

高维大码距 Hamilton 阵列编码理论与综合算法¹

林柏钢

(福州大学计算机系 福州 350002)

摘 要 该文定义了高维大码距 Hamilton 阵列编码理论的基本概念, 分析了 $d = 2k - 1 (k \geq 3)$ 类型和 $d = 2k (k \geq 3)$ 类型阵列编码的 Hamilton 逻辑拓扑结构模型和一般 Hamilton 阵列编码的存在拓扑条件, 并给出 $d = 2k - 1 (k \geq 3)$ 与 $d = 2k (k \geq 3)$ 高阶高维 Hamilton 阵列编码的构造原理和综合算法. 文中还讨论了两类模型的区别, 以及实例设计, 这为新型阵列密码研究提供一个新方向.

关键词 高维大码距 SM 阵列编码, Hamilton 逻辑路径, 拓扑结构模型, 存在约束条件, 综合算法
中图分类号 TN911.31

1 引 言

设一类二进制阵列编码的码长为 n , 码字集合 $U = \{v_0, v_1, \dots, v_{2^n-1}\} (v_i = x_{n-1}, x_{n-2}, \dots, x_1, x_0 \in [0, 1])$, 码距集 $D = \{d_1, d_2, \dots, d_{2k-1}, d_{2k}\} (k \geq 1)$. 若 U 中任一相邻码字 (或镜像相邻码字) 从 $v_i \rightarrow v_j$ 按某种 d 关系排列, 并组成阵列编码 $SM^n(d) = (n, d, v)_{2^k \times 2^l}$. 其中 $k \geq 1$, 或 $k < l, k + l = n$; k, l 分别对应阵列的行和列, 则称 $SM^n(d)$ 为二进制阵列相邻编码序列. 简称 SM (Sequence Matrix) 阵列编码.

由于 SM 阵列码在新型密码系统以及相关编码领域有实际的应用背景, 所以, 文献 [1-4] 分别对 $d = 1 \sim 4$ 情形编码作过讨论, 并解决了各自存在与实现问题. 对于 $d \geq 5$ 更大情形的 SM 阵列编码是否存在, 以及如何构造等问题, 这仍然是值得研究的课题. 本文仍以图工具, 借助 Q_{bos}^n 逻辑拓扑空间理论, 进一步研究高维大码距情形 SM 阵列编码的存在拓扑条件, 建立了 $d = 2k - 1 (k \geq 3)$ 和 $d = 2k (k \geq 3)$ 高维大码距 SM 阵列编码的拓扑结构模型, 并讨论了它们的构造原理和基本算法. 这为构造不同类型的高维大码距 SM 阵列编码提供新的理论依据和实现方法, 也为这类阵列编码研究和设计提供一个有力的工具.

2 逻辑拓扑结构模型

为讨论方便, 另设 SM 阵列编码的码距为 d, n 为维数 (n 亦可理解为给定码长), 并把 $n \geq 6, d = 2k - 1 (k \geq 3)$ 和 $d = 2k (k \geq 3)$ 看成高维大码距编码, 简记 $SM = (n, d)$. 很显然, 随着码距 d 和维数 n 的加大, 使研究对象更加复杂, 难度更大, 给实现带来不少麻烦. 进一步分析发现, 对于 $d = 2k - 1 (k \geq 3)$ 和 $d = 2k (k \geq 3)$ 高维大码距情形的 SM 阵列编码, 实质上可归结为讨论 Q_{bos}^n 逻辑拓扑空间中不同码距 d 关系排列的一种 Hamilton 逻辑路径 (或半 Hamilton 逻辑路径) 编码问题. 为此, 下面分两种情形讨论.

2.1 $d = 2k - 1 (k \geq 3)$ 类型逻辑拓扑结构模型

定义 1 在 Q_{bos}^n 逻辑拓扑空间, 凡按 d 关系由 $v_i^n(d) \rightarrow v_j^n(d)$, 并满足 Q_{bos}^n 中所有 2^n 个

¹ 2001-12-17 收到, 2002-07-15 改回

国家自然科学基金 (60172017) 和福建省自然科学基金 (A0010011) 资助课题

* SM — 特指 $S_{bos}M$, 即布尔序集相邻逻辑对称序列的阵列编码. 其中 bos —Boolean Order Set. 详见文献 [1, 2] 定义.

布尔顶点相邻逻辑有序排列的路径, 称为 Hamilton 逻辑路径 (或称 Hamilton 逻辑完备回路), 记为 $H^n(d)$.

引理 1 $SM^n(d) = (n, d, U)$ ($d = 2k - 1 (k \geq 3)$) 阵列编码与 Q_{bos}^n 逻辑拓扑空间中的布尔顶点从 $v_i^n(d) \rightarrow v_j^n(d)$ 满足一种 d 排列的 Hamilton 逻辑路径等价.

证明 因为 Q_{bos}^n 逻辑拓扑空间的定义是指: $Q_{bos}^n = \{(U_t, E_l) | t = 0, 1, \dots, 2^n - 1; l = 1, 2, \dots, m \geq n\}$ 为逻辑拓扑空间正则图; 其中 $U_t = \{v_0, v_1, \dots, v_{2^n-1}\}$ 为布尔顶点元素集合, $E_l = \{e_1, e_2, \dots, e_m\}$ 为各布尔顶点元素间的相邻链路. 若码距 d 给定时, 从任一顶点 $v_i^n(d) \rightarrow v_j^n(d)$ 按 d 关系排列时组成的序列, 正与 $SM^n(d)$ 阵列编码的概念是一致的.

所以, 以下的讨论仍把 $d = 2k - 1 (k \geq 3)$ 和 $d = 2k (k \geq 3)$ SM 阵列编码的研究对象放在 Q_{bos}^n 逻辑拓扑空间中来考察. 由定义 1 知, 文献 [2] 讨论的 S_{bos}^n 序列, 即为 $d = 1$ 情形的 Hamilton 逻辑路径. 由此易得:

定理 1 若 $d = 1$, 则在 Q_{bos}^n 中, 必有一条 Hamilton 逻辑路径过所有布尔顶点.

定理 1 的证明是显然的. 因为 Q_{bos}^n 逻辑拓扑空间本质上是一个 n 维立方体正则图, 它可由两个 $n - 1$ 维立方体间顶标一致的相互布尔顶点加上相关边构成. 当 $d = 1$ 时, Hamilton 逻辑通路则按“一顶点一边弧”规则, 沿 $v_{i1}(1) \xrightarrow{e_1(1)} v_{j1}(1) \xrightarrow{e_2(1)} v_{i2}(1) \xrightarrow{e_3(1)} v_{j2}(1) \xrightarrow{e_4(1)} \dots$ 路径排列.

