1-Perfect Codes Over the Quad-Cube

Pranava K. Jha

Abstract—A vertex subset $S$ of a graph $G$ constitutes a 1-perfect code if the one-halls centered at the nodes in $S$ effect a vertex partition of $G$. This paper considers the quad-cube $CQ_m$ that is a connected $(m + 2)$-regular subgraph of the hypercube $Q_{m+2}$, and shows that $CQ_m$ admits a vertex partition into 1-perfect codes iff $m = 2^k - 3$, where $k \geq 2$. The scheme for that purpose makes use of a procedure by Jha and Slutzki that constructs Hamming codes using a Latin square. The result closely parallels the existence of a 1-perfect code over the dual-cube, which is another derivative of the hypercube.

Index Terms—Graph theory, error-correction codes, quad-cubes, hypercubes, Hamming codes, metacube, perfect dominating set, error-detection codes.

I. INTRODUCTION

A 1-PERFECT code has the capability to correct a single error, and detect two or fewer errors. Applications abound in areas such as communication systems, network systems, multiprocessor systems, and computer architecture in the wide digital world. Not surprisingly, the topic commands a rich literature [10]. Among various codes, the 1-perfect Hamming codes and 3-perfect Golay codes based on the topology of the hypercube, are the foremost [10], [15].

A quad-cube (formally defined below) is a special version of a more general network topology called the metacube, devised by Li et al. [19], that itself is derivable from the hypercube. The basic idea is to mitigate the problem of the rapid increase in the degree of the hypercube when the node size exceeds several million. It retains most good characteristics of the hypercube, notably, efficient collective communication, high connectivity, fault tolerance, low diameter, and easy routing [19]. This paper adds another significant property to that list, viz., a vertex partition of the graph into 1-perfect codes.

In an analogous study, the author [14] earlier presented a perfect code over the dual-cube that is another (relatively simpler) version of the metacube.

Motivation: Assuming that there is a maximum of one error, any possible word in a message transmission can, in a unique way, be corrected to one of the words in a 1-perfect code. Optimal resource placement in an interconnection network is another area of application. In particular, elements of a 1-perfect code may be viewed as nodes that house (expensive) resources such as power sources, function libraries and algorithmic information, whereas other nodes are users of the resources. Since every user node is adjacent to a unique resource node, optimality is achieved in the number of resource nodes. A closely related concept is that of domination. Indeed, a 1-perfect code corresponds to a smallest (independent) dominating set in the graph in an obvious way. Other applications include construction of an efficient backbone for routing and partition of a network into small clusters.

A. Related Studies

Apart from the study of perfect codes on hypercube-like networks, there have been a number of such studies in other settings, too. For example, Biggs [2] presented codes on the topology of general graphs, and Kratochvîl [17], [18] later followed with several useful results. The stimulus comes from applications of the idea in engineering, computer science and the related disciplines.

Products of graphs [6] are natural candidates where to seek perfect codes. Not surprisingly, they command a rich literature. In particular, the famous $r$-perfect Lee metric codes by Golomb and Welch [7] are over the Cartesian product of finitely many cycles. For later studies in this area, see Špacapan [22] and Mollard [21]. For $r$-perfect codes over the Kronecker product (also known as direct product and tensor product) of finitely many cycles, the author [11]–[13] presented several results that eventually led to a complete characterization by Žerovnik [25]. For analogous studies over the strong product and the lexicographic product, see Abay-Asmerom et al. [1] and Taylor [23], respectively.

Perfect codes have been a topic of study in several other contexts, notably, Cayley graphs and circulant graphs [4], [9], [20], Towers-of-Hanoi graphs [3], and Sierpinski graphs [16]. See Heden [8] for a survey of 1-perfect binary codes.

B. Definitions and Preliminaries

A graph connotes a finite, simple, undirected and connected graph. Let $G$ be a graph, and let $\text{dist}(u, v)$ denote the (shortest) distance between vertices $u$ and $v$ in $G$ [24]. Further, let $\text{dia}(G)$ denote the diameter of $G$, i.e., the largest of the distances between any two nodes in $G$.

For a vertex subset $S$ of a graph $G$, let $\langle S \rangle$ denote its closed neighborhood, i.e., $S \cup \{ x \in V(G) \mid x \text{ is adjacent to some vertex in } S \}$. $S$ is said to constitute a dominating set of $G$ if $\langle S \rangle = V(G)$. If, in addition, the distance between any two distinct elements of $S$ is at least three, then $S$ constitutes a 1-perfect code. Thus the closed neighborhoods of the vertices...
TABLE I
AN ILLUSTRATION OF DEFINITION 1.1 FOR 0 ≤ x ≤ 2^3 − 1

| x | x(0) | x(1) | x(2) |
|---|------|------|------|
| 0 | 1    | 2    | 4    |
| 1 | 0    | 3    | 5    |
| 2 | 3    | 0    | 6    |
| 3 | 2    | 1    | 7    |
| 4 | 5    | 6    | 0    |
| 5 | 4    | 7    | 1    |
| 6 | 7    | 4    | 2    |
| 7 | 6    | 5    | 3    |

in a 1-perfect code are mutually exclusive and collectively exhaustive.

The problem of obtaining a smallest dominating set is NP-complete, and so is the problem of deciding whether or not a graph admits a 1-perfect code [18]. For any undefined term, see West [24].

For n-bit binary strings x and y, let Ham(x, y) denote the Hamming distance between the two, i.e., the number of bit positions in which they differ from each other. The n-dimensional hypercube Q_n (also called the n-cube) is the graph on the vertex set \{0, 1\}^n, where nodes x and y are adjacent if Ham(x, y) = 1.

Let x · y (or xy) denote the concatenation of the binary strings x and y, and for sets X and Y of binary strings, let X · Y := \{xy | x ∈ X and y ∈ Y\}. Meanwhile let \(\mathbb{P} := 1 − a\), where \(a ∈ \{0, 1\}\).

**Definition 1.1:** For an n-bit binary string \(x = b_{n-1}...b_0\) (so \(0 ≤ x ≤ 2^n − 1\) in decimal), let \(x^{(a)}\) be the n-bit integer obtainable from x by replacing \(b_a\) by \(b^{!a}\), where \(0 ≤ a ≤ n−1\).

It is clear that \(x^{(0)}, ..., x^{(n−1)}\) are precisely the neighbors of x in \(Q_n\). See Table I for an illustration, where \(n = 3\), and x, \(x^{(0)}, x^{(1)}, x^{(2)}\) are in decimal.

**Definition 1.2:** For n-bit binary strings x and y, let \(x ⊕ y\) denote the n-bit string obtainable by the bitwise XOR operation between x and y. Further, for integers r and s, where \(0 ≤ r, s ≤ 2^n − 1\), let \(r ⊕ s\) denote the integer \(N(b(r) ⊕ b(s))\), where \(b(r)\) and \(b(s)\) are n-bit strings that represent r and s, respectively.

**Note:** A precise definition of \(N(x)\) appears below, x being a binary string.

**Proposition 1.1 (Gale [5]):**  
1) \(\bigoplus\) is commutative as well as associative.  
2) (Cancellation law) \(x ⊕ y = x ⊕ z\) iff \(y = z\).  
3) \(x ⊕ y \approx z\) iff \(y = x ⊕ z\).

**Remark:** The XOR operation between two bits is viewable as an addition modulo two.

**Proposition 1.2:** Let x and y be n-bit binary strings, and let \(0 ≤ a, b ≤ n−1\). Then  
1) \(x^{(a)} = x \bigoplus 2^a\).  
2) \(\text{Ham}(x, x^{(a)}) = 1\).  
3) If \(a ≠ b\), then \(\text{Ham}(x^{(a)}, x^{(b)}) = 2\).

**Definition 1.3:** For a set \(X\) of n-bit strings, let \(X^{(a)} = \{x^{(a)} | x ∈ X\}, 0 ≤ a ≤ n−1\).

**Proposition 1.3:** Let X and Y be sets of n-bit strings of equal cardinality. Then  
1) \(X^{(a)} = Y\) iff \(Y^{(a)} = X\).  
2) If \(X^{(a)} = Y\), then there exists a “perfect” matching between X and Y, given by \(x ⇔ x^{(a)}\).

**Definition 1.4:** For \(m ≥ 1\), the quad-cube \(CQ_m\) is a spanning subgraph of the hypercube \(Q_{4m+2}\). Its edge set is given by \(E_0 \cup E_1 \cup E_2 \cup E_3 \cup E_4\), where  
1) \(E_0 = \{ ux00, ux(0)00, ..., ux00, ux(m−1)00 | u ∈ \{0, 1\}^{3m} \text{ and } x ∈ \{0, 1\}^m \}\)  
2) \(E_1 = \{ ux01, ux(0)01, ..., ux01, ux(m−1)01 | u ∈ \{0, 1\}^{2m} \text{ and } x ∈ \{0, 1\}^m \}\)  
3) \(E_2 = \{ ux10, ux(0)10, ..., ux10, ux(m−1)10 | u, v ∈ \{0, 1\}^{m} \text{ and } x ∈ \{0, 1\}^{2m} \}\)  
4) \(E_3 = \{ ux11, ux(0)11, ..., ux11, ux(m−1)11 | u ∈ \{0, 1\}^{m} \text{ and } x ∈ \{0, 1\}^{3m} \}\), and  
5) \(E_4 = \{ u00, u01, \{ u00, u10, \{ u01, u11, \{ u10, u11 \}| \text{ } u, v ∈ \{0, 1\}^{4m} \}\}\)

**Definition 1.5:** The nodes of \(CQ_m\) are distinguishable into four types, as follows:  
- Type 0: those that are of the form u00 (binary) or 4i + 0 (decimal)  
- Type 1: those that are of the form u01 (binary) or 4i + 1 (decimal)  
- Type 2: those that are of the form u10 (binary) or 4i + 2 (decimal), and  
- Type 3: those that are of the form u11 (binary) or 4i + 3 (decimal).

Let \(e ∈ E(CQ_m)\). Call e an edge of Type i if \(e ∈ E_i, 0 ≤ i ≤ 3\), and call e a cross edge if \(e ∈ E_4\). See Figure 1 for a depiction of the five edge types. Meanwhile, a node of the hypercube/quad-cube is viewable both as a binary string, say, \(x\) and as the corresponding nonnegative integer \(N(x)\). A formula for the latter appears below.

**Theorem 1.4 ([19]):** \(CQ_m\) is a regular graph of degree \(m + 2\), and its diameter is equal to \(4(m + 1)\).

**Corollary 1.3:** If \(CQ_m\) admits a 1-perfect code, then \(m = 2^k − 3, k ≥ 2\).

**Proof:** \(CQ_m\) is a regular graph of degree \(m + 2\), so the closed neighborhood of each vertex in it consists of \(m + 3\) vertices. In that light, the existence of a 1-perfect code requires that \(m + 3\) divide \(V(CQ_m) = 2^{2m+1}\), i.e., \(m + 3\) must be a power of two. Hence the result.

