个数为 $2^3 \times 2^{4p-2j-i-6} = 2^{4p-2j-i-3}$ 。同理当周期变成 $q+1$ 时, $s^{(q+1)}$ 的个数 $2^{5q-p-2j-i-3}$ 。

所以, 满足条件 $W_H(e) = 6, L_4(e) = 2^n - (2^p + 2^q)$ 的二元序列 e 的个数为:

$$\frac{2^{5q-p-2j-i-1}}{\gamma} \times (2^6)n - q - 1 = 2^{6n-(i+2j+p+q)-7} / \gamma$$

其中, 当 $i < j < p < q$ 时, $\gamma = 1$; 当 $i < p < j < q$ 时, $\gamma = 2$; 当 $p < i < j < q$ 时, $\gamma = 4$ 。

下面给出实例证明:

① 当 $i < j < p < q$ 时, $\gamma = 1$ 。假设 $n = 4, i = 0, j = 1, p = 2, q = 3$ 时, 有 $u^{(4)} = \{1001\ 1100\ 0000\ 0010\}$, 只能来自于序列 $v_1(4) = \{1000\ 1000\ 1000\ 1000\}$, 并且 $L_4(v_1(4)) = 2^4 - (2^2 + 2^3)$ 。

② 当 $i < p < j < q$ 时, $\gamma = 2$ 。假设 $n = 4, i = 0, j = 2, p = 1, q = 3$ 时, 有 $u^{(4)} = \{1001\ 1011\ 0000\ 0010\}$, 只能来自于序列 $v_1(4) = \{0000\ 1010\ 0000\ 1010\}, v_2(4) = \{1000\ 0010\ 1000\ 0010\}$, 并且 $L_4(v_1(4)) = L_4(v_2(4)) = 2^4 - (2^1 + 2^3)$ 。

③ 当 $p < i < j < q$ 时, $\gamma = 4$ 。假设 $n = 4, i = 1, j = 2, p = 0, q = 3$ 时, 有 $u^{(4)} = \{1001\ 1010\ 0011\ 0000\}$, 只能来自于序列 $v_1(4) = \{0001\ 0010\ 0001\ 0010\}, v_2(4) = \{0001\ 1000\ 0001\ 1000\}, v_3(4) = \{0011\ 0000\ 0011\ 0000\}, v_4(4) = \{1001\ 0000\ 1001\ 0000\}$, 并且 $L_4(v_1(4)) = \dots = L_4(v_4(4)) = 2^4 - (2^0 + 2^3)$ 。

3) 上述已分别求得 t 和 e 的个数。当 $L(t) = 0$ 时, $t + e$ 的个数为 $2^{6n-(i+2j+p+q)-7} / \gamma$, (2) 得证; 当 $L(t) > 0$ 时, $t + e$ 的个数小于 $2^{6n-(i+2j+p+q)-7} / \gamma$, 因为此时 $t + e$ 的个数存在重复情况, 即存在这种情况: $s + u, t + v \in TE, L_6(s + u) = L_6(t + v) = L$, 其中 $s \neq t, u \neq v$, 但 $s + u = t + v$ 。排除重复序列的思想源自筛选法第 2 类的情况, 需要检查是否存在这样的 v , 使得 $L(u + v) = L(s + t) < L$, 以及这时 v 的个数。其中, $W_H(u) = W_H(v) = 6, L_4(u) = L_4(v) = 2^n - (2^p + 2^q)$ 。下面考虑 2 种情况:

① 与 i, j, i_0 有关

定理 2 已证得, $L_6(s^{(n)})$ 不存在形如 $2^n - 2^{i_m}, 2^n - (2^{i_0} + 2^q), i_0 < q < n$, 和部分 $2^n - (2^{i_1} + 2^{i_2} + 2^{i_3})$ 的形式。并且将在这些使得 $L_6(s^{(n)})$ 不连续处取 L 的值。