对于更广义情形的 $d = 2k - 1 (k \geq 3)$ 和 $d = 2k (k \geq 3)$ 高维大码距的 Hamilton 逻辑路径是否存在? 其存在条件是什么? 需我们从理论上作一基本分析. 首先讨论 $d = 3$ 情形存在 Hamilton 逻辑路径的最基本拓扑结构模型, 见图 1.

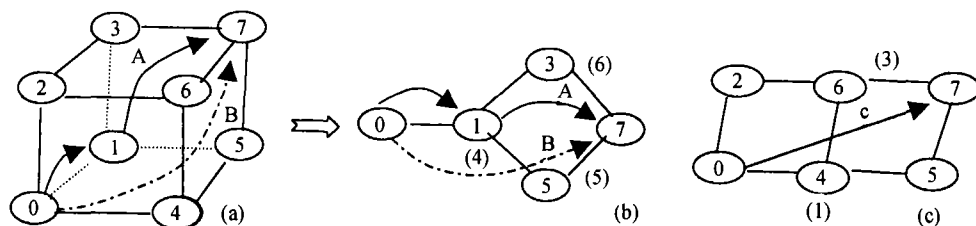


图 1 $d = 3$ 时描述的相邻顶点简化结构模型

在图 1(b) 中, “虚踩点” 只是一个当中过度的虚拟设置的连接点, 比如①它为第一虚踩点. 在图 1(a) 中分别可取①, ②, ④各顶点作第一虚踩点. 以 A 路径表征: $0-1-3-7$; $0-1-5-7$; 还可以 $0-2-3-7$; $0-2-6-7$; $0-4-5-7$; $0-4-6-7$. 表示存在 3 个链接链路边, 实际是不经过这些边. 当然, 第一虚踩点也可取③, ⑤, ⑥各点, 其结构模型刚好颠倒过来. 真正 $d = 3$ 含义是沿 B 路径从 $0 \rightarrow 7$, 满足 $d = E = 3$. 因此, c 模型用这两个链接的空间平行四边形表示对顶角的走向, 由顶点 $v_0 \rightarrow v_7$ (即 $000 \rightarrow 111, d = 3$). 依此类推, 不同 $d = 2k - 1 (k \geq 3)$ 时的相邻逻辑拓扑结构模型如图 2 所示.

这个模型告诉我们: 空间对角线走向的 c 路径其对应的两侧链路边个数 E_l 相等, 即呈对称性. 不同 $d = 2k - 1 (k \geq 3)$ 情形的 Hamilton 逻辑路径排列, 其每个相邻布尔顶点 v_i 与 v_j 之间的拓扑结构模型很相似. 其基本特点是: 在 Q_{bos}^n 逻辑拓扑空间中, 相邻布尔顶点的逻辑拓扑结构恒为: $g = 2k (k \geq 2)$ 个拓扑空间平行四边形的对顶角的走向顶点 ($d = 1$ 例外, 只有边弧数) 构成相邻顶点. 即从 v_i 出发, 经虚边 $E_l (l = 2m - 1, m = 1, 2, \dots)$ 边到达 v_j 的顶点,

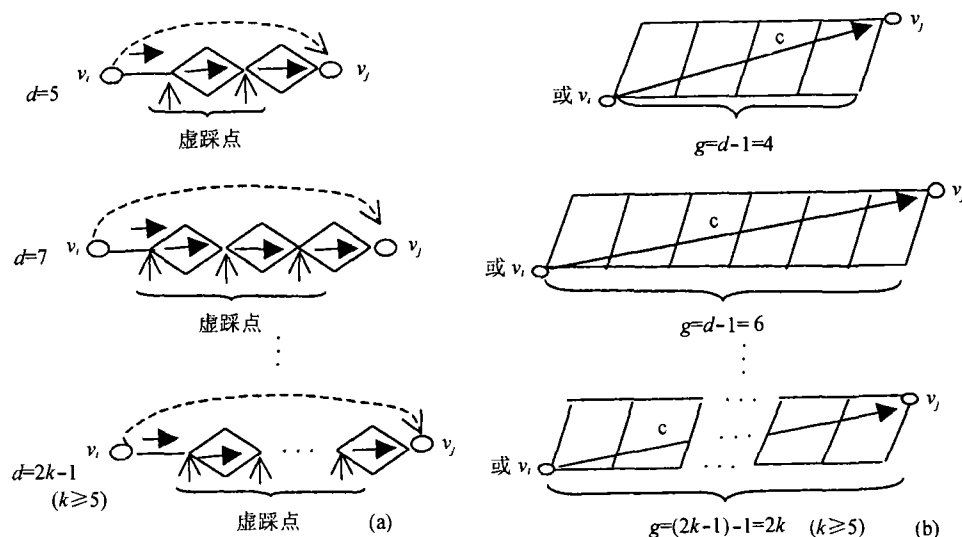


图 2 不同大码距 $d = 2k - 1 (k \geq 3)$ 情形的相邻逻辑路径拓扑结构模型.

才是满足 $d = 2k - 1 (k \geq 3)$ 布尔相邻的顶点. 如 $k = 1$ 时, $d = 1$, 从 $v_i(1) \rightarrow v_j(1)$ 相邻, $E_l(l = 1)$, 边弧数为 1; $k = 2, d = 3$, 从 $v_i(3) \rightarrow v_j(3)$ 相邻, 则 $E_l(l = 3)$ 边弧数为 3; $k = 3, d = 5$, 从 $v_i(5) \rightarrow v_j(5)$ 相邻, 则 $E_l(l = 5)$ 边弧数为 5. 其它依此类推.

根据这些性质, 易得: 在 Q_{bos}^n 逻辑拓扑空间, 若满足 $d = 2k - 1 (k \geq 3)$ 的布尔相邻顶点排列有限群存在. 则有

定理 2 当 $d = 2k - 1 (k \geq 3)$ 时, $k \geq 2$ 情形与 $k = 1$ 情形构成的 Hamilton 逻辑路径类型等价.