The central objective of this paper is to prove that the converse of Corollary 1.5 holds true. For the special case of \(CQ_1\), see Figure 2, where nodes that are circled constitute a 1-perfect code of the graph. It is further clear from the depiction that this graph admits a vertex partition into such codes.
**Proposition 1.6 ([19]):** $CQ_m$ admits a vertex partition into a total of $2^{3m+2}$ $m$-cubes, segregated into four kinds as follows.

- **Collection 0** (based on the nodes of Type 0) in which the $i$-th cube is on the vertex set \( \{2^{m+2}i + 4a \mid 0 \leq a \leq 2^m - 1\} \), $0 \leq i \leq 2^{3m} - 1$.

- **Collection 1** (based on the nodes of Type 1) in which the $i$-th cube is on the vertex set \( \{2^{m+2}q + 4r + 1 + 2^{m+2}a \mid 0 \leq a \leq 2^m - 1\} \), where $0 \leq i \leq 2^{3m} - 1$, $q = \lfloor \frac{i}{2^m} \rfloor$, and $r = i \mod 2^m$.

- **Collection 2** (based on the nodes of Type 2) in which the $i$-th cube is on the vertex set \( \{2^{m+2}q + 4r + 2 + 2^{m+2}a \mid 0 \leq a \leq 2^m - 1\} \), $0 \leq i \leq 2^{3m} - 1$, $q = \lfloor \frac{i}{2^m} \rfloor$, and $r = i \mod 2^m$.

- **Collection 3** (based on the nodes of Type 3) in which the $i$-th cube is on the vertex set \( \{4i + 3 + 2^{3m+2}a \mid 0 \leq a \leq 2^m - 1\} \), $0 \leq i \leq 2^{3m} - 1$.

See Figure 3 for a set of certain 5-cubes in $CQ_5$.

**Definition 1.6:** For an integer $i$ and a set $S$ of integers, let $i + S$ denote the set $\{i + x \mid x \in S\}$. 
C. A Special Latin Square

An $r \times r$ Latin square is a matrix, in which each of $0, \ldots, r-1$ appears exactly once in each row and each column. Let $r$ be a power of two. For a permutation \( \left( \begin{array}{cccc} 0 & 1 & \cdots & r-1 \\ p_0 & p_1 & \cdots & p_{r-1} \end{array} \right) \), let \( L(p_0, \ldots, p_{r-1}) \) be the Latin square, defined below.

\[
L(p_{2i}, p_{2i+1}) = \left( \begin{array}{c} \frac{p_{2i}}{p_{2i+1}} \end{array} \right), \quad \text{where } i \geq 0, \text{ and}
\]

\[
L(p_0, \ldots, p_{r-1}) = \left( \begin{array}{c} \frac{L(p_0, \ldots, p_{s-1})}{L(p_0, \ldots, p_{r-1})} \end{array} \right),
\]

where \( r = 2^k; \ s = r/2; \) and \( k \geq 2. \)

It is not difficult to see that \( L(p_0, \ldots, p_{r-1}) \) is a well-defined, symmetric matrix.

**Definition 1.7:** Let \( M_r = L(0, \ldots, r-1) \), i.e., the \( r \times r \) Latin square on the identity permutation.

See Table II for \( M_4 \) and \( M_8 \).

**Proposition 1.7** (Gale [5], p. 192): \( M_r[i, j] = i \neq j \), where \( 0 \leq i, j \leq r - 1. \)

D. A Permutation Function \( \pi \)

**Definition 1.8:** Let \( r \) be a power of two, \( r \geq 4 \), and let

\[
\pi_4(i) = \begin{cases} 
0 & i = 0 \\
3 & i = 1 \\
2 & i = 2 \\
1 & i = 3 
\end{cases}
\]

and

\[
\pi_2(i) = \begin{cases} 
\pi_r(i) & 0 \leq i \leq (r/2) - 1 \\
( r + \pi_r(i - r/2) & r/2 \leq i \leq (3r/2) - 1 \\
\pi_r(i - r) & 3r/2 \leq i \leq 2r - 1. 
\end{cases}
\]

Here is how the \( \pi_{2r} \)-array is obtainable from the \( \pi_r \)-array:

- Copy the elements in the leftmost \( r/2 \) cells of the \( \pi_r \)-array to the leftmost cells (indexed 0 to \( r/2 - 1 \)) of the \( \pi_{2r} \)-array.
- Copy the elements in the rightmost \( r/2 \) cells of the \( \pi_r \)-array to the rightmost cells (indexed \( 3r/2 \) to \( 2r - 1 \)) of the \( \pi_{2r} \)-array, and
Add $r$ to each element of the $\pi_r$-array, and systematically copy the resulting elements to the cells in the “middle” segment (indexed $r/2$ to $(3r/2) - 1$) of the $\pi_{2r}$-array.

Let $P_r = L(\pi_r)$. See Figure 4 for the recursive structure of $P_{2r}$ vis-à-vis $P_r$. Further, $\pi_4$, $\pi_8$ and $\pi_{16}$ appear in Equation (1), shown at the bottom of the page, whereas $P_4$ and $P_8$ appear in Table III.

**Lemma 1.8:** The $i$-th element and the $(r - 1 - i)$-th element of the $\pi_r$-array differ in exactly the rightmost bit, i.e., $(\pi_r(i))^{(0)} = \pi_r(r - 1 - i)$, where $0 \leq i \leq r - 1$ and $r = 2^k$, $k \geq 2$.

**Proof:** Use induction on $r$. For $r = 4$, the claim follows by inspection of $\pi_4$. For the inductive step, recall the construction of the $\pi_{2r}$-array from the $\pi_r$-array that follows Definition 1.8, and make use of the fact that $(r + \pi_r(i))^{(0)} = r + (\pi_r(i))^{(0)}$, since $r = 2^k$, $k \geq 2$.

Observe next that the way $P_r$ is obtainable from $\pi_r$ is identical to the way $M_r$ is obtainable from the identity permutation, hence the following result.

**Proposition 1.9:** $P_r[i,j] = \pi_r(M_r[i,j]) = \pi_r(i \cup j)$, where $0 \leq i, j \leq r - 1$.

\[
\begin{align*}
\pi_4 &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 \\ 2 & 1 & 3 & 0 \end{pmatrix} \\
\pi_8 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 0 & 5 & 4 & 3 & 2 & 7 & 6 \\ 1 & 3 & 4 & 5 & 6 & 7 & 2 & 1 \\ 2 & 1 & 4 & 3 & 5 & 6 & 7 & 0 \end{pmatrix} \\
\pi_{16} &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 0 & 5 & 4 & 3 & 2 & 7 & 6 & 11 & 10 & 9 & 8 & 15 & 14 & 13 & 12 \\ 1 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 2 & 1 \\ 2 & 1 & 4 & 3 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 0 \end{pmatrix}
\end{align*}
\]
2) For \( r/2 \leq i \leq r-1 \), \( P_{2r}[i, 2r-2] = r + L[i - r/2, 0] \) and \( P_{2r}[i, 2r-2] = r + L[i - r/2, r/2 - 2] \). Let \( P_{2r}[i, 0] = r + x \), where \( L[i - r/2, 0] = x \). It is clear that \( 0 \leq x \leq r - 1 \). By induction hypothesis, \( L'[i - r/2, r/2 - 2] = x(1) \). It follows that \( P_{2r}[i, 2r-2] = r + x(1) = (r+x)(1) \).

3) For \( r \leq i < 3r/2 - 1 \), \( P_{2r}[i, 0] = r + L[i - r, 0] \) and \( P_{2r}[i, 2r-2] = r + L[i - r, r/2 - 2] \). The rest of the argument is similar to that in (2) above.

4) For \( 3r/2 \leq i \leq 2r - 1 \), \( P_{2r}[i, 0] = L'[i - 3r/2, 0] \) and \( P_{2r}[i, 2r-2] = L[i - 3r/2, r/2 - 2] \). The rest of the argument is similar to that in (1) above.

**Corollary 11.1:** If \( r = 2^k \), \( k \geq 2 \), then \( \{ \pi_r(i), (\pi_r(i))^1, (\pi_r(i))^1 \} \cap \{ \pi_r(i \not\subset 1), \ldots, \pi_r(i \not\subset (r - 3)) \} = \emptyset \), where \( 0 \leq i \leq r - 1 \).

**Corollary 11.2:** If \( r = 2^k \), \( k \geq 2 \), then \( \pi_r(i) \not\subset 1 = \pi_r(i \not\subset (r - 1)) \) and \( \pi_r(i) \not\subset 2 = \pi_r(i \not\subset (r - 2)) \), where \( 0 \leq i \leq r - 1 \).

**Proof:** Observe that \( \pi_r(i) \not\subset 1 = \pi_r(i)^0 \) and \( \pi_r(i) \not\subset 2 = \pi_r(i)^1 \). The claim is then immediate from Lemma 11.10.

**E. A Distinguishing Function \( \phi \)**

Let \( k \geq 3 \) and \( m = 2^k - 3 \).

**Definition 1.9:** Let \( p_0 = 0 \), and let \( p_1, \ldots, p_m \) be the integers between 1 and \( m \) that are not powers of two.

The statement of Definition 1.9 itself is well-defined in view of the fact that there are exactly \( k \) integers between 1 and \( m \) that are powers of two, viz., \( 2^0, \ldots, 2^{k-1} \). Here are \( p_0, p_1, \ldots, p_m \) for \( k = 4 \):

| \( p_0 \) | \( p_1 \) | \( p_2 \) | \( p_3 \) | \( p_4 \) | \( p_5 \) | \( p_6 \) | \( p_7 \) | \( p_8 \) | \( p_9 \) |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 3 | 5 | 6 | 7 | 9 | 10 | 11 | 12 | 13 |

**Definition 1.10:** let \( \phi : \{0, \ldots, 2^{m-1} - 1\} \rightarrow \{0, \ldots, 2^{k-1}\} \) be the map, where \( \phi(r) \) is equal to

- 0 if \( r = 0 \)
- \( p_{x+1} \) if \( r = 2^x \) and \( 0 \leq x \leq m - k - 1 \), and
- \( p_{x+1} \) if \( r = 2^x + \ldots + 2^{x_1} \), \( x_d \geq x_2 > \ldots > x_1 \geq 0 \) and \( 0 \leq d \leq m - k \).

where \( p_1, \ldots, p_m \) are as in Definition 1.9.

It is easy to see that \( \phi \) is well-defined. Next, \( \phi(2^x + \ldots + 2^{x_1}) = \phi(2^x) \vee \ldots \vee \phi(2^{x_1}) \). See Table IV for an illustration.

**Lemma 11.13:** If \( 0 \leq r \leq 2^{m-1} - k - 1 \), then \( \phi(r(x)) = (\phi(r) \vee p_{x+1}) \), where \( 0 \leq x \leq m - k - 1 \).

**Proof:** Note that \( r(x) \) is equal to either \( r + 2x \) or \( r - 2x \). First suppose that \( r(x) = r + 2x \), then \( \phi(r(x)) = \phi(r) \vee p_{x+1} \). Next suppose that \( r(x) = r - 2x \), \( r = r(x) + 2x \), whence \( \phi(r) \neq \phi(r(x)) \vee p_{x+1} \). By Prop. 1.1(3), \( \phi(r(x)) = \phi(r) \not\subset p_{x+1} \).