当 $p < i < j < q$ 时, 对于 $\forall u \in E$, 若 $2^n - (2^{i_0} + 2^q) < L, i_0 < q < n$ 且 $i_0 = i_{m-1} + 1$, 存在 $2^{q-i_0} - 1$ 个 $v, \theta = 2^{q-i_0}$, 使得 $L(u + v) < L$ 。对于 $\forall u \in E$, 使得满足 $L(u + v) < L$ 中的 v 的个数和 δ 值满足以下结论: 若 $L(u + v) = 2^n - (2^i + 2^j + 2^q) < L$, 存在 1 个 v , 此时 $\delta = 1$; 若 $L(u + v) = 2^n - (2^j + 2^p + 2^q) < L$, 存在 3 个 v , 此时 $\delta = 2$; 若 $L(u + v) = 2^n - (2^i + 2^p + 2^q) < L$, 存在 7 个 v , 此时 $\delta = 3$; 若同时满足 $2^n - (2^{i_0} + 2^q) < L$ 和 $2^n - (2^{i_1} + 2^{i_2} + 2^{i_3}) < L$ 这 2 种情况时, v

的个数为 $2^{q-i_0} \times 2^\delta - 1$ 。

给出例子说明: 假设 $n = 5, i = 2, j = 3, p = 1, q = 4$, 有序列:

$$u^{(5)} = \{1010\ 1000\ 1000\ 1000\ 0010\ 0000\ 0000\ 0000\}$$

满足 $2^n - (2^i + 2^j + 2^q) = 4 < L$ 的 v 的总个数有 1 个:

$$v_1(5) = \{0010\ 0000\ 0000\ 0000\ 1010\ 1000\ 1000\ 1000\}$$

满足 $2^n - (2^j + 2^p + 2^q) = 6 < L$ 的 v 的总个数有 3 个:

$$v_2(5) = \{0000\ 1000\ 0010\ 1000\ 1000\ 0000\ 1010\ 0000\}$$

$$v_3(5) = \{1000\ 0000\ 1010\ 0000\ 0000\ 1000\ 0010\ 1000\}$$

满足 $2^n - (2^j + 2^q) = 8 < L$ 的 v 的总个数有 7 个。其中满足 $2^5 - (2^3 + 2^4) = 8 < L$ 的个数 2^{4-3} ; 满足 $2^n - (2^j + 2^p + 2^q) = 6 < L$ 时的 $\delta = 2$ 。所以 v 的个数共为 $2^{4-3} \times 2^2 - 1 = 7$:

$$v_4(5) = \{0000\ 0000\ 0010\ 0000\ 1000\ 1000\ 1010\ 1000\}$$

$$v_5(5) = \{0010\ 1000\ 0000\ 1000\ 1010\ 0000\ 1000\ 0000\}$$

$$v_6(5) = \{1000\ 1000\ 1010\ 1000\ 0000\ 0000\ 0010\ 0000\}$$

$$v_7(5) = \{1010\ 0000\ 1000\ 0000\ 0010\ 1000\ 0000\ 1000\}$$

满足 $2^n - (2^i + 2^p + 2^q) = 10 < L$ 的 v 的总个数有 15 个。其中满足 $2^5 - (2^3 + 2^4) = 8 < L$ 的个数 2^{4-3} ; 满足 $2^n - (2^i + 2^p + 2^q) = 10 < L$ 时的 $\delta = 3$ 。所以 v 的个数共为 $2^{4-3} \times 2^3 - 1 = 7$:

$$v_8(5) = \{0000\ 0000\ 1000\ 1010\ 1000\ 1000\ 0000\ 0010\}$$

$$v_9(5) = \{0000\ 0010\ 1000\ 1000\ 1000\ 1010\ 0000\ 0000\}$$

$$v_{10}(5) = \{0000\ 1000\ 1000\ 0010\ 1000\ 0000\ 0000\ 1010\}$$

$$v_{11}(5) = \{0000\ 1010\ 1000\ 0000\ 1000\ 0010\ 0000\ 1000\}$$

$$v_{12}(5) = \{1000\ 0000\ 0000\ 1010\ 0000\ 1000\ 1000\ 0010\}$$

$$v_{13}(5) = \{1000\ 0010\ 0000\ 1000\ 0000\ 1010\ 1000\ 0000\}$$

$$v_{14}(5) = \{1000\ 1000\ 0000\ 0010\ 0000\ 0000\ 1000\ 1010\}$$

$$v_{15}(5) = \{1000\ 1010\ 0000\ 0000\ 0000\ 0010\ 1000\ 1000\}$$

同理得到:

当 $i < j < p < q$ 时, 对于 $\forall u \in E$, 若 $2^n - (2^{i_0} + 2^q) < L, i_0 < q < n$ 且 $i_0 = i_{m-1} + 1$, 存在 $2^{q-i_0} - 1$ 个 $v, \theta = 2^{q-i_0}$, 使得 $L(u+v) < L$ 。对于 $\forall u \in E$, 使得满足 $L(u+v) < L$ 中的 v 的个数和 δ 值满足以下结论: 若 $L(u+v) = 2^n - (2^j + 2^p + 2^q) < L$, 存在 1 个 v , 此时 $\delta = 1$; 若 $L(u+v) = 2^n - (2^i + 2^p + 2^q) < L$, 存在 3 个 v , 此时 $\delta = 2$; 若 $L(u+v) = 2^n - (2^i + 2^j + 2^q) < L$, 存在 7 个 v , 此时 $\delta = 3$; 若 L 同时满足 $2^n - (2^{i_0} + 2^q) < L$ 和 $2^n - (2^{i_1} + 2^{i_2} + 2^{i_3}) < L$ 这 2 种情况时, v 的个数为 $2^{q-i_0} \times 2^\delta - 1$ 。

当 $i < p < j < q$ 时, 对于 $\forall u \in E$, 若 $2^n - (2^{i_0} + 2^q) < L, i_0 < q < n$ 且 $i_0 = i_{m-1} + 1$, 存在 $2^{q-i_0} - 1$ 个 $v, \theta = 2^{q-i_0}$, 使得 $L(u+v) < L$ 。对于 $\forall u \in E$, 使得满足 $L(u+v) < L$ 中的 v 的个数和 δ 值满足以下结论: 若 $L(u+v) = 2^n - (2^j + 2^p + 2^q) < L$, 存在 1 个 v , 此时 $\delta = 1$; 若 $L(u+v) = 2^n - (2^i + 2^j + 2^q) < L$, 存在

3 个 v , 此时 $\delta = 2$; $L(u+v) = 2^n - (2^i + 2^p + 2^q) < L$, 存在 7 个 v , 此时 $\delta = 3$; 若 L 同时满足 $2^n - (2^{i_0} + 2^q) < L$ 和 $2^n - (2^{i_1} + 2^{i_2} + 2^{i_3}) < L$ 这 2 种情况时, v 的个数为 $2^{q-i_0} \times 2^\delta - 1$ 。

②与 $i_m < w < n$ 有关

对于 $i_m < w < n$, 存在 $63 \times (2^6)w - i_m - 1$ 个序列 v , 使得 $L(u+v) = 2^n - (2^q + 2^w) < L$ 或 $L(u+v) = 2^n - (2^i + 2^j + 2^w) < L$ 或 $L(u+v) = 2^n - (2^j + 2^w) < L$ 或 $L(u+v) = 2^n - (2^i + 2^w) < L$ 或 $L(u+v) = 2^n - (2^p + 2^w) < L$ 或 $L(u+v) = 2^n - 2^w < L$ 。

对于满足任意条件的 v , 若 v 的周期加倍, 一个原序列将会产生 2^6 个新序列。因此, 存在 $63 + 63 \times 2^6 + \dots + 63 \times (2^6)n - i_m - 2 = (2^6)n - i_m - 1$ 个序列 v , 使得 $L(u+v) < L$ 。

例如: 当 $p < i < j < q$ 时, 假设存在 $n = 5, i = 1, j = 2, p = 0, q = 3, i_1 = 0, i_2 = 1, i_3 = 2, i_4 = 3, w = 4$, 有:

$$u^{(5)} = \{1110\ 1010\ 0100\ 0000\ 0000\ 0000\ 0000\ 0000\}$$

存在:

$$v_1(5) = \{1010\ 1010\ 0000\ 0000\ 0100\ 0000\ 0100\ 0000\}$$

使得:

$$L(u^{(5)} + v_1(5)) = 2^n - (2^q + 2^w) = 2^5 - (2^3 + 2^4)$$

$$v_2(5) = \{0000\ 0000\ 0000\ 0000\ 1110\ 1010\ 0100\ 0000\}$$

$$v_3(5) = \{0100\ 0000\ 0100\ 0000\ 1010\ 1010\ 0000\ 0000\}$$

使得:

$$L(u^{(5)} + v_2(5)) = L(u^{(5)} + v_3(5)) = 2^n - (2^i + 2^j + 2^w) = 2^5 - (2^1 + 2^2 + 2^4)。$$