证明 由文献 [1, 2] 知, 若把 SM 看成由布尔顶点组成的排列置换群, 当 $k = 1, 2$, $\text{SM}(d)$ 对应 $d = 1, 3$ 时, 呈现出明显的对称群性质. 因此, 当 $k \geq 3$ 时, 其任何一种变换群必同构于 $k = 1$ 时对称群的一个子群, 二者模型同构. 且满足

$$H^n(d = 2k - 1, k \geq 3) \cong H^n(d = 1)$$

这是因为 $k > 1$ 情形, $H^n(d)$ 路径的顶点元素与 $k = 1$ 情形 $H^n(d)$ 路径中元素之间存在一个一一对应关系:

$$\Theta : H^n(d \geq 2k - 1, k \geq 3) \leftrightarrow H^n(d = 1)$$

双方之间且有唯一的像元素特征:

$$v_i(d = 2k - 1, k \geq 3) = \Theta v_i(d = 1), v_i(d = 1) = \Theta' v_i(d = 2k - 1, k \geq 3) \text{ 并且明显构成一种等价关系, 满足下列条件:}$$

种等价关系, 满足下列条件:

(1) $H(d = 2k - 1, k \geq 3) \cong H(d = 2k - 1, k \geq 3)$, (自反性);

(2) 若 $H(d \geq 2k - 1) \cong H(d = 1)$, 则 $H(d = 1) \cong H(d \geq 2k - 1)$ (对称性);

(3) 若 $H(d = 2k - 1, k \geq 3) \cong H(d = 1)$, 且 $H(d = 1) \cong H'(d = 2k - 1, k \geq 3)$, 则 $H(d = 2k - 1, k \geq 3) \cong H'(d = 2k - 1, k \geq 3)$ (传递性). 证毕

为便于理解, 我们给出四维情形 Q_{bos}^n 逻辑拓扑空间模型, 见图 3. 依据该结构模型, 不难从中确定几种低阶情形的 Hamilton 逻辑路径存在性. $d = 1$ 的存在是显然的. 当 $d = 3$ 时, 有

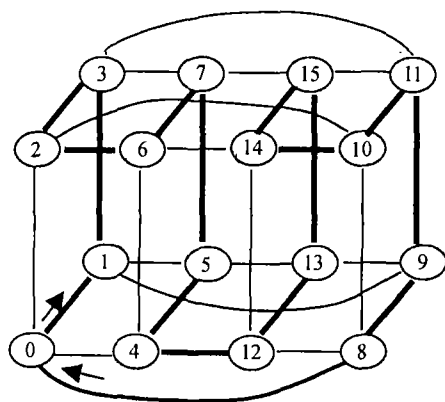


图 3 四维逻辑拓扑空间模型

2.2 $d = 2k (k \geq 3)$ 类型逻辑拓扑结构模型

定义 2 设 $Q_{\text{bos}}^n = \{(U_t, E_l) \mid t = 0, 1, \dots, 2^n - 1; l = 1, 2, \dots, m; m \geq n\}$ 为逻辑拓扑空间, $U_t = \{v_0, v_1, \dots, v_{2^n-1}\}$ 为布尔顶点元素集合, $E_l = \{e_1, e_2, \dots, e_m\}$ 为各顶点元素间的相邻链路. 若任一相邻顶点间, 按给定码距 d 关系由 $v_i^n(d=2k) \rightarrow v_j^n(d=2k)$ 遍历相关顶点, 且只满足 2^{n-1} 个相邻布尔顶点的有序排列, 并构成独立闭环回路的逻辑路径, 则称为半 Hamilton 逻辑路径, 记为 $H_b^n(d=2k, k \geq 3)$, 且有 $H_b^n(d) = (H_{bl}^n(d), H_{br}^n(d))$, 其中 $H_{bl}^n(d) \not\leftrightarrow H_{br}^n(d)$, $d = 2k, k \geq 3$).

研究 $d = 2k$ 类型的 SM 阵列编码, 借助半 Hamilton 逻辑路径的概念来解决问题是比较方便的. 原因是二者间构成相互等价关系. 对于广义情形的 $d = 2k (k \geq 3)$ 高维大码距的 SM 阵列编码是否存在以及如何表达, 这实际上均归结为回答半 Hamilton 逻辑路径是否存在问题. 因此, 下面以 $d = 4$ 为例, 并以 $H_{br}^5(4)$ 中的 $v_1 \rightarrow v_{28}$ 的部分拓扑关系图来说明 $D = 4$ 简化模型描述.

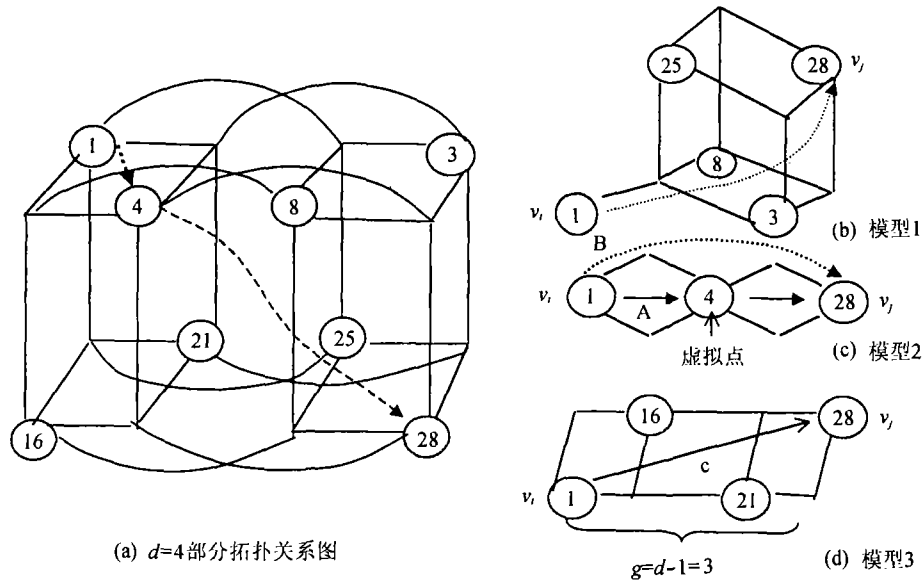
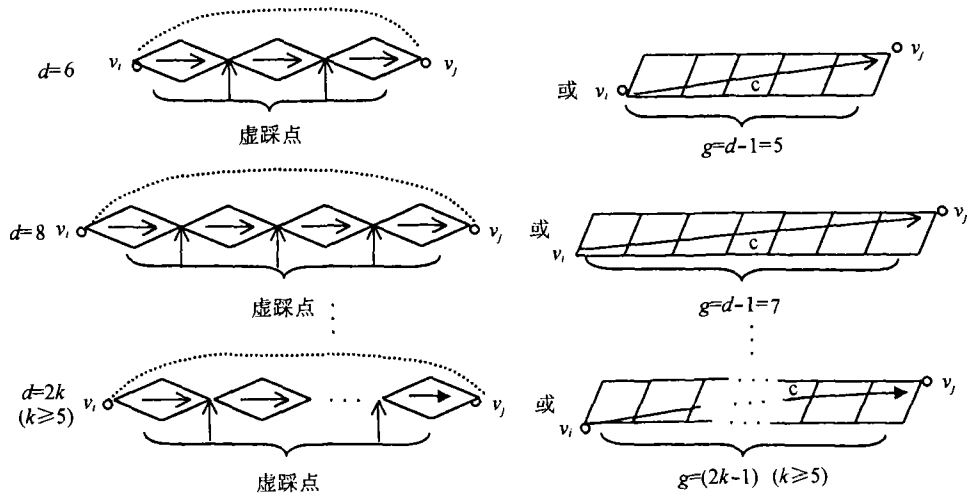
图 4 中, 图 4(b) 为图 4(a) 的部分对象分析简化模型图, 图 4(c) 为“一顶点四边弧”描述关系图, 图 4(d) 是直观矩形网格对顶角相邻关系图. 实际上, 图 4(d) 借助的是一个平行四边形对角线相接的方式来表达. 图 4(c) 中顶点④仍将它看成是“虚踩点”, A 路径实际并不经过它, 只反映一种链路边转接点关系, 即 B 路径轨迹. 图 4(d) 中采用更直观描述模型, 即由 $v_1 \rightarrow v_{28}$, 是沿 c 路径从起点到相邻点. 空间对角线走向经过 $g = d - 1 = 3$ 个网格格点. 反映出两边链路边个数相等, 即路径 $d = 4$, 且对称. 以下主要采用图 4(d) 的简化模型来描述. 因此就有不同大码距 $d = 2k (k \geq 3)$ 时的相邻顶点逻辑拓扑结构关系模型, 如图 5 所示.