**Lemma 11.14:** If \( 0 \leq r \leq 2^{m-1} - k \), then \( \phi(r) \not\subset \phi(r(x)) \), where \( 0 \leq x \leq m - k - 1 \).

**Proof:** By Lemma 11.13, \( \phi(r(x)) = \phi(r) \vee p_{x+1} \). Further, \( p_{x+1} > 0 \) for all \( x \geq 0 \).

**Lemma 11.15:** If \( r_1 \neq r_2 \) and \( \phi(r_1) = \phi(r_2) \), then \( \text{Ham}(r_1, r_2) \geq 3 \), where \( 0 \leq r_1, r_2 \leq 2^{m-1} - k - 1 \).

**Proof:** Proceed by contradiction. First suppose that \( \text{Ham}(r_1, r_2) = 1 \), in which case \( |r_1 - r_2| = 2^t \) for some \( t \), so \( \phi(r_1) = \phi(r_2) \not\subset p_{t+1} \). Therefore, \( \phi(r_1) \neq \phi(r_2) \).

Next suppose that \( \text{Ham}(r_1, r_2) = 2 \). Without loss of generality, let \( r_1 \) and \( r_2 \) differ in the rightmost two bits. Then \( r_1 = xab \) (binary) and \( r_2 = x\bar{a}b \) (binary), where \( a, b \in \{0, 1\} \).

- Let \( a = 0 \) and \( b = 0 \). Then \( r_1 = 4x \) and \( r_2 = 4x + 3 \). In that light, \( \phi(r_1) = \phi(4x) \not\subset \phi(4x) \not\subset \phi(4x) \), whence \( \phi(r_1) \neq \phi(r_2) \).
- Let \( a = 0 \) and \( b = 1 \). Then \( r_1 = 4x + 1 \) and \( r_2 = 4x + 2 \). In that light, \( \phi(r_1) = \phi(4x) \not\subset \phi(4x) \not\subset \phi(4x) \), whence \( \phi(r_1) \neq \phi(r_2) \).

The other two cases are similar.

**F. Method of Attack**

The evolution of the 1-perfect code in this paper crucially relies upon a number of concepts and results. To that end, let \( n = 2^k - 1 \), \( k \geq 3 \), and \( m = n - 2 \).

At heart of the code construction is a scheme [15] that constructs Hamming codes using a Latin square. See Section II for the scheme itself. In a nutshell, it returns a partition.
of $V(Q_n)$ into Hamming codes, say, $V_0, \ldots, V_n$, each of cardinality $2^{n-k}$.

Other major concepts/results employed are as follows:

1) A mapping $\delta : \{0, \ldots, 2^m-1\} \rightarrow \{0, \ldots, 2^{k-1}\}$, where $\delta(j) = i$ iff $j \in W_i$, where $W_i$ itself is the collection of the numerically smallest first quarter of the elements of $V_i$ (see Definition 3.1).

2) A quadripartition of each $V_i$ into equal-size sets $A_i$, $B_i$, $C_i$ and $D_i$, based on elements of $V_i$ distinguishable modulo four (see Definition 3.2), and

3) Relationships among $V_0, \ldots, V_n$ (vide Results 3.1 through 3.9, particularly Theorem 3.7).

Section III presents the theoretical foundation of the overall procedure. It systematically builds upon the scheme of Section II, and derives a number of results that are crucial to the correctness of the claims in the sequel.

The code construction itself relies on a vertex partition $V_0, \ldots, V_m$ (vide Algorithm 1) into equal-size sets $A_i, B_i, C_i$ and $D_i$, which themselves come from a set among $V_0, \ldots, V_m$. Figure 5 depicts this idea.

The foregoing vertex partition is further refined in Section IV that also presents the scheme itself. (See Figure 10.) The four sections that come next are then devoted to proving that the set returned by the main scheme is indeed a 1-perfect code of the graph.

Section IX takes the final step of proving that $CQ_m$ admits a vertex partition into 1-perfect codes, whereas Section X presents certain concluding remarks.

II. A SCHEME TO CONSTRUCT HAMMING CODES

This section recapitulates a scheme [15] that builds Hamming codes over $Q_n$. See Algorithm 1.

**Theorem 2.1:** [15] For $n = 2^k - 1, k \geq 2$, Algorithm 1 returns a partition, say, $\langle V_0, \ldots, V_n \rangle$ of $V(Q_n)$ having the following properties:

1) $|V_i| = 2^n/(n+1), 0 \leq i \leq n,$ and

2) Every pair of two distinct elements in each set is at a Hamming distance of at least three, and the set is maximal with respect to this property.

Whereas any $(n+1) \times (n+1)$ Latin square (at Step 13 of Algorithm 1) would lead to a partition of $V(Q_n)$ into Hamming codes, the schemes in this paper exclusively employ the Latin square on the identity permutation, viz., $M_\cdot$. (See Definition 1.7 and Table II in Section I-C.) Further, the resulting vertex partition $\langle V_0, \ldots, V_n \rangle$ of $Q_n$ is referred to as the *canonical partition*, where $V_i = \{v_i,0, \ldots, v_i,r-1\}$, $r = 2^n/(n+1)$ and $0 \leq i \leq n$. Additionally, each $V_i$ is deemed to be sorted into the ascending order. See Tables V, VI and VII that illustrate the working of the algorithm.

![Fig. 5. Top-level vertex partition.](image-url)
TABLE V
Sets at Steps 2 - 4 and Steps 6 - 11 (N = 3) of Algorithm 1

| i   | Elements of \( V_i \) |
|-----|-----------------------|
| 0   | 0, 1, 7, 25, 30, 42, 45, 51, 52, 75, 76, 82, 85, 97, 102, 120, 127 |
| 1   | 1, 6, 24, 31, 43, 44, 50, 53, 74, 77, 83, 84, 96, 103, 121, 126 |
| 2   | 2, 5, 27, 28, 40, 47, 49, 54, 73, 78, 80, 87, 99, 100, 122, 125 |
| 3   | 3, 4, 26, 29, 41, 46, 48, 55, 72, 79, 81, 86, 98, 101, 123, 124 |
| 4   | 8, 15, 17, 22, 34, 37, 59, 60, 67, 68, 90, 93, 105, 110, 112, 119 |
| 5   | 9, 14, 16, 23, 35, 36, 58, 61, 66, 69, 91, 92, 104, 111, 113, 118 |
| 6   | 10, 13, 19, 20, 32, 39, 57, 62, 65, 70, 88, 95, 107, 108, 114, 117 |
| 7   | 11, 12, 18, 21, 33, 38, 56, 63, 64, 71, 89, 94, 106, 109, 115, 116 |

**Remark:** Algorithm 1 is extendable to a scheme that leads to an upper bound on the (independent) domination number of the hypercube that is within twice the optimal [15].

III. THEORETICAL FOUNDATION

This section derives a number of useful properties relating to the canonical partition \( \langle V_0, \ldots, V_n \rangle \). Let \( k \geq 3, n = 2^k - 1 \), and \( m = n - 2 \) throughout.

**Lemma 3.1:** There exists a “perfect matching” between each pair of distinct \( V_i \) and \( V_j \).

**Proof:** Let \( v \in V_i \), where \( 0 \leq i \leq n \). Because of the distance-three property of each \( V_j \) and the degree of \( v \) being equal to \( n \), it is easy to see that \( v \) has a unique neighbor in each \( V_j, j \neq i \). \( \square \)

**Lemma 3.2:** Let \( U_i, C_i \) and \( D_i \) be as in Algorithm 1, \( 0 \leq i \leq n \). Then

1) \( C_i^{(0)} = D_i \) (hence \( D_i^{(0)} = C_i \)), and
2) If \( U_i^{(a)} = U_j \), then \( C_i^{(a+1)} = D_j \) and \( D_i^{(a+1)} = C_j \), where \( 0 \leq a \leq n - 1 \).

**Proof:** Let \( r = 2^{n-k} \), and let \( U_i = \{ u_{i,0}, \ldots, u_{i,r-1} \} \), where \( |u_{i,k}| = n \) and \( 0 \leq r \leq r - 1 \).

1) It is clear that there exists a matching between sets \( C_i \) and \( D_i \) given by \( u_{i,k} \leftrightarrow u_{i,k} \), where \( b_{i,k} \in \{0, 1\} \), \( 0 \leq k \leq r - 1 \). Accordingly, \( C_i^{(0)} = D_i \).

2) Let \( U_i^{(a)} = U_j \), and note that \( C_i = \{ u_{i,0} \cdot b_{i,0}, u_{i,1} \cdot b_{i,1}, \ldots, u_{i,r-1} \cdot b_{i,r-1} \} \) and \( D_j = \{ u_{j,0} \cdot b_{j,0}, u_{j,1} \cdot b_{j,1}, \ldots, u_{j,r-1} \cdot b_{j,r-1} \} \). It is clear that \( u_{i,k} \) and \( u_{j,k} \) differ in exactly the \( a \)-th bit position, so they are of different parities. Therefore, \( b_{i,k} = 0 \) iff \( b_{j,k} = 1 \), i.e., \( b_{i,k} = \overline{b}_{j,k} \). It follows that \( u_{i,k} \cdot b_{i,k} \) and \( u_{j,k} \cdot \overline{b}_{j,k} \) differ in precisely the \( (a+1)\)-st bit position. Accordingly, \( C_i^{(a+1)} = D_j \). By a symmetrical argument, \( D_i^{(a+1)} = C_j \). \( \square \)

**Lemma 3.3:** For \( 0 \leq a \leq n - 1 \), \( (C_i \cup U_j)^{(a)} = C_i \cup U_j^{(a)} \) and \( (D_i \cup U_j)^{(a)} = D_i \cup U_j^{(a)} \), where \( C_i, D_i, U_j \) are as in Algorithm 1, and where \( 0 \leq i, j \leq n \).
Proof: Each binary string in $C_i$ (resp. $D_i$) is of length $n+1$, whereas that in $U_j$ is of length $n$. The claim then follows from the fact that $a$ is between 0 and $n-1$. □

Lemma 3.4: For $n \leq a \leq 2n$, $(C_i \cup U_j)^{(a)} = (C_i^{a(n-a)} \cup U_j)$ and $(D_i \cup U_j)^{(a)} = D_i^{a(n-a)} \cup U_j$, where $C_i$, $D_i$, and $U_j$ are as in Algorithm 1, and where $0 \leq i, j \leq n$.

Lemma 3.5: If $0 \leq d, i \leq n = 2^k - 1$, then

1) $(C_d \cup U_i)^{(x)} \cup \ldots \cup (C_d \cup U_i)^{(x)} = (C_d \cup U_i)^{(x)} \cup \ldots \cup (C_d \cup U_i)^{(x)}$, and

2) $(D_d \cup U_i)^{(x)} \cup \ldots \cup (D_d \cup U_i)^{(x)} = (D_d \cup U_i)^{(x)} \cup \ldots \cup (D_d \cup U_i)^{(x)}$.