$$v_4(5) = \{0010\ 0010\ 0000\ 0000\ 1100\ 1000\ 0100\ 0000\}$$

$$v_5(5) = \{0110\ 0010\ 0100\ 0000\ 1000\ 1000\ 0000\ 0000\}$$

$$v_6(5) = \{1000\ 1000\ 0000\ 0000\ 0110\ 0010\ 0100\ 0000\}$$

$$v_7(5) = \{1100\ 1000\ 0100\ 0000\ 0010\ 0010\ 0000\ 0000\}$$

使得:

$$L(u^{(5)} + v_4(5)) = \dots = L(u^{(5)} + v_7(5)) = 2^n - (2^j + 2^w) = 2^5 - (2^2 + 2^4)$$

$$v_8(5) = \{0000\ 1010\ 0000\ 0000\ 1110\ 0000\ 0100\ 0000\}$$

$\vdots$

$$v_{15}(5) = \{1110\ 0000\ 0100\ 0000\ 0000\ 1010\ 0000\ 0000\}$$

使得:

$$L(u^{(5)} + v_8(5)) = \dots = L(u^{(5)} + v_{15}(5)) = 2^n - (2^i + 2^w) = 2^5 - (2^1 + 2^4)$$

$$v_{16}(5) = \{0000\ 0010\ 0100\ 0000\ 1110\ 1000\ 0000\ 0000\}$$

$\vdots$

$$v_{31}(5) = \{1110\ 1000\ 0000\ 0000\ 0000\ 0010\ 0100\ 0000\}$$

使得:

$$L(u^{(5)} + v_{16}(5)) = \dots = L(u^{(5)} + v_{31}(5)) = 2^n - (2^p + 2^w) = 2^5 - (2^0 + 2^4)$$

$$v_{32}(5) = \{0000\ 0000\ 0100\ 0000\ 1110\ 1010\ 0000\ 0000\}$$

$\vdots$

$$v_{63}(5) = \{1110\ 1010\ 0000\ 0000\ 0000\ 0000\ 0100\ 0000\}$$

使得:

$$L(u^{(5)} + v_{32}(5)) = \dots = L(u^{(5)} + v_{63}(5)) = 2^n - 2^w = 2^5 - 2^4$$

由以上可知,在 $p < i < j < q$ 情况下,若 $q < i_m$:

当 $2^n - (2^q + 2^{i_m}) < L$, v 的个数增加 $(2^6)n - i_m - 1, \varepsilon = 1$ 。

当 $2^n - (2^i + 2^j + 2^{i_m}) < L$ 并且 $2^n - (2^j + 2^{i_m}) > L$, v 的个数增加 $3 \times (2^6)n - i_m - 1, \varepsilon = 2$ 。

当 $2^n - (2^j + 2^{i_m}) < L$ 并且 $2^n - (2^i + 2^{i_m}) > L$, v 的个数增加 $7 \times (2^6)n - i_m - 1, \varepsilon = 3$ 。

当 $2^n - (2^i + 2^{i_m}) < L$ 并且 $2^n - (2^p + 2^{i_m}) > L$, v 的个数增加 $15 \times (2^6)n - i_m - 1, \varepsilon = 4$ 。

当 $2^n - (2^p + 2^{i_m}) < L$ 并且 $2^n - 2^{i_m} > L$, v 的个数增加 $31 \times (2^6)n - i_m - 1, \varepsilon = 5$ 。

同理可得:在 $i < j < p < q$ 和 $i < p < j < q$ 情况下,当 $q < i_m$ 时, ε 的取值。

综上所述,定理 3 得证。

下面给出 2 个不同的示例,并通过计算机编程得到的数据佐证定理 3 的结论。

例 1 若 $n = 5, i = 2, j = 3, p = 1, q = 4, i_1 = 0, i_2 = 1, i_m = 4$, 那么 $L = 2^5 - (2^0 + 2^1 + 2^4) = 13$ 。当 $q = 4$ 时, $i_2 + 1 = 2 < q$, 存在 $i_0 = 2$, 从而 $\theta = 2^2$ 。因为 $p < i < j < q$, 所以 $\gamma = 4$; 又因为 $2^n - (2^i + 2^p + 2^q) < L$, $\delta = 3$; 在本例中 $q = i_m$, 故 $\varepsilon = 0$ 。由此得出, 满足 $L(s^{(n)}) = 20, L_4(s^{(n)}) = 14, L_6(s^{(n)}) = 13$ 的以 2^5 为周期的二元序列 $s^{(n)}$ 的个数为:

$$\frac{2^{30 - (2 + 6 + 1 + 4) - 7}}{4} \times 2^{13 - 1} = 2^{15}$$

例 2 若 $n = 5, i = 0, j = 2, p = 1, q = 3, i_1 = 1, i_2 = 2, i_m = 4$, 那么 $L = 2^5 - (2^1 + 2^2 + 2^4) = 10$ 。当 $q = 3$ 时, $i_2 + 1 = 3$, 不存在这样的 i_0 , 从而 $\theta = 1$ 。因为 $i < p < j < q$, 所以 $\gamma = 2$; 又因为 $2^5 - (2^j + 2^p + 2^q) = 18 > L, \delta = 0$; 在本例中 $q < i_m, 2^n - (2^q + 2^{i_m}) = 8 < L$, 所以 $\varepsilon = 1$ 。由此得出, 满足 $L(s^{(n)}) = 27, L_4(s^{(n)}) = 22, L_6(s^{(n)}) = 10$ 的以 2^5 为周期的二元序列 $s^{(n)}$ 的个数为:

$$\frac{2^{30 - (0 + 4 + 1 + 3) - 7} \times 2^{10 - 1}}{2 \times (2^0 \times 2^0 \times 2^1 \times 645 - 4 - 1)} = 2^{22}$$

4 结束语

本文基于方体理论和筛选法,研究了 k 错线性复杂度具有第一下降点 $k = 4$ 且第二下降点 $k' = 6$ 的

2^n 周期序列的若干性质。研究的二元序列在进行方体分解时,第一个方体为一个 2 方体,所以对于其他第一个方体为 2 方体的二元序列,也可采用本文的方法进行研究,如线性复杂度第一下降点 $k = 4$ 且第二下降点 $k' = 8$ 的情况。下一步将使用方体理论和筛选法研究线性复杂度具有第三下降点的情况,进一步完善关键错误线性复杂度。

参考文献

- [1] Stamp M, Martin C F. An Algorithm for the k -error Linear Complexity of Binary Sequences with Period 2^n [J]. IEEE Transactions on Information Theory, 1993, 39(1): 1398-1401.
- [2] Etzion T, Kolokotronis N, Limniotis K, et al. Properties of the Error Linear Complexity Spectrum [J]. IEEE Transactions on Information Theory, 2009, 55(10): 4681-4686.
- [3] Kurosawa K, Sato F, Sakata T. A Relationship Between Linear Complexity and k -error Linear Complexity [J]. IEEE Transactions on Information Theory, 2000, 46(2): 694-698.
- [4] 皮飞, 戚文峰. 二元周期序列的 4 错线性复杂度 [J]. 电子学报, 2011, 39(12): 2914-2920.
- [5] Games R A, Chan A H. A Fast Algorithm for Determining the Complex of a Binary Sequence with Period 2^n [J]. IEEE Transactions on Information Theory, 1983, 29(1): 144-146.
- [6] 谭琳. 伪随机序列的 k 错线性复杂度研究 [D]. 郑州: 解放军信息工程大学, 2012.
- [7] Zhou Jianqin. On the k -error Linear Complexity for 2^n -periodic Binary Sequence via Cube Theory [EB/OL]. (2013-09-07). <http://arxiv.org/abs/1309.1829>.
- [8] 周建钦, 戴小平. 具有稳定 k 错线性复杂度的周期序列 [J]. 通信学报, 2011, 32(11A): 213-220.
- [9] Medidl W. On the Stability of 2^n -periodic Binary Sequence [J]. IEEE Transactions on Information Theory, 2005, 51(3): 1151-1155.
- [10] 周建钦. 具有 2^n 线性复杂度的 2^n 周期二元序列的 3 错线性复杂度 [J]. 应用数学学报, 2013, 36(3): 399-413.
- [11] Zhou Jianqin, Wang Xifeng, Liu Wanquan. Structure Analysis on the k -error Linear Complexity of 2^n -periodic Binary Sequences [EB/OL]. (2014-08-09). <http://arxiv.org/abs/1312.6927>.
- [12] Zhou Jianqin, Liu Wanquan. The k -error Linear Complexity Distribution for 2^n -periodic Binary Sequence [J]. Designs Codes and Cryptography, 2014, 73(1): 55-75.
- [13] 苏明. 周期序列线性复杂度的 k 位置错误谱 [J]. 计算机工程, 2007, 33(22): 1-3.

编辑 索书志