该模型表明: $d = 2k (k \geq 3)$ 的基本特点是: 相邻两顶点间的逻辑拓扑结构模型恒为: $g = 2k - 1 (k \geq 1)$ 个拓扑空间网格平行四边形的对顶角顶点构成. 即从 v_i 出发, 经虚边 $E_l (l = 2m, m \geq 1)$ 边到达 v_j 终点. 才是满足 $d = 2k (k \geq 1)$ 布尔相邻顶点的必要条件 (实际充要条件是定理 9). 这一点, 与 $d = 2k - 1$ 情形相类似. 因此有

定理 3 若 $d \equiv 2$, 则在 Q_{bos}^n 中必有两条相互独立的半 Hamilton 逻辑路径分别过所有 2^{n-1} 个布尔顶点.

$H^4(3)$ 的 Hamilton 逻辑路径为: $v_0 \rightarrow v_7 \rightarrow v_{10} \rightarrow v_4 \rightarrow v_9 \rightarrow v_2 \rightarrow v_{15} \rightarrow v_1 \rightarrow v_{12} \rightarrow v_{11} \rightarrow v_6 \rightarrow v_8 \rightarrow v_5 \rightarrow v_{14} \rightarrow v_3 \rightarrow v_{13} \rightarrow v_0$.

现在问题是, 若维数不变, 当 $d \geq 5$ 时, 在 Q_{bos}^n 逻辑拓扑空间, Hamilton 逻辑路径 (或半 Hamilton 逻辑路径) 还成立吗? 回答显然是否定的. 那么, 它们之间存在的条件是什么? 与维数 n 之间的约束关系又是怎样? 这就要我们作进一步的分析 (见第 3 节).

图 4 $d=4$ 时描述的相邻顶点简化结构模型图 5 不同大码距 $d=2k(k \geq 3)$ 情形的简化相邻逻辑拓扑结构模型

证明 当 $d \equiv 2$ 时, 半 Hamilton 逻辑通路则按“一顶点二边弧”(即对顶角)规则, 沿 $v_{i1}(2) \xrightarrow{e_1(2)e_2(2)} v_{i2}(2) \xrightarrow{e_3(2)e_4(2)} v_{i3}(2) \xrightarrow{e_5(2)e_6(2)} \dots$ 路径排列。实际上, 考虑 Q_{bos}^n 逻辑拓扑空间中的所有布尔顶点元素个数为 2^n 个, 当维数 n 给定时, 其位数 W 也给定。即 $n=W$ 。若按所对应的不同码重 w 组合来分类, 则有

$$\text{偶数码重子集为 } C_e(n, w) = \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \dots + \binom{n}{2w} = 2^{n-1},$$

$$\text{奇数码重子集为 } C_o(n, w) = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \dots + \binom{n}{2w-1} = 2^{n-1}.$$

而且, 根据码重个数的奇偶关系有两个运算规则. 规则 1: “偶 $\oplus$ 奇 = 奇, 奇 $\oplus$ 偶 = 奇”; 规则 2: “偶 $\oplus$ 偶 = 偶, 奇 $\oplus$ 奇 = 偶”. 由此可见, 若要满足 $d \equiv 2$, 只能按照规则 2 的结果分别在 $C_e(n, w)$ 和 $C_o(n, w)$ 码重子集中, 得到独立封闭的 Hamilton 逻辑路径结果. 故在 Q_{bos}^n 中按照二部图划分聚类得到的两条独立存在的半 Hamilton 逻辑路径, 必定分别过 2^{n-1} 个布尔顶点.

定理 4 $d = 2k (k \geq 3)$ 时, $\forall k \geq 2$ 与 $k = 1$ 情形构成的 Hamilton 逻辑路径类型等价.

证明 根据定理 1. 考虑 $k \geq 2$ 时, 由 $SM(d)$ 构成的任何一种变换群必同构于 $k = 2$ 时对称群的一个子群. 二者模型同构. 且满足

$$H_b^n(d = 2k, k \geq 2) \cong H_b^n(d = 2)$$

双方间且有唯一的像元素特征

$$v_j(d = 2k, k \geq 2) = \Theta v_j(d = 2), v_j(d = 2) = \Theta' v_j(d = 2k, k \geq 2)$$

所构成的等价关系必满足下列条件:

- (1) $H_b(d = 2k) \cong H_b(d = 2k)$ (自反性)
- (2) 若 $H_b(d = 2k) \cong H_b(d = 2)$, 则 $H_b(d = 2) \cong H_b(d = 2k)$ (对称性)
- (3) 若 $H_b(d = 2k, k \geq 3) \cong H_b(d = 2)$, 且 $H_b(d = 2) \cong H'_b(d = 2k, k \geq 3)$, 则 $H_b(d = 2k, k \geq 3) \cong H'_b(d = 2k, k \geq 3)$ (传递性) 证毕

3 高维大码距存在的约束条件

现在我们来回答分析图 3 时留下的问题. 图 3 的例子告诉我们, 当 $d = 2k - 1, k \geq 3$ 时, 给定 $n = 4$, $H^n(d)$ 的排列是不存在的. 这是因为不同的码距 d , 其存在的约束条件是不一样的. 所以就有:

定理 5 给定 k , 若 H 满足 $D = 2k - 1 (k \geq 3)$ 的 Hamilton 逻辑路径, 则 Q_{bos}^n 逻辑拓扑空间的维数 $n \geq 2k$ (其中 $D = \max d$).