Proof: First note that each of $(d \uplus 0, \ldots, d \uplus n)$ and $(i \uplus 0, \ldots, i \uplus n)$ is a permutation of $(0, \ldots, n)$. Next observe that $C_{d \uplus x}$ uniquely “conjugates” with $U_i$ in the expression $(C_{d \uplus 0} \cup U_i)^{(x)} \cup \ldots \cup (C_{d \uplus n} \cup U_i)^{(x)}$, where $0 \leq d, x \leq n$. Accordingly, $C_{d \uplus x}$ (that is equal to $C_x$) uniquely conjugates with $U_i$ for each $(d \uplus x)$. (1) follows. The argument for (2) is similar. □

Lemma 3.6: If $0 \leq x, y \leq n$, then $(x + n + 1) \uplus y = (n + 1) + (x \uplus y)$.

Proof: Note that $n + 1 = 2^k \leq (x + n + 1) \leq 2n + 1 = 2^{k+1} - 1$, so $x + n + 1 = 1u$ (binary), where $u$ is a k-bit number that is equal to $x$ (decimal). On the other hand, $y = 0v$ (binary), where $v$ is a k-bit number that is equal to $y$ (decimal). In that light, $(x + n + 1) \uplus y = (1u) \uplus (0v) = 1(u \uplus v)$, where $u \uplus v$ (in decimal) is equal to $2^k + N(u \uplus v) = (n + 1) + (x \uplus y)$. □

The following is a key result.

Theorem 3.7: $V_i^{(a)} = V_i \uplus (a+1)$, where $0 \leq i \leq n$; $0 \leq a \leq n - 1$; and $n = 2^k - 1, k \geq 2$.

Proof: Use induction on $n$, and make use of the notations as in Algorithm 1. For $n = 3$, see Figure 6, where $U_{-1}$ is $U_{1}$. $U_j$ stands for $U_j^{(1)}$.

The induction hypothesis states that $U_i^{(a)} = U_i \uplus (a+1)$, where $0 \leq i \leq n$ and $0 \leq a \leq n - 1$, whereas the induction step calls for proving that $V_i^{(a)} = V_i \uplus (a+1)$, where $0 \leq i \leq 2n + 1$ and $0 \leq a \leq 2n$.

There are four cases.

1) Let $0 \leq i \leq n$ and $0 \leq a \leq n - 1$. Then $V_i = (C_0 \cup U_i)^{(a)} \cup \ldots \cup (C_n \cup U_i)^{(n)}$, so $V_i^{(a)}$ is equal to $V_i^{(n)}$.

2) Let $0 \leq i \leq n$ and $0 \leq a \leq 2n$. Then $V_i^{(a)}$ is equal to $V_i^{(n)}$.

3) Let $n + 1 \leq i \leq 2n + 1$ and $0 \leq a \leq n - 1$. Then $V_i$ is equal to $V_i^{(n)}$.

4) Let $n + 1 \leq i \leq 2n + 1$ and $0 \leq a \leq 2n$. Then $V_i$ is equal to $V_i^{(n)}$.

In that light, $V_i^{(a)}$ is given by 

$$(D_0 \cup U_{(a-n+1)} \cup \ldots \cup (D_n \cup U_{(a-n+1)} \uplus U_i)^{(a)}$$

by Lemma 3.5(2).

In that case, $V_i^{(a-1)}$ is equal to $V_i \uplus (a+1)$ by Lemma 3.6.

Note that $i \uplus (a+1)$ in this case is of the form $1u$ (binary), where $u$ is a k-bit number. Therefore, $i \uplus (a+1)$ is between $n + 1$ and $2n + 1$ (decimal).

3) Let $n + 1 \leq i \leq 2n + 1$ and $0 \leq a \leq n - 1$. Then $V_i$ is equal to $V_i^{(n)}$.

4) Let $n + 1 \leq i \leq 2n + 1$ and $0 \leq a \leq 2n$. Then $V_i$ is equal to $V_i^{(n)}$.

In that light, $V_i^{(a)}$ is given by 

$$(D_0 \cup U_{(a-n+1)} \cup \ldots \cup (D_n \cup U_{(a-n+1)} \uplus U_i)^{(a)}$$

by Lemma 3.5(2).

In that case, $V_i^{(a-1)}$ is equal to $V_i \uplus (a+1)$ by Lemma 3.6.

Note that $i \uplus (a+1)$ in this case is of the form $1u$ (binary), where $u$ is a k-bit number. Therefore, $i \uplus (a+1)$ is between $n + 1$ and $2n + 1$ (decimal).

3) Let $n + 1 \leq i \leq 2n + 1$ and $0 \leq a \leq n - 1$. Then $V_i$ is equal to $V_i^{(n)}$.

4) Let $n + 1 \leq i \leq 2n + 1$ and $0 \leq a \leq 2n$. Then $V_i$ is equal to $V_i^{(n)}$.

In that light, $V_i^{(a)}$ is given by 

$$(D_0 \cup U_{(a-n+1)} \cup \ldots \cup (D_n \cup U_{(a-n+1)} \uplus U_i)^{(a)}$$

by Lemma 3.5(2).

In that case, $V_i^{(a-1)}$ is equal to $V_i \uplus (a+1)$ by Lemma 3.6.

Note that $i \uplus (a+1)$ in this case is of the form $1u$ (binary), where $u$ is a k-bit number. Therefore, $i \uplus (a+1)$ is between $n + 1$ and $2n + 1$ (decimal).

3) Let $n + 1 \leq i \leq 2n + 1$ and $0 \leq a \leq n - 1$. Then $V_i$ is equal to $V_i^{(n)}$.

4) Let $n + 1 \leq i \leq 2n + 1$ and $0 \leq a \leq 2n$. Then $V_i$ is equal to $V_i^{(n)}$.

In that light, $V_i^{(a)}$ is given by 

$$(D_0 \cup U_{(a-n+1)} \cup \ldots \cup (D_n \cup U_{(a-n+1)} \uplus U_i)^{(a)}$$

by Lemma 3.5(2).

In that case, $V_i^{(a-1)}$ is equal to $V_i \uplus (a+1)$ by Lemma 3.6.
Fig. 7. Illustrating various cases in the proof of Theorem 3.7.

\[ = (D_0 \bullet U_{i \geq 0} \cup \ldots \cup (D_n \bullet U_{i \leq n}), \]
\[ \text{where } j = i - (n + 1), \text{ so } 0 \leq j \leq n. \]

Accordingly, \( V_i^{(a)} \) is equal to
\[ (D_0 \bullet U_{j \geq 0}) \cup \ldots \cup (D_n \bullet U_{j \leq n}) \]
\[ \text{by Lemma 3.3} \]
\[ = (D_0 \bullet U_{j \geq 0}) \cup \ldots \cup (D_n \bullet U_{j \leq n}) \]
\[ \text{by induction hypothesis} \]
\[ = V_{(n+1)+j \geq (a+1)} \]
\[ \text{by Step 13 of Algorithm 1} \]
\[ = V_{(n+1)+j \geq (a+1)} \]
\[ = V_{j \geq (a+1)} \]
\[ \text{by Lemma 3.6} \]
\[ = V_{i \geq (a+1)}. \]

Analogous to (2) above, \( i \geq (a+1) \) in this case is between \( n+1 \) and \( 2n+1 \).

4) Let \( n+1 \leq i \leq 2n+1 \) and \( n \leq a \leq 2n \). Then \( V_i \) is equal to
\[ (D_0 \bullet U_{i-(n+1) \geq 0}) \cup \ldots \cup (D_n \bullet U_{i-(n+1) \leq n}) \]
\[ = (D_0 \bullet U_{j \geq 0}) \cup \ldots \cup (D_n \bullet U_{j \leq n}), \]
\[ \text{where } j = i - (n + 1), \text{ so } 0 \leq j \leq n. \]

In that light, \( V_j^{(a)} \) is equal to
\[ (D_0 \bullet U_{j \geq 0}) \cup \ldots \cup (D_n \bullet U_{j \leq n}) \]
\[ \text{by Lemma 3.4} \]
\[ = (C_{(a-n) \geq 0} \bullet U_{j \geq 0}) \cup \ldots \cup (C_{(a-n) \geq 0} \bullet U_{j \leq n}) \]
\[ \text{by a reasoning as in (2) above} \]
\[ = (C_0 \bullet U_{(a-n) \geq 0}) \cup \ldots \cup (C_n \bullet U_{(a-n) \leq n}) \]
\[ \text{by Lemma 3.5(1)} \]
\[ = V_{(a-n) \geq j} \]
\[ = V_{(a-n) \geq (i-(n+1))}. \]

Notice at this point that \( i \) and \( a+1 \), in this case, are representable in binary as \( 1u \) and \( 1v \), respectively, where \( u \) and \( v \) are \( k \)-bit numbers that denote \( (i-(n+1)) \) and \( (a-n) \), respectively. In that light, \( i \geq (a+1) = (1u \geq 1v) = u \geq v \), and is equal to \( (i-(n+1)) \geq (a-n) \).

It follows that \( V_i^{(a)} = V_i^{(b)} \). Meanwhile, \( i \geq (a+1) \), in this case, is between 0 and \( n \).

Figure 7 illustrates the four cases in the proof of Theorem 3.7 for the collection \( \{V_0, \ldots, V_7\} \) with respect to \( Q_7 \).

(See Table VII in Section II for descriptions of \( V_0, \ldots, V_7 \).)

**Lemma 3.8:** \( V_i^{(a)} = V_i^{(b)} \) iff \( a = b \), where \( 0 \leq i \leq n; 0 \leq a < b \leq n - 1 \); and \( n = 2^k - 1, k \geq 2 \).

**Proof:** Assume that \( V_i^{(a)} = V_i^{(b)} \). By Theorem 3.7 then, \( V_i^{(a+1)} = V_i^{(b+1)} \). It is clear that each of \( (i \leq (a+1)) \) and \( (i \leq (b+1)) \) is between 0 and \( n \). Also, \( x = y \) iff \( V_x = V_y \), where \( 0 \leq x, y \leq n \). It then follows that \( i \leq (a+1) = i \leq (b+1) \). By Prop. 1.1(2), \( a+1 = b+1 \), i.e., \( a = b \). The converse is obvious. \( \square \)

**Theorem 3.9:** For \( 0 \leq a \leq 2^{n-k-2} - 1, \) each “horizontal” block \( \{v_{i,4a}, v_{i,4a+1}, v_{i,4a+2}, v_{i,4a+3}\} \) of four consecutive nodes in each \( V_i \) contains one element each of Type 0, Type 1, Type 2, and Type 3 (not necessarily in that order), where \( 0 \leq i \leq n \).

**Proof:** Use induction on \( n \). For \( n = 7 \), the claim follows by an inspection of the sets in Table VII in Section II. Using the notations as in Algorithm 1, each element of \( V_i \)...
is of the form $u \cdot v$ (binary), where $u \in C_p$ (or $u \in D_p$) and $v \in U_q$ for some $p$ and $q$, with $|u| = n + 1$ and $|v| = n$. Notice that $N(uv) = 2^{|u|}N(u) + N(v)$, and that $0 \leq N(v) \leq 2^{|u|} - 1 < 2^{|u|}$. Accordingly, $N(uv) \equiv i \pmod{4}$ if $N(v) \equiv i \pmod{4}$, where $0 \leq i \leq 3$. By induction hypothesis, every block of four nodes (starting at an index divisible by four) in $U_q$ has the stated property. That property is, in turn, inherited by the set $C_p \cup U_q$ (or $D_p \cup U_q$) and the union of such disjoint sets. □

The next result shows that the elements in each $V_i$ are uniformly “spread out.”