证明 令 $D = \max d$, 给定 $k, n < D = 2k - 1$ 时, Q_{bos}^n 中绝对不存在对应 D 的 Hamilton 逻辑通路. 由归纳法知, 当 $n < D = 2k - 1$ 时, 无须讨论; 而当 $n = D = 2k - 1$ 时, 由于 Q_{bos}^n 是正则的超维立方体, 任一布尔顶点的链路数 $l = n = D$. 换句话说, 任一 $v_i(D = 2k - 1)$ 仅与 $v_j(D = 2k - 1)$ 相邻, 才能够满足 $D = 2k - 1$ 的可达路径要求, 因为两两都是互为反码关系对应独立的离散顶点. 即为

$v_i(D = 2k - 1) \rightarrow v_j(D = 2k - 1)$ (可达), 或 $v_i(D = 2k - 1) \sim v_j(D = 2k - 1)$ (相邻) 写成下列表达式:

$$\begin{aligned} v_i(D = 2k - 1) &= (x_1 x_2 \cdots \bar{x}_{i-r} \bar{x}_{i-r+1} \cdots \bar{x}_{i-1} x_i \bar{x}_{i+1} \cdots \bar{x}_{i+r-1} \bar{x}_{i+r} \cdots x_{n-1} x_n) \xrightarrow{\text{or } \sim} \\ v_j(D = 2k - 1) &= (\bar{x}_1 \bar{x}_2 \cdots x_{i-r} x_{i-r+1} \cdots x_{i-1} \bar{x}_i = \bar{x}_j x_{j+1} \cdots x_{j+r-1} x_{j+r} \cdots \bar{x}_{n-1} \bar{x}_n) \end{aligned}$$

当且仅当 $n > D$ 时, 才唯有对应 D 的 Hamilton 逻辑路径存在. 因为 $n = D + 1 = 2k$ 时, Q_{bos}^n 中布尔顶点增加一倍, 即为 $2^{n=2k}$. 又由于 $D = 2k - 1$, 其中任一顶点对应的变量与其相邻顶点至少总有一位保持不变, 即

$$\begin{aligned} v_i(D = 2k) &= (x_1 x_2 \cdots \bar{x}_{i-r} \bar{x}_{i-r+1} \cdots \bar{x}_{i-1} x_i \bar{x}_{i+1} \cdots \bar{x}_{i+r-1} \bar{x}_{i+r} \cdots x_{n-1} x_n) \xrightarrow{\text{or } \sim} \\ v_j(D = 2k) &= (\bar{x}_1 \bar{x}_2 \cdots x_{i-r} x_{i-r+1} \cdots x_{i-1} x_i = x_j x_{j+1} \cdots x_{j+r-1} x_{j+r} \cdots \bar{x}_{n-1} \bar{x}_n) \end{aligned}$$

结果则有: $v_i(D=2k) \xrightarrow{\text{or } \sim} v_j(D=2K)$.

v_i, v_j 所表征的逻辑拓扑结构按图 2(b) 方式转换, 故只要 $n=2k$ 能满足 $H^n(d)$ 存在条件, 则当 $n>D$ 时, Hamilton 通路必定都满足.

推论 1 给定 $k \geq 3$, Q_{bos}^n 中必定存在 $d=2k-1$ 的相邻逻辑顶点的 Hamilton 完备回路.

由上述定义 1 及定理 2, 5, 易得出该推论结果.

定理 6 给定 k , 若存在满足 $D=2k(k \geq 3)$ 的半 Hamilton 逻辑路径 H_b , 则 Q_{bos}^n 逻辑拓扑空间的维数 $n \geq 2k+1=d+1$ (其中 $D=\max d$).

证明过程仿定理 5(证明略).

推论 2 给定 $k \geq 1$, Q_{bos}^n 中必定存在 $d=2k$ 相邻逻辑顶点的半 Hamilton 完备回路.

定理 7 若存在 $d=2k-1(k \geq 3)$ 的相邻逻辑顶点排列的 Hamilton 逻辑路径, 则任意两顶点相邻的拓扑图充要条件分别为 $L \equiv 2k-1$, 且 $v_i(d=2k-1) \not\sim v_j(d \leq (2k-3))$, 其中 L 为相邻顶点间最长可达链路数, 符号 “ $\not\sim$ ” 为不相邻.

证明 必要性 从超维 Q_{bos}^n 逻辑拓扑空间分析可知, 若 $d=2k-1$ 的相邻逻辑顶点 Hamilton 路径存在, 据定理 3, 必须 $n \geq 2k$. 假定 $v_i(d=2k-1)$ 与 $v_j(d=2k-1)$ 相邻, 显然, 从 $v_i(d=2k-1) \rightarrow v_j(d=2k-1)$ 必须经过 $L=d=2k-1$ 个可达路径边(或弧), 其间经过 $2k-2$ 个顶点, 才能从 $v_i(d=2k-1)$ 到达 $v_j(d=2k-1)$ 顶点. 其路径如图 6 中的 H_1 所示: $v_i(d=2k-1) \circ \xrightarrow{e_1} \circ \xrightarrow{e_2} \circ \xrightarrow{e_3} \circ \cdots \circ \xrightarrow{e_{2k-2}} \circ \xrightarrow{e_{2k-1}} \circ v_j(d=2k-1)$. 当 $L \equiv 2k-1$ 时, 反映出所经过的 $2k-1$ 个可达路径边, 有 $2k-1$ 个变量相异, 说明 $v_i(d=2k-1)$ 与 $v_j(d=2k-1)$ 相邻. 也就是说, 若 $v_i(d=2k-1)$ 与 $v_j(d=2k-1)$ 相邻, 则必须 $L \equiv 2k-1$, 这是必要条件.

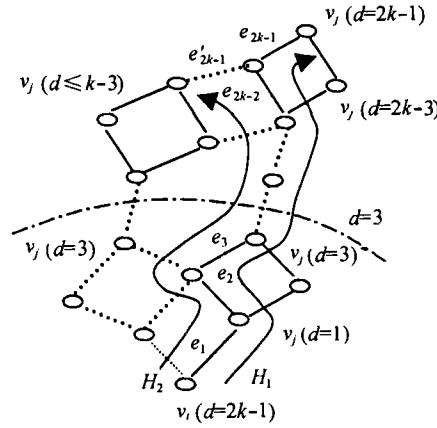


图 6 $d=2k-1(k \geq 3)$ 情形 $v_i(d)$ 与 $v_j(d)$ 相邻顶点模型示意图

充分性 $L=2k-1$ 虽为必要拓扑条件, 但非充分条件. 因为在超维 Q_{bos}^n 中, 从 $v_i(2k-1) \rightarrow v_j(2k-1)$ 所经过的 $2k-1$ 个边, 如果只满足 $L=2k-1$ 个边条件, 就有可能出现图 6 中 H_2 等其它形式路径, 即从 $v_i(d=2k-1) \circ \xrightarrow{e_1} \circ \xrightarrow{e_2} \circ \xrightarrow{e_3} \circ \cdots \circ \xrightarrow{e_{2k-2}} \circ \xrightarrow{e_{2k-1}} \circ v_j(d=2k-3)$, 表明 $v_i(d=2k-1)$ 与 $v_j(d=2k-3)$ 相邻. 其实不然, H_2 由 $v_i(d=2k-1) \rightarrow v_j(d=2k-3)$ 的路径, 只要 $L=2k-3$ 就行. 实际是 $v_i(d=2k-3) \sim v_j(2k-3)$, 而 $v_i(d=2k-1) \not\sim v_j(2k-3)$. 由此分析可知, 因路径 L 条件满足的, 还有可能出现: $v_i(d=2k-1)$ 与 $v_j(d < 2k-3)$ 相邻情形. 事实上,

这种相邻都只满足 d 降一维 (或降若干维) 情形的相邻. 故只有 $v_i(d=2k-1) \sim v_j(d=2k-1)$, 且 $v_i(d=2k-1) \not\sim v_j(d \leq 2k-3)$ 的条件才是充分的.

证毕

定理 8 若存在 $d=2k(k \geq 3)$ 的相邻逻辑顶点排列的半 Hamilton 逻辑路径, 则任意两顶点相邻的拓扑图充要条件必须为 $L \equiv 2k$, 且 $v_i(d=2k) \not\sim v_j(d \leq 2k-2)$. 其中 L 为相邻顶点间最长可达链路数, 符号 “ $\not\sim$ ” 为不相邻.

证明过程仿定理 7. (证明略)

定理 9 (相邻顶点简易判别法) (1) 给定 $k \geq 1$, 则有满足 $H^n(d)$ 路径中 v_i 与 v_j 相邻的充要条件是

$$v_i(d=2k-1) \oplus v_j(d=2k-1) \equiv d$$

(2) 给定 $k \geq 1$, 则有满足半 Hamilton 逻辑路径中 v_i 与 v_j 相邻的充要条件是:

$$v_i(d=2k) \oplus v_j(d=2k) \equiv d$$

证明 由定义 1 和定理 5, 7, 易证本定理 (1) 成立; 由定义 2 和定理 6, 8, 易证本定理 (2) 成立.

推论 3 (1) 给定 $k \geq 1$, 在 Q_{bos}^n 逻辑拓扑空间中, 只要满足大码距 d 的 H 路径存在, 则有 $d < D=2k-1$ 的 Hamilton 逻辑路径均存在;

(2) 给定 $k \geq 1$, 在 Q_{bos}^n 逻辑拓扑空间中, 只要满足大码距 d 的 H 路径存在, 必有 $d < D=2k$ 的半 Hamilton 逻辑路径亦均存在.

证明(只证 1) 由归纳法知 $k=1$, 有 $d=1$ 类型的 Hamilton 逻辑路径存在. 当 $k > 1$ 时, 取 $k=2$, 则有 $d=3, d=1$ 两种 H 完备回路存在. 以此类推, 取 $k=l$, 有 $d=2l-1, d=2l-3, \dots, d=3, d=1$ 的 H 完备回路存在. 由此可见, 一旦 $k > 1$ 给定, 根据定理 2, 5, 只要 $d=2k-1$ 满足存在条件, 在 Q_{bos}^n 逻辑拓扑空间中, 则有 $d < 2k-1$ 类型的 Hamilton 逻辑路径必定全部存在. 同理, 可证 (2) 成立.

4 综合算法与编码实现

由上述分析知道, 不同 d 关系的 Hamilton 逻辑路径或半 Hamilton 逻辑路径唯一存在 Q_{bos}^n 超维逻辑拓扑空间中. 借助不同 d 关系 ($d=2k-1$, or: $d=2k, k \geq 3$) 的 Hamilton 逻辑路径来构造 $d \geq 5$ 高维大码距 SM 阵列编码, 这是必须遵循的一个基本构造原则. 因为构造 SM 阵列编码的生成元和阵列综合, 都必须满足 H 路径的关系.

SM 阵列编码结构模型^[6] 正因为 SM 阵列编码与 $H(d)$ 之间的等价性. 所以, SM 阵列编码的实质就是寻找二者之间的一种映射关系:

$$F: H(d=2k-1, \text{ or } : d=2k, k \geq 3) \rightarrow \text{SM}^n(d=2k-1, \text{ or } : d=2k, k \geq 3)$$

对于 $d=2k-1(k \geq 3)$ 来说, 当 $d \geq 5$ 时, SM 阵列编码的结构形式描述如下:

$$\text{SM}^n(d=2k-1) = \left(\begin{array}{ccccccc} v_{11}(2k-1) & \rightarrow & v_{12}(2k-1) & \rightarrow & \cdots & \rightarrow & v_{1r}(2k-1) \\ v_{21}(2k-1) & \leftarrow & v_{22}(2k-1) & \leftarrow & \cdots & \leftarrow & v_{2r}(2k-1) \\ \vdots & & & & \vdots & & \vdots \\ v_{s1}(2k-1) & \leftarrow & v_{s2}(2k-1) & \leftarrow & \cdots & \leftarrow & v_{sr}(2k-1) \end{array} \right)_{s \times r = 2^n}$$

由于 $SM^n(d=2k-1) \cong H^n(d=2k-1)$, 所以, 实现 SM 阵列编码综合, 实质上就是要完成构造 $H^n(d)$ 的逻辑路径问题。