**Theorem 3.10:** For $0 \leq i \leq n$, let

- $W_i = \{v \in V_i \mid 0 \leq v < 2^{n-i} - 1\}$
- $X_i = \{v \in V_i \mid 2^{n-i} \leq v < 2 \cdot 2^{n-i} - 1\}$
- $Y_i = \{v \in V_i \mid 2 \cdot 2^{n-i} \leq v < 3 \cdot 2^{n-i} - 1\}$, and
- $Z_i = \{v \in V_i \mid 3 \cdot 2^{n-i} \leq v \leq 4 \cdot 2^{n-i} - 1\}$.

Then $|W_i| = |X_i| = |Y_i| = \frac{1}{4}|V_i|$.

**Proof:** Recall that each element of each $V_i$ is between 0 and $2^n - 1$. Therefore, the sets $W_i$, $X_i$, $Y_i$, and $Z_i$ are well-defined. (See Figure 8 for an illustration.)

To prove the claim, use induction on $n$, the basis being clear from the sets that appear in Table VII in Section II. For the induction step, first examine the sets $C_i$ and $D_i$ in the “for” loop at Steps 6-11 in Algorithm 1, where $0 \leq i \leq n$. The elements in each such set are between 0 and $2^{n+i} - 1$.

By induction hypothesis, each of $U_0, \ldots, U_n$ (appearing at Step 5 of the algorithm) has the stated property. Note next that

1) If $x \in U_0$, then either $2x \in C_i$ and $2x + 1 \in D_i$, or $2x + 1 \in C_i$ and $2x \in D_i$,

2) For $0 \leq t \leq 3$, if $t2^{m+1} \leq x < (t + 1)2^{m+1} - 1$, then $t2^{m+1} \leq 2x < (t + 1)2^{m+1} - 1$.

It follows that each $C_i$ or $D_i$ admits a partition into four (sub)sets in which the elements range (i) from 0 to $2^{n-1} - 1$, (ii) from $2^{n-1}$ to $2 \cdot 2^{n-1} - 1$, (iii) from $2 \cdot 2^{n-1}$ to $3 \cdot 2^{n-1} - 1$, and (iv) from $3 \cdot 2^{n-1}$ to $4 \cdot 2^{n-1} - 1$, respectively.

Consider next the sets $C_a \cup U_b$ and $D_a \cup U_b$ that appear in the unions at Step 14 of Algorithm 1, where $0 \leq a, b \leq n$, and note that

1) $x \in C_a$ (resp. $D_a$) and $y \in U_b$ iff $2^n x + y \in C_a \cup U_b$ (resp. $D_a \cup U_b$),

2) if $x$ is in the first quarter (resp. second quarter, third quarter or fourth quarter) of $C_a$ or $D_a$, and $y \in U_b$,

It follows that each of $C_a \cup U_b$ and $D_a \cup U_b$ admits a partition into four subsets having the stated property. Finally, this property is seamlessly inherited by each union appearing at Step 14 of Algorithm 1.

**Corollary 3.11:** $W_i^a = W_i \cup (a+1)$, where $0 \leq i \leq n$ and $0 \leq a \leq n - 3$, and where $W_i$ is as in the statement of Theorem 3.10.

**Remark:** The sets $W_0, \ldots, W_n$ appear pretty frequently in the rest of the paper.

**Definition 3.1:** Let $d : \{0, \ldots, 2^m - 1\} \to \{0, \ldots, 2^k - 1\}$ be given by $d(i) = j$ iff $i \in W_j$.

See Figure 9 for an illustration of Definition 3.1.

**Corollary 3.12:** If $d(x) = d(y)$, $x \not= y$, then $H(x, y) \geq 3$.

**Lemma 3.13:** $d(i^{(t)}) = d(i) \times (t + 1)$, where $0 \leq i \leq 2^m - 1$ and $0 \leq t \leq m - 1$.

**Proof:** Note that $i$ is an $m$-bit integer, so $i^{(t)}$ itself is an $m$-bit integer, which is in $W_{d(i^{(t)})}$, vide Definition 3.1. Next, $i$ is in $W_{d(i)}$, so $i^{(t)}$ is in $W_{d(i^{(t)})} = W_{d(i) \times (t+1)}$, by Corollary 3.11. Note further that each of $d(i)$, $d(i^{(t)})$, and $t + 1$ is less than or equal to $m + 2 = 2^k - 1$. Therefore, $0 \leq d(i^{(t)}) \leq (t + 1) \leq 2^k - 1$. It follows that $d(i^{(t)}) = d(i) \times (t + 1)$.

**Corollary 3.14:** If $d(i) = d(j)$, then $d(i^{(a)}) = d(j^{(a)})$, where $0 \leq i, j \leq 2^m - 1$ and $0 \leq a \leq m - 1$.

**Definition 3.2:** For $0 \leq i \leq m + 2$, let

1) $A_i = \{x \in V_i \mid x \equiv 0 \pmod{4}\}$
2) $B_i = \{x \in V_i \mid x \equiv 1 \pmod{4}\}$
3) $C_i = \{x \in V_i \mid x \equiv 2 \pmod{4}\}$, and
4) $D_i = \{x \in V_i \mid x \equiv 3 \pmod{4}\}$.

By Theorem 3.9, $|A_i| = |B_i| = |C_i| = |D_i| = \frac{1}{4}|V_i| = 2^m/(m + 3) = 2^{m-k}$. Table VIII presents the sets $A_i$, $B_i$, $C_i$, and $D_i$, where $m = 5$ and $0 \leq i \leq 7$. Since each element in each $V_i$ is between $0^{m+2}$ and $1^{m+2}$ (binary), or between $0^{m+2} = (\text{decimal})$, so is each element in each of $A_i$, $B_i$, $C_i$, and $D_i$.

**Remark:** The sets $C_i$ and $D_i$ appearing in Definition 3.2 have nothing to do with those in the description of Algorithm 1.

**IV. THE MAIN SCHEME**

This section presents the main scheme that returns a 1-perfect code of $CQ_n$. See Algorithm 2. The scheme itself relies on successive vertex partitions of the graph, depicted in Figure 10 that, in turn, is viewable as a refinement of the partition that appeared in Figure 5 in Section I. As stated earlier, the smallest unit in the vertex partition is a set of the form $2^m x + \{0, \ldots, 2^m - 1\}$, of which a subset $2^{m+x} x \cup V_i$ is designated as a set of code elements, $0 \leq x \leq 2^{m-1} - 1$.

The next four sections are devoted to proving that the set returned by the main scheme is indeed a 1-perfect code of the graph.

**V. STEP 1**

This section focuses on the innermost two loops of the main scheme, which themselves appear in Algorithm 3 for a quick reference. It builds a code set that is a subset of $\bigcup_{x=0}^{2^m-1} \bigcup_{t=0}^{2^m-1} T_{a,b,c,d}$, where $T_{a,b,c,d}$ is as at Line 12 of Algorithm 2. As usual, $m = 2^k - 3$, $k \geq 3$. 
Algorithm 2 Main Scheme

Require: \( k \geq 3 \) and \( m = 2^k - 3 \)

1: \( Z = \emptyset \)
2: for \( (a = 0 \text{ to } 2^m - 1) \) do
3: \hspace{1em} let \( P_a = 2^{3m+2} a + \{0, \ldots, 2^{3m+2} - 1\} \)
4: \hspace{1em} Comment: \( |P_a| = 2^{3m+2} \); and \( P_0, \ldots, P_{2^m-1} \) constitute a partition of \( V(CQ_m) = \{0, \ldots, 2^{4m+2} - 1\} \).
5: for \( (b = 0 \text{ to } 2^{m-k}-1) \) do
6: \hspace{2em} let \( Q_{a,b} = 2^{3m+2} a + 2^{2m+k+2} b + \{0, \ldots, 2^{2m+k+2} - 1\} \)
7: \hspace{2em} Comment \( |Q_{a,b}| = 2^{2m+k+2} \); and \( Q_{a,0}, \ldots, Q_{a,2^{m-k}-1} \) constitute a partition of \( P_a \).
8: for \( (c = 0 \text{ to } 2^k-1) \) do
9: \hspace{3em} let \( R_{a,b,c} = 2^{3m+2} a + 2^{2m+k+2} b + 2^{2m+2} c + \{0, \ldots, 2^{2m+2} - 1\} \)
10: \hspace{3em} Comment \( |R_{a,b,c}| = 2^{2m+2} \); and \( R_{a,0,0}, \ldots, R_{a,b,c} = \{0, \ldots, 2^m - 1\} \) constitute a partition of \( Q_{a,b} \).
11: for \( (d = 0 \text{ to } 2^{m} - 1) \) do
12: \hspace{4em} let \( T_{a,b,c,d} = 2^{3m+2} a + 2^{2m+k+2} b + 2^{2m+2} c + 2^{m+2} d + \{0, \ldots, 2^{m+2} - 1\} \)
13: \hspace{4em} Comment \( |T_{a,b,c,d}| = 2^{m+2} \); and \( T_{a,0,0,0}, \ldots, T_{a,b,c,d} = \{0, \ldots, 2^m - 1\} \) constitute a partition of \( R_{a,b,c} \).
14: \hspace{1em} \( Z = Z \cup \{2^{3m+2} a + 2^{2m+k+2} b + 2^{2m+2} c + 2^{m+2} d + \{0, \ldots, 2^{m+2} - 1\}\} \)
15: \hspace{1em} Comment: \( V_0, \ldots, V_{m+2} \) are the sets as in the statement of Theorem 2.1 (vide Algorithm 1).
16: end for
17: end for
18: end for
19: end for
20: return \( Z \)

**Lemma 5.1:** If \( 0 \leq c \leq 2^k - 1 \) and \( 0 \leq d \leq 2^m - 1 \), then \( \langle 2^{m+2} (2^m c + d) + A_{\pi(c \not\in \delta(d))} \rangle \) consists of the following sets that are mutually disjoint:

1) \( 2^{m+2} (2^m c + d) + A_{\pi(c \not\in \delta(d))} \cap \{0, \ldots, 2^{m+2} - 1\} \cup B_{\pi(c \not\in \delta(d)) \cup \{m+1\}} \),
2) \( 2^{m+2} (2^m c + d) + A_{\pi(c \not\in \delta(d))} \cap \{0, \ldots, 2^{m+2} - 1\} \cup A_{\pi(c \not\in \delta(d)) \cap \{m+1\}} \).

**Proof:** \( \delta(d) \) is between 0 and \( 2^k - 1 \), and so is \( c \not\in \delta(d) \), hence \( \{c \not\in \delta(d) \not\subseteq \{0, \ldots, 2^k - 2\} \not\subseteq \{m+2\}\} \) is a permutation of \( \{0, \ldots, 2^k - 1\} \), and so must be \( \pi(c \not\in \delta(d)) \not\subseteq \{0, \ldots, 2^m - 2\} \) \( \not\subseteq \{m+2\} \).