同理, 对 $d=2k(k \geq 3)$ 来说, 当 $d \geq 5$ 时, SM 阵列编码的结构模型如下:

$$SM^n(d=2k) = (SM_{bl}^n(d=2k), SM_{br}^n(d=2k)) \quad (k \geq 3)$$

$$= \left(\begin{array}{c} \left[\begin{array}{cccc} v_{i11}^n(2k) & \rightarrow & v_{i12}^n(2k) & \rightarrow \cdots \rightarrow v_{i1t}^n(2k) \\ v_{i21}^n(2k) & \leftarrow & v_{i22}^n(2k) & \leftarrow \cdots \leftarrow v_{i2t}^n(2k) \\ \vdots & & \vdots & \\ v_{it1}^n(2k) & \leftarrow & v_{it2}^n(2k) & \leftarrow \cdots \leftarrow v_{it t}^n(2k) \end{array} \right]_{i \times t=2^{n-1}} \\ \left[\begin{array}{cccc} v_{r11}^n(2k) & \rightarrow & v_{r12}^n(2k) & \rightarrow \cdots \rightarrow v_{r1t}^n(2k) \\ v_{r21}^n(2k) & \leftarrow & v_{r22}^n(2k) & \leftarrow \cdots \leftarrow v_{r2t}^n(2k) \\ \vdots & & \vdots & \\ v_{rit}^n(2k) & \leftarrow & v_{rit2}^n(2k) & \leftarrow \cdots \leftarrow v_{rit t}^n(2k) \end{array} \right]_{j \times t=2^{n-1}} \end{array} \right)_{(i+j) \times t=2^n}$$

实际上, 由于

$$SM^n(2k) = (SM_{bl}^n(2k), SM_{br}^n(2k)) \quad (k \geq 3) \cong H_b^n(2k) = (H_{bl}^n(2k), H_{br}^n(2k))$$

所以, 实现 SM 阵列编码综合, 同样要借助 $H_b^n(d)$ 的逻辑路径排列来完成的。限于篇幅, 下面只讨论 $d=2k-1$ 情形的编码算法和具体示例。

$D=2k-1$ SM 阵列编码综合算法 关于 $d \geq 5$ SM 阵列编码的实现, 都可看成是由低阶 $H^n(d)$ 路径组成。因为通常可令: $SM^n(d+i) = f(n, d+i, U+i)$, $i=0, 1, 2, \dots, 2k-1, 2k$; 则顶点元素集 $U = (v_0(d), v_1(d), \dots, v_{2^n-1}(d))$ 为生成元, 显然, 阵列编码序列 $SM^n(d+i)$ 由 f 和初始值 $(v_0(d), v_1(d), \dots, v_{2^n-1}(d))$ 唯一确定。下面介绍两种综合算法。

算法 1 设 H 是有限集, 取低阶 $H^n(d=1)$ 作生成元阵列, 并求出 $d=2$ 偶图聚类 SM 阵列 $H_b^n(d=2)$, 由此再选取某种约定规则 G , 导引产生高阶 SM 阵列编码 $H^n(d \geq 5)$, 综合算法步骤如下:

(1) $d \equiv 1$ 生成元阵列 $H_{s \times r=2^n}^n(d=1)$ 的制作。由文献 [3] 则有

定理 10^[5] 设 $H_{s \times r=2^n}^n(d=1)$ 为 $d \equiv 1$ 时的有限集生成元阵列, 若 G' 为产生 $d \equiv 1$ 路径的约定规则, 则构造 $H_{s \times r=2^n}^n(d=1)$ 的下列方法等价:

- (a) $P(SM) : T^n \rightarrow T_{bos}^n \quad (d=1)$
- (b) $P(SM) : T^n \rightarrow S_{bos}^n \quad (d=1)$
- (c) $P(SM) : T^n \rightarrow SB \quad (d=1)$
- (d) $P(SM) : T^n \rightarrow SM' \quad (d=1)$
- (e) $P(SM) : T^n \rightarrow \Psi \quad (d=1)$ (Ψ — 其他方法)

(2) $d \equiv 2$ 偶图聚类 SM 阵列的 $H_b^n(d)$ 求解。由文献 [1] 易得步骤 (2) 的唯一性。

(3) 基于 (2), 令 G 为产生 $d \geq 5$ SM 阵列码的某种约定产生规则, 则有综合结果:

$$F(SM) : G \times H^n(d=2) \rightarrow H_{s \times r=2^n}^n(d=2k-1), \quad (k \geq 3)$$

算法 1 选取的布尔顶点元素均为布尔序集编号, 因此算法 1 适合于计算机求解, 对于低维小码距情形, 亦适用于人工实现。

算法 2 设 H 是有限集, 选取任一 v_i 作源点, 根据定理 5(相邻简易判别法) 原则, 分别综合实现下列结果:

$$F(SM) : (v_i^n(2k-1) \oplus v_j^n(2k-1) \equiv d) \rightarrow H_{s \times r=2^n}^n(d=2k-1)$$

算法 2 选取的 v_i, v_j 元素只能为二进制数。因此, 算法 2 适合于计算机求解。

限于篇幅, 具体算法实现步骤将结合下面实例给出。最后, 给出一个按照算法 1 得到 7 维码距为 5 的 SM 阵列编码主要过程与结果。

实例求解 构造一个 $SM_{8 \times 16}^7(5)$ 阵列编码

问题分析 设由算法 1 已求出 7 维情形 $d = 1$ 时阵列编码为 $H_{8 \times 16=2^7}^7(d = 1)$, $d = 2$ 时阵列编码为 $H_{b(8 \times 16=2^7)}^7(d = 2)$ 。现进一步讨论, 基于 $H_b^7(d = 2)$ 阵列, 令产生 $d = 5$ 的 SM 阵列编码的规则 G 如 $H_b^7(d = 2)$ 阵列中箭头方向顺序编号排列:

$$H_b^7(d = 2) = \begin{pmatrix} \xrightarrow{H_{b11}} (1) & \xleftarrow{H_{b12}} (3) & \xrightarrow{H_{b13}} (5) & \xleftarrow{H_{b14}} (7) \\ \xrightarrow{H_{b21}} (15) & \xleftarrow{H_{b22}} (13) & \xrightarrow{H_{b23}} (11) & \xleftarrow{H_{b24}} (9) \\ \xrightarrow{H_{b31}} (17) & \xleftarrow{H_{b32}} (19) & \xrightarrow{H_{b33}} (21) & \xleftarrow{H_{b34}} (23) \\ \xrightarrow{H_{b41}} (31) & \xleftarrow{H_{b42}} (29) & \xrightarrow{H_{b43}} (27) & \xleftarrow{H_{b44}} (25) \\ \xrightarrow{H_{b51}} (22) & \xleftarrow{H_{b52}} (24) & \xrightarrow{H_{b53}} (18) & \xleftarrow{H_{b54}} (20) \\ \xrightarrow{H_{b61}} (28) & \xleftarrow{H_{b62}} (26) & \xrightarrow{H_{b63}} (32) & \xleftarrow{H_{b64}} (30) \\ \xrightarrow{H_{b71}} (6) & \xleftarrow{H_{b72}} (8) & \xrightarrow{H_{b73}} (2) & \xleftarrow{H_{b74}} (4) \\ \xrightarrow{H_{b81}} (12) & \xleftarrow{H_{b82}} (10) & \xrightarrow{H_{b83}} (16) & \xleftarrow{H_{b84}} (14) \end{pmatrix}_{8 \times 16=2^7}$$

其中: 任一 $H_{bij}(2) = (v_{aij}, v_{bij}, v_{cij}, v_{dij})$ 均为不同的四元素, 每行共 16 个元素, $i = 1, 2, \dots, 8$; $j = 1, 2, \dots, 16$ 。

最后综合结果得到下列 H 路径排列:

$$H^7(d = 7) = v_0 \rightarrow v_{115} \rightarrow v_6 \rightarrow v_{117} \rightarrow v_{12} \rightarrow \dots \rightarrow v_9 \rightarrow v_{122} \\ 0000000 \ 1110011 \ 0000110 \ 1110101 \ 0001100 \ \dots \ 0001001 \ 1111010$$

即得到维数 $n = 7$, 码距 $d = 5$ 的 $SM_{8 \times 16}^7(5)$ 阵列编码的全部集合为

$$SM^7(5) = \begin{pmatrix} 0 & 115 & 6 & 117 & 12 & 127 & 10 & 121 & 18 & 97 & 20 & 103 & 30 & 109 & 24 & 107 \\ 91 & 40 & 93 & 46 & 87 & 36 & 81 & 24 & 73 & 58 & 79 & 60 & 69 & 54 & 67 & 48 \\ 96 & 19 & 102 & 21 & 108 & 31 & 106 & 25 & 114 & 1 & 116 & 7 & 126 & 13 & 120 & 11 \\ 59 & 72 & 61 & 78 & 35 & 68 & 49 & 66 & 41 & 90 & 47 & 92 & 37 & 86 & 35 & 80 \\ 65 & 50 & 71 & 52 & 77 & 62 & 75 & 56 & 83 & 32 & 85 & 38 & 95 & 44 & 89 & 42 \\ 26 & 105 & 28 & 111 & 22 & 101 & 16 & 99 & 8 & 123 & 14 & 125 & 4 & 119 & 2 & 113 \\ 33 & 82 & 39 & 84 & 45 & 94 & 43 & 88 & 51 & 64 & 53 & 70 & 63 & 76 & 57 & 74 \\ 122 & 9 & 124 & 15 & 118 & 5 & 112 & 3 & 104 & 27 & 110 & 29 & 100 & 23 & 98 & 17 \end{pmatrix}_{8 \times 16}$$

显然, $SM^7(5) = H^7(5)$, 该阵列编码满足 Hamilton 逻辑路径的唯一性, 且码距 $d \equiv 5$ 。对于高维 $SM^n(d = 5)$ 情形的构造结果也是一致的。同理, $d = 2k$ 类型的高维大码距 Hamilton 阵列编码也可以仿照上述类似步骤进行, 这里不在赘述。

5 结束语

综上所述, 应用 Q_{bos}^n 逻辑拓扑空间中的 Hamilton 逻辑路径理论, 可以解决高维大码距情形 SM 阵列编码构造与综合算法问题。作者已获得一大类 $d \geq 3$ SM 阵列编码的满意结果。这对组合编码与阵列密码研究无疑是有益的。应当指出, 本文的结果, 实质上也给出了 Q_{bos}^n 中 $d = 2k - 1 (k \geq 3)$ 类型的 Hamilton 逻辑路径存在的唯一性问题, 同时也给出了 $d = 2k (k \geq 3)$

类型的半 Hamilton 逻辑路径存在性问题。限于篇幅, 对于其它高维大码距 SM 阵列编码的具体构造和应用, 将在其它文章中讨论。

参 考 文 献

- [1] 林柏钢, 基于 $D = 2$ 的 SM 阵列码构造, 密码学进展——CHINACRYPT'94, 第三届中国密码学学术会议论文集, 北京, 科学出版社, 155–160.
- [2] 林柏钢, S_{box} 相邻逻辑对称序列构造与实现方法, 电子科学学刊, 1991, 13(5), 502–508.
- [3] 林柏钢, 邱宏端, 高维 $D = 3$ SM 阵列编码构造与实现, 电子科学学刊, 2000, 22(2), 198–204.
- [4] 林柏钢, 邱宏端, 用图论方法实现 $D = 4$ SM 阵列编码, 电路与系统学报, 1999, 4(4), 62–67.
- [5] Lin Bogang, The process of integrated learning and the model of parallel search for solution tactics, International Conference Proceeding of ICNNSP'95, P.R.China, Dec., 1995, 60–63.
- [6] C. J. A. Jansen, W. G. Franx, D. E. Boeke, An efficient algorithm for the generation of De-Bruijn cycles, IEEE Trans. on Inform. Theory, 1991, IT-37(5), 1475–1478.

THE THEORY OF HAMILTON ARRAY CODES FOR HIGH DIMENSION AND BIG HAMMING DISTANCE AND THE SYNTHESIS ALGORITHM

Lin Bogang

(Dept. of Computer Science and Technology, Fuzhou University, Fuzhou 350002, China)

Abstract In this paper, the theory of Hamilton array codes for high dimension and big Hamming distance is proposed. The model of logical topology structure for $d = 2k - 1, d = 2k(k \geq 3)$ types and the existence topology condition for general high order SM array codes are analyzed. The construction principle and the synthesis algorithm of SM array codes for $d = 2k - 1$ and $d = 2k(k \geq 3)$ high dimension and high order are discussed. Finally, the distinction between the two models and the example design are given. The result provides a new direction for a class of new type array ciphers research.

Key words SM array codes for high dimension and big Hamming distance, Hamilton logical path, Topology structure model, Existence restraint condition, Synthesis algorithm

林柏钢: 男, 1953 年生, 教授, 主要从事数据通信与计算机网络、编码与密码, 网络与信息安全的教学与科研工作。