Let \( x \in \langle 2^{m+2} (2^m c + d) + A_{\pi(c \not\in \delta(d))} \rangle \). Then \( 0 \leq x \leq (2^{m+2} (2^m c + d) + A_{\pi(c \not\in \delta(d))}) \). Each element of \( A_r \) being less
than or equal to $2^{m+2} - 1$ (where $0 \leq r \leq m + 2$), it is clear that $x = uv00$ (binary), where $u = 2^mc + d$ (decimal), $|u| = m + k$; $|v| = m$ and $v00 \in A_{π(c \lessdot δ(d))}$. The structure of $x$ is shown in Figure 11. Note that $x \equiv 0 \pmod{4}$. Here are the $m + 2$ neighbors of $uv00$ in $CQ_m$, vide Definition 1.4:

- $uv01$ and $uvt0$ (binary), and
- $uv(0)00, \ldots, uv(m-1)00$ (binary).

Observe that $v00 \in V_{π(c \lessdot δ(d))}$, so $(v00)(0) = v01$ is in $V_{π(c \lessdot δ(d))}$ that is equal to $V_{π(c \lessdot δ(d)) \cup \emptyset}$, by Theorem 3.7. Next, $v01 \equiv 1 \pmod{4}$, so $v01 \in B_{π(c \lessdot δ(d)) \cup \emptyset}$. Similarly, $(v00)(1) = v10 \in C_{π(c \lessdot δ(d)) \cup \emptyset}$.

By Corollary 1.12, $π(c \lessdot δ(d)) \cup \emptyset = π(c \lessdot δ(d)) \cup (m + 2)$ and $π(c \lessdot δ(d)) \cup 2 = π(c \lessdot δ(d)) \cup (m + 1)$. In that light, $v01 \in B_{π(c \lessdot δ(d)) \cup (m + 2)}$ and $v10 \in C_{π(c \lessdot δ(d)) \cup (m + 1)}$. By an argument as in the proof of Lemma 3.1, $v00$ is not adjacent to any other node in $V_{π(c \lessdot δ(d)) \cup (m + 1)}$ or $V_{π(c \lessdot δ(d)) \cup (m + 2)}$. Accordingly, $A_{π(c \lessdot δ(d))}$ is disjoint from $A_{π(c \lessdot δ(d)) \cup (m + 1)} \cup A_{π(c \lessdot δ(d)) \cup (m + 2)}$. Therefore, each of $v(0)00, \ldots, v(m-1)00$ belongs to a unique set among $A_{π(c \lessdot δ(d)) \cup \emptyset}, \ldots, A_{π(c \lessdot δ(d)) \cup m}$. It is easy to see that the sets involved are pairwise disjoint. The claim follows.

Figure 12 illustrates the argument in the proof of Lemma 5.1 for the case where $m = 5$, and where $X \rightarrow Y$ stands for (the binary relation) “Set $Y$ is dominated by Set $X$.”

**Corollary 5.2.** $(2^{m+2}(2mc + d) + A_{π(c \lessdot δ(d)) \cup (m + 1)})$ and $(2^m + (2mc + d) + A_{π(c \lessdot δ(d)) \cup (m + 2)})$ are not dominated by $(2^{m+2}(2mc + d) + A_{π(c \lessdot δ(d)) \cup (m + 1)})$.

**Corollary 5.3.** $(2^{m+2}(2mc + d) + A_{π(c \lessdot δ(d)) \cup (m + 1)})$ is a subset of $(2^{m+2}(2mc + d) + \brace{0, \ldots, 2^m - 1})$.

**Corollary 5.4.** If $0 \leq c_1, c_2 \leq 2^k - 1$ and $0 \leq d_1, d_2 \leq 2^m - 1$, where $c_1 \neq c_2$ or $d_1 \neq d_2$, then $(2^{m+2}(2mc_1 + d_1) + A_{π(c_1 \lessdot δ(d_1))}) \cup (2^{m+2}(2mc_2 + d_2) + A_{π(c_2 \lessdot δ(d_2))})$ are mutually disjoint.
Proof: If $c_1 \neq c_2$, then $2^m c_1 + d_1 \neq 2^m c_2 + d_2$. This is because $2^m > d_1, d_2$. An identical conclusion is reached if $c_1 = c_2$ and $d_1 \neq d_2$. The claim then follows from Lemma 5.1 and the fact that each element of each $A_x, B_y$ or $C_z$ is smaller than $2^m - 1$, where $0 \leq x, y, z \leq 2^k - 1$. □

Lemma 5.5: If $0 \leq c \leq 2^k - 1$ and $0 \leq d \leq 2^m - 1$, then $(2^{m+2}(2^m c + d) + B_{\pi(c \leq \delta(d))})$ consists of the following sets that are mutually disjoint:

1. $2^{m+2}c + 2^{m+2}d + B_{\pi(c \leq \delta(d) \leq (m+1)) \cup A_{\pi(c \leq \delta(d) \leq (m+2))}}$.
2. $(2^{m+2}c + 2^{m+2}d + B_{\pi(c \leq \delta(d) \leq (m+2)))})$.
3. $(2^{m+2}c + 2^{m+2}d + B_{\pi(c \leq \delta(d) \leq (m+3)))})$.

Proof: Let $x \in (2^{m+2}(2^m c + d) + B_{\pi(c \leq \delta(d))})$. Then $x = uv01$ (binary) where $u = 2^m c + d$ (decimal); $|u| = m + k$; $|v| = m$; and $v01 \in B_{\pi(c \leq \delta(d))}$. The structure of $x$ is similar to that of the node that appears in Figure 11, with the trailing “00” replaced by “01”. Note that $x = 1 (mod 4)$. Here are the $m + 2$ neighbors of $v01 \in CQ_m$:

- $uv11$ and $u000$ (binary), and
- $(2^{m+2}(2^m c + d) + v01), (2^{m+2}(2^m c + d + 1)) + v01),\ldots,(2^{m+2}(2^m c + d + 1)) + v01).

Note that $v01 \in V_{\pi(c \leq \delta(d))}$, so $(v01)1 = v11 \in V_{\pi(c \leq \delta(d))}$. Next, $v01 = 3 (mod 4)$, so $v11 \in D_{\pi(c \leq \delta(d)) \leq (m+1)) \cap \pi(c \leq \delta(d)) \leq (m+2))$. Each element of $D_{\pi(c \leq \delta(d) \leq (m+3)\cup A_{\pi(c \leq \delta(d) \leq (m+2))}}$ is smaller than $2^m - 1$. Notice that next $d$ is an $m$-bit integer, hence must be each of $d(0),\ldots,d(m-1)$. In that light, $(2^{m+2}(2^m c + d) + v01$ belongs to $(2^{m+2}(2^m c + d)) + B_{\pi(c \leq \delta(d))}$, $0 \leq t \leq m - 1$. Finally, it is easy to see that the sets involved are mutually disjoint.

Figure 13 illustrates the argument in the proof of Lemma 5.5 for the case where $m = 5$. Meanwhile, the following result is analogous to Corollary 5.4.

Corollary 5.6: If $0 \leq c_1, c_2 \leq 2^k - 1$ and $0 \leq d_1, d_2 \leq 2^m - 1$, where $c_1 \neq c_2$ or $d_1 \neq d_2$, then $(2^{m+2}(2^m c_1 + d_1) + B_{\pi(c_1 \leq \delta(d_1))})$ and $(2^{m+2}(2^m c_2 + d_2) + B_{\pi(c_2 \leq \delta(d_2))})$ are mutually disjoint.

Proof: First note that each element of $(2^{m+2}d + (2^m c + d))$ is smaller than $2^m$, and so is each element of $(2^{m+2}d(t) + B_x)$, where $0 \leq t \leq m - 1$. In that light, if $c_1 \neq c_2$, then $(2^{m+2}(2^m c_1 + d_1) + B_{\pi(c_1 \leq \delta(d_1))})$ and $(2^{m+2}(2^m c_2 + d_2) + B_{\pi(c_2 \leq \delta(d_2))})$ are mutually disjoint, vide Lemma 5.5.

Let $c_1 = c_2$ and $d_1 \neq d_2$ next.

1. If $\delta(d_1) = \delta(d_2)$, then $\text{Ham}(d_1, d_2) \geq 3$ (vide Corollary 3.12), so $\{d_1, d_1 + d_2, \ldots, d_1 + (m-1)\}$ is a subset of $\{d_2, d_2 + d_1, \ldots, d_2 + (m-1)\}$ and the claim follows.

2. If $\delta(d_1) \neq \delta(d_2)$, then $d_1 = d_2$ (for some $t$) is a distinct possibility; however, $D_{\pi(c_1 \leq \delta(d_1)) \leq (m+1)} \cap D_{\pi(c_2 \leq \delta(d_2)) \leq (m+1)} = 0$, and the claim follows.

Corollary 5.7: If $0 \leq c \leq 2^k - 1$ and $0 \leq d \leq 2^m - 1$, then $(2^{m+2}(2^m c + d) + B_{\pi(c \leq \delta(d))})$ is a subset of $2^{m+2}c + \{0, \ldots, 2^m - 2 \}$. Proof: Each of $2^{m+2}d$ and $2^{m+2}d(t), 2^{m+2}d(t)$, $2^{m+2}d(t)$ is less than or equal to $2^{m+2}d(t)$, and $2^{m+2}d(t)$ is a subset of $\{0, \ldots, 2^m - 2 \}$. Similarly, $(2^{m+2}(2^m c + d))$ is a subset of $\{0, \ldots, 2^m - 2 \}$, and so is $(2^{m+2}(2^m c(t) + d(t))$, $0 \leq x, y, z \leq 2^k - 1$; and $0 \leq t \leq m - 1$. The claim follows.

Corollary 5.8: If $0 \leq c \leq 2^k - 1$ and $0 \leq d \leq 2^m - 1$, then $2^{m+2}(2^m c + d) + B_{\pi(c \leq \delta(d))}$ is dominated by $2^{m+2}(2^m c + d(t)) + B_{\pi(c \leq \delta(d))}$, where $1 \leq t \leq m$. Proof: Let $1 \leq t \leq m$. By Lemma 5.5:

- $2^{m+2}(2^m c + d(t)) + B_{\pi(c \leq \delta(d))}$ is dominated by $2^{m+2}(2^m c + d(t)) + B_{\pi(c \leq \delta(d))}$.

Like $d(t)$, each of $d(t), \ldots, d(m-1)$ is between $0$ and $2^m - 1$. Also, $(d(t))^{-1} = d(t)$, so the statement obtainable by substituting $d(t)$ for $d(t)$ in (t) holds. The claim then follows by application of the following identity: $\delta(d(t)) = t$. □

Figure 14 illustrates the argument in the proof of Corollary 5.8 for the case where $m = 5$. As stated earlier, “X → Y” stands for (the binary relation) “Set Y is dominated by Set X.”
Lemma 5.9: If $0 \leq c \leq 2^k - 1$ and $0 \leq d \leq 2^m - 1$, then $(2^{m+2}(2^m c + d) + C_{\pi(c \leq \delta(d))})$ consists of the following sets that are mutually disjoint:

1. $2^{m+2}(2^m c + d)$ (binary),
2. $2^{m+2}(2^m c + d) + D_{\pi(c \leq \delta(d) \cup \{m+2\}}($,
3. $2^{m+2}(2^m c + d) + C_{\pi(c \leq \delta(d) \cup \{m+2\})}$,
4. $2^{m+2}(2^m c + d) + (C_{\pi(c \leq \delta(d))} \cup A_{\pi(c \leq \delta(d))} \cup \{m+1\} \cup D_{\pi(c \leq \delta(d))} \cup \{m+2\})).$

Proof: Let $x \in (2^{m+2}(2^m c + d) + C_{\pi(c \leq \delta(d))})$. Then $x = uv10$ (binary), where $u = 2^m c + d$ (decimal), $|v| = m$ and $v10 \in C_{\pi(c \leq \delta(d))}$. The structure of $x$ is similar to that of the node that appears in Figure 11, with the trailing “00” replaced by “10”. Note that $x \equiv 2 \pmod{4}$. Here are the $m + 2$ neighbors of $uv10$ in $CQ_m$, vide Definition 1.4:

- $uv10$ (binary)
- $(2^{m+2}(2^m c^{(0)}) + d) + v10$,
- $(2^{m+2}(2^m c^{(k-1)}) + d) + v10$,
- $2^{m+2}(2^m c^{(k+1)} + d) + v10$,
- $2^{m+2}(2^m c + d)$ + $v10$.

Since $c$ is a $k$-bit integer, so must be $c^{(0)}$, ..., $c^{(k-1)}$. The rest of the argument is similar to that in the proof of Lemma 5.5.

Figure 15 illustrates the argument in the proof of Lemma 5.9 for the case where $m = 5$.

Corollary 5.10: If $0 \leq c_1, c_2 \leq 2^k - 1$ and $0 \leq d_1, d_2 \leq 2^m - 1$, where $c_1 \neq c_2$ or $d_1 \neq d_2$, then $(2^{m+2}(2^m c_1 + d_1) + C_{\pi(c_1 \leq \delta(d_1))})$ and $(2^{m+2}(2^m c_2 + d_2) + C_{\pi(c_2 \leq \delta(d_2))})$ are mutually disjoint.

Proof: First let $d_1 \neq d_2$. Then $2^{m+2}(2^m c_1 + d_1) \neq 2^{m+2}(2^m c_2 + d_2)$, since $2^{m+2}(2^m c_1 + d_1) \mod 2^{m+2}$ is different from $2^{m+2}(2^m c_2 + d_2) \mod 2^{m+2}$. This and the fact that each element of $C_{\pi}$, $D_{\pi}$ or $A_{\pi}$ is smaller than $2^{m+2}$ together imply that $2^{m+2}(2^m p + d_1) + X$ and $2^{m+2}(2^m q + d_2) + Y$ are disjoint, even if $X = Y$, where $p \in \{c_1, c_1(0), \ldots, c_1(k-1)\}$, and $q \in \{c_2, c_2(0), \ldots, c_2(k-1)\}$. Similarly, $2^{m+2}(2^m c + d_1) + C_{\pi(c \leq \delta(d_1))}$ and $2^{m+2}(2^m c + d_2) + C_{\pi(c \leq \delta(d_2))}$ are disjoint, where $0 \leq t \leq m - k - 1$.

Next let $c_1 \neq c_2$ and $d_1 = d_2$. Then $\pi(c_1 \leq \delta(d_1))$ and $\pi(c_2 \leq \delta(d_2))$ are necessarily distinct. The claim follows. □

Corollary 5.11: If $0 \leq c \leq 2^k - 1$ and $0 \leq d \leq 2^m - 1$, then $2^{m+2}(2^m c + d) + C_{\pi(c \leq \delta(d))}$ is dominated by $2^{m+2}(2^m c^{(t-1)} + d) + C_{\pi(c \leq \delta(d))}$, where $1 \leq t \leq k$.

Proof: Similar to that of Corollary 5.8. □

Remark: The expression $c^{(t-1)}$ may be replaced by $c \leq 2^{t-1}$, vide Prop. 1.2(1).

Figure 16 illustrates the argument in the proof of Corollary 5.11 for the case where $m = 5$, where “?” indicates that the respective sets are yet to be defined.

Lemma 5.12: If $0 \leq c \leq 2^k - 1$ and $0 \leq d \leq 2^m - 1$, then $(2^{m+2}(2^m c + d) + D_{\pi(c \leq \delta(d))})$ consists of the following sets that are mutually disjoint:

1. $2^{m+2}(2^m c + d) + (D_{\pi(c \leq \delta(d))} \cup \{m+2\})$ (binary),
2. $2^{m+2}(2^m c + d) + (D_{\pi(c \leq \delta(d))} \cup \{m+2\})$,
3. $2^{m+2}(2^m c + d) + (D_{\pi(c \leq \delta(d))} \cup \{m+2\})$.

Proof: Let $x \in (2^{m+2}(2^m c + d) + D_{\pi(c \leq \delta(d))})$. Then $x = uv11$ (binary), where $u = 2^m c + d$ (decimal), $|v| = m$ and $v11 \in D_{\pi(c \leq \delta(d))}$. The structure of $x$ is similar to that of the node that appears in Figure 11, with the trailing “00”
replaced by “11”. Note that \( x \equiv 3 \pmod{4} \). Here are the m + 2 neighbors of \( uv11 \) in \( CQ \), vide Definition 1.4:

- \( uv10 \) and \( uv01 \) (binary), and
- \((2^{3m+2} + 2^{m+2}(2^mc + d) + v11), \ldots, (2^{4m+1} + 2^{m+2}(2^mc + d) + v11)\), the count being \( m \).

The rest of the argument is similar to that in the proof of Lemma 5.9.

Figure 17 illustrates the argument in the proof of Lemma 5.12 for \( m = 5 \), whereas Figure 18 depicts the statements of Lemmas 5.1(1)/5.5(1)/5.9(1)/5.12(1) for \( m = 5 \).

Based on the distance-three property, \( (2^{m+2}(2^mc + d) + V_{\pi(c \neq \delta(d))}) \) is equal to the union of \( (2^{m+2}(2^mc + d) + A_{\pi(c \neq \delta(d))}) \), \( (2^{m+2}(2^mc + d + B_{\pi(c \neq \delta(d))}) \), \( (2^{m+2}(2^mc + d) + C_{\pi(c \neq \delta(d))}) \), and \( (2^{m+2}(2^mc + d) + D_{\pi(c \neq \delta(d))}) \). Figure 19 depicts \( 2^7 \times 0 \times V0 \).

Corollary 5.13: If \( 0 \leq c, c_2 \leq 2k - 1 \) and \( 0 \leq d_1, d_2, d_3 \leq 2m - 1 \), then \( 2^{m+2}(2^mc + d_1) + D_{\pi(c_1 \neq \delta(d_1))} \) and \( 2^{m+2}(2^mc + d_2) + D_{\pi(c_2 \neq \delta(d_2))} \) are mutually disjoint.

Proof: Similar to that of Corollary 5.10.

Theorem 5.14: Algorithm 3 returns the set \( \bigcup_{c=0}^{m-1} \left( \bigcup_{d=0}^{m-1} (2^{m+2}(2^mc + d) + V_{\pi(c \neq \delta(d))}) \right) \) that dominates the following sets that are mutually disjoint:

1) The set of all elements of Type 0 between 0 and \( 2^{m+2+k-2} - 1 \), the count being \( 2^{m+k} \).
2) The set of all elements of Type 1 between 0 and \( 2^{m+k+2} \), the count being \( 2^{2m+k} \).
3) a) \( \bigcup_{c=0}^{2^k-1} \left( \bigcup_{d=0}^{m-1} \left( 2^{m+2}(2^mc + d) + (S_1 \cup S_2) \right) \right) \), where

\[ S_1 = C_{\pi(c \neq \delta(d) \leq (m+1))} \cup C_{\pi(c \neq \delta(d) \leq (m+2))} \]

\[ S_2 = C_{\pi(c \neq \delta(d) \leq (m+1))} \cup C_{\pi(c \neq \delta(d) \leq (m+2))} \]

i.e., \((3+2^k):2^{2m}\) elements of Type 2, between 0 and \( 2^{m+2+k-2} - 1 \), and

b) \((2^{m+k+2} + S) \cup \ldots \cup (2^{m+2}(2^mc + d) + V_{\pi(c \neq \delta(d))}) \), i.e., \((m-k):2^{2m}\) elements of Type 2, between \( 2^{m+k+2} \) and \( 2^{m+2+k} - 1 \).

4) a) \( \bigcup_{c=0}^{2^k-1} \left( \bigcup_{d=0}^{m-1} \left( 2^{m+2}(2^mc + d) + (D_{\pi(c \neq \delta(d) \leq (m+1))} \cup D_{\pi(c \neq \delta(d) \leq (m+2))} \right) \right) \), i.e.,

\[ 3 \cdot 2^{2m} \text{ elements of Type 3, between 0 and } 2^{m+k+2} - 1, \] and

b) \((2^{3m+2} + S) \cup \ldots \cup (2^{4m+1} + S) \), where \( S = \bigcup_{c=0}^{2^k-1} \left( \bigcup_{d=0}^{m-1} (2^{m+2}(2^mc + d) + C_{\pi(c \neq \delta(d))}) \right) \), i.e., \((m-2^k):2^{2m}\) elements of Type 3, between \( 2^{m+2} \) and \( 2^{m+2+k} - 1 \).

Proof: Let \( 0 \leq c \leq 2k - 1 \) and \( 0 \leq d \leq 2m - 1 \).

1) By Lemmas 5.1(1-2), 5.9(1), and 5.1(1), \( 2^{m+2}(2^mc + d) + A_{\pi(c \neq \delta(d) \leq (m+2))} \) dominated by \( 2^{m+2}(2^mc + d + A_{\pi(c \neq \delta(d))}) \), \( (2^{3m+2} + S) \cup \ldots \cup (2^{4m+1} + S) \), where \( S = \bigcup_{c=0}^{2^k-1} \left( \bigcup_{d=0}^{m-1} (2^{m+2}(2^mc + d) + D_{\pi(c \neq \delta(d))}) \right) \), i.e., \( m^2:2^{2m}\) elements of Type 3, between \( 2^{m+2} \) and \( 2^{m+2+k} - 1 \).

By Corollary 5.8 and the fact that \( \delta(d^{t-1}) = \delta(d) \neq t \), \( 2^{m+2}(2^mc + d) + B_{\pi(c \neq \delta(d) \leq (m+2))} \) dominated by \( 2^{m+2}(2^mc + d + B_{\pi(c \neq \delta(d))}) \).

i.e., \((m-k):2^{2m}\) elements of Type 2, between \( 2^{m+k+2} \) and \( 2^{m+2+k} - 1 \), the count being \( 2^{2m+k} \).
JHA: 1-PERFECT CODES OVER THE QUAD-CUBE

Fig. 19. Depicting \( \mathbf{b} = 2^7 \), \( \mathbf{c} = 2^{12} \), \( \mathbf{d} = 2^{17} \)

3) a) By Lemmas 5.9(1), 5.1(1) and 5.12(1),
\[
2^{m+2}(2^m c + d) + \left( C_{\pi(c \leq \delta(d) \leq m)} \cup C_{\pi(c \leq \delta(d) \leq (m+1))} \cup C_{\pi(c \leq \delta(d) \leq (m+2))} \right)
\]
is dominated by \( 2^{m+2}(2^m c + d) + V_{\pi(c \leq \delta(d))} \).

By Corollary 5.11 next, \( (2^{m+2}(2^m c + d) + C_{\pi(c \leq \delta(d) \leq (m+1))} \cup C_{\pi(c \leq \delta(d) \leq (m+2))}) \) is dominated by \( 2^{m+2}(2^m c + d) + V_{\pi(c \leq \delta(d))} \).

b) Immediate from Lemma 5.9(3).

4) a) By Lemmas 5.12(1), 5.5(1) and 5.9(1),
\[
2^{m+2}(2^m c + d) + \left( D_{\pi(c \leq \delta(d) \leq m)} \cup D_{\pi(c \leq \delta(d) \leq (m+1))} \cup D_{\pi(c \leq \delta(d) \leq (m+2))} \right)
\]
is dominated by \( 2^{m+2}(2^m c + d) + V_{\pi(c \leq \delta(d))} \).

b) Immediate from Lemma 5.12(2).

It is easy to see that the sets involved are mutually disjoint.

Corollary 5.15: Among elements between 0 and \( 2^{2m+k+2} - 1 \), those in the following sets are not dominated by the set returned by Algorithm 3:
The objective of the present section is to slowly "spread the wings" beyond what appeared in Section V. See Algorithm 4 that subsumes Algorithm 3. In particular, it returns a code set that is a subset of $\bigcup_{c=0}^{2^{k-1}} \bigcup_{d=0}^{2^{m-k}} T_{a,b,c,d}$, where $0 \leq b \leq 2^{m-k} - 1$. (See Line 12 of Algorithm 2 for the definition of $T_{a,b,c,d}$.) As usual, $k \geq 3$ and $m = 2^k - 3$.

**Algorithm 4 Innermost Two Loops of Algorithm 2**

**Require:** Integer $b$ between 0 and $2^{m-k} - 1$

1. $S = \emptyset$;
2. **for** $(c = 0$ to $2^{k-1})$ **do** $\triangleright 2^k - 1 = m + 2$
3. **for** $(d = 0$ to $2^{m-k} - 1)$ **do**
4. $S = S \cup \left( \bigcup_{c=0}^{2^{k-1}} \left( \bigcup_{d=0}^{2^{m-k}+2} (2^{m-k} \cdot 2^{2m+c+d}) + V_{\pi(\phi(b) \leq c \leq d))} \right) \right)$
5. **end for**
6. **end for**
7. **Comment:** At this point, $|S| = 2^{m-k} + 2$
8. **return** $S$

**Theorem 6.1:** For an arbitrary but fixed integer $b$ between 0 and $2^{m-k} - 1$, Algorithm 4 returns the set $\bigcup_{c=0}^{2^{k-1}} \left( \bigcup_{d=0}^{2^{m-k}+2} (2^{m-k} \cdot 2^{2m+c+d}) + V_{\pi(\phi(b) \leq c \leq d))} \right)$ that dominates the following sets that are mutually disjoint:

1. The set of all elements of Type 0 between $2^{m-k+2} b$ and $2^{m-k+2} (b+1) - 1$, the count being $2^{m-k}$.
2. The set of all elements of Type 1 between $2^{m-k+2} b$ and $2^{m-k+2} (b+1) - 1$, the count being $2^{m-k}$.
3. a) $2^{m-k+2} b + \bigcup_{c=0}^{2^{k-1}} \left( \bigcup_{d=0}^{2^{m-k}+2} (2^{2m+c+d} + V_{\pi(\phi(b) \leq c \leq d))} \right)$, where
   - $S_1 = C_{\pi(\phi(b) \leq c \leq d))} \cup C_{\pi(\phi(b) \leq c \leq d))} \cup C_{\pi(\phi(b) \leq c \leq d))} \cup C_{\pi(\phi(b) \leq c \leq d))}$
   - $S_2 = C_{\pi(\phi(b) \leq c \leq d))} \cup C_{\pi(\phi(b) \leq c \leq d))} \cup C_{\pi(\phi(b) \leq c \leq d))} \cup C_{\pi(\phi(b) \leq c \leq d))}$

**Algorithm 5 Innermost Three Loops of Algorithm 2**

**Require:** $m = 2^k - 3$, $k \geq 3$

1. $S = \emptyset$;
2. **for** $(b = 0$ to $2^{m-k} - 1)$ **do**
3. **for** $(c = 0$ to $2^{k-1})$ **do**
4. **for** $(d = 0$ to $2^{m-k} - 1)$ **do**
5. $S = S \cup (2^{2m-k+2} b + 2^{m-k+2} c + 2^{m-k+2} d + 2^{2m-k+2} b + 2^{m-k+2} c + 2^{m-k+2} d)$
6. **end for**
7. **end for**
8. **end for**
9. **Comment:** At this point, $|S| = 2^{m-k} + 2$
10. **return** $S$

**Theorem 6.2:** Among the elements between $2^{m-k+2} b$ and $2^{m-k+2} (b+1) - 1$, those in the following sets are not dominated by the set returned by Algorithm 4:

1. $2^{m-k+2} b + 2^{m-k+2} (2^{2m+c+d}) + C_{\pi(\phi(b) \leq c \leq d))} \cup C_{\pi(\phi(b) \leq c \leq d))} \cup \ldots \cup C_{\pi(\phi(b) \leq c \leq d))}$, the number of elements being equal to $(m-k) \cdot 2^{2m}$, and
2. $2^{m-k+2} b + 2^{m-k+2} (2^{m-k+2} b)$, the number of elements being equal to $m \cdot 2^{2m}$, where $0 \leq b \leq 2^{m-k} - 1$, $0 \leq c \leq 2^k - 1$, $0 \leq d \leq 2^m - 1$, and $p_1, \ldots, p_{m-k}$ are as in Definition 1.9.

**Proof:** The arguments in this case are practically identical to those in the proof of Theorem 5.14.

This follows is analogous to Corollary 5.15.

**Corollary 6.2:** Among the elements between $2^{m-k+2} b$ and $2^{m-k+2} (b+1) - 1$, those in the following sets are not dominated by the set returned by Algorithm 4:

1. $2^{m-k+2} b + 2^{m-k+2} (2^{2m+c+d}) + C_{\pi(\phi(b) \leq c \leq d))} \cup C_{\pi(\phi(b) \leq c \leq d))} \cup \ldots \cup C_{\pi(\phi(b) \leq c \leq d))}$, the number of elements being equal to $(m-k) \cdot 2^{2m}$, and
2. $2^{m-k+2} b + 2^{m-k+2} (2^{m-k+2} b)$, the number of elements being equal to $m \cdot 2^{2m}$, where $0 \leq b \leq 2^{m-k} - 1$, $0 \leq c \leq 2^k - 1$, $0 \leq d \leq 2^m - 1$, and $p_1, \ldots, p_{m-k}$ are as in Definition 1.9.

**VII. Step 3**

This section focuses on the inner three loops of the main scheme, viz., Algorithm 2 of Section IV. In the process, it builds a code set that is a subset of $\bigcup_{c=0}^{2^{k-1}} \left( \bigcup_{d=0}^{2^{m-k}+2} T_{a,b,c,d} \right)$. See Algorithm 5. As usual, $k \geq 3$ and $m = 2^k - 3$.

See Figure 21 for the basic element used in Algorithm 5.
Lemma 7.1: If
\[
0 \leq b \leq 2^{m-k} - 1; \quad 0 \leq c \leq 2^k - 1; \quad \text{and} \quad 0 \leq d \leq 2^m - 1,
\]
then \(2^{m+k+2}b + 2^m + 2(2^mc + d) + \mathcal{A}_{\phi(b) \not\equiv c \not\equiv \delta(d) \not\equiv 0} \cup \mathcal{A}_{\phi(b) \not\equiv c \equiv \delta(d) \not\equiv \delta((m+1))} \cup \mathcal{B}_{\phi(b) \not\equiv c \equiv \delta(d) \equiv \delta((m+2))} \), and

\[
2^{m+k+2}b + 2^m + 2(2^mc + d) + \left( \bigcup_{t=1}^m \mathcal{A}_{\phi(b) \not\equiv c \equiv \delta(d) \not\equiv \delta(t)} \right).
\]

Proof: Similar to that of Lemma 5.1.

Corollary 7.2: If \(0 \leq b_1, b_2 \leq 2^{m-k} - 1; \quad 0 \leq c_1, c_2 \leq 2^k - 1; \quad \text{and} \quad 0 \leq d_1, d_2 \leq 2^m - 1; \quad \text{where} \quad (b_1 \neq b_2 \text{ or } c_1 \neq c_2 \text{ or } d_1 \neq d_2), \quad \text{then} \quad \left(2^{m+k+2}b_1 + 2^m + 2(2^mc_1 + d_1) + \mathcal{A}_{\phi(b_1) \not\equiv c_1 \equiv \delta(d_1)} \right) \quad \text{and} \quad \left(2^{m+k+2}b_2 + 2^m + 2(2^mc_2 + d_2) + \mathcal{A}_{\phi(b_2) \not\equiv c_2 \equiv \delta(d_2)} \right)
\]
are mutually disjoint.

Proof: If \(b_1 \neq b_2\), then the claim follows from the fact that \(2^{m+k+2}\) is greater than \(2^m + 2(2^mc + d)\) for all \(c\) and \(d\), where \(c \leq 2^k - 1\) and \(d \leq 2^m - 1\). On the other hand,
if \(b_1 = b_2\) and \((c_1 \neq c_2\) or \(d_1 \neq d_2\)\), then the claim follows from the proof of Corollary 5.4.

**Lemma 7.3.** If \(0 \leq b \leq 2^{m-k} - 1\); \(0 \leq c \leq 2^{k-1}\); and \(0 \leq d \leq 2^{m-1} - 1\), then \(2^{m-k+2} b + 2^{m-2} (2^{m-1} c + d) + B_{\pi(b)}(c, d)\) is among the following sets that are mutually disjoint:

1. \(2^{m-k+2} b + 2^{m-2} (2^{m-1} c + d) + \left( B_{\pi(b)}(c, d) + D_{\pi(b)}(c, d) \right) \cup A_{\pi(b)}(c, d) \subseteq \delta(d) \cup \delta(m+1) \cup \left( \pi(b) \right) \subseteq \delta(d) \subseteq \delta(m+2))\), and
2. \(\pi(b) \subseteq \delta(d)\).

**Proof:** Similar to that of Lemma 5.5.

**Corollary 7.4.** If \(0 \leq b_1, b_2 \leq 2^{m-k} - 1\); \(0 \leq c_1, c_2 \leq 2^{k-1}\); and \(0 \leq d_1, d_2 \leq 2^{m-1} - 1\), where \((b_1 \neq b_2\) or \(c_1 \neq c_2\) or \(d_1 \neq d_2\)), then \(2^{m-k+2} b_1 + 2^{m-2} (2^{m-1} c_1 + d_1) + B_{\pi(b_1)}(c_1, d_1)\) and \(2^{m-k+2} b_2 + 2^{m-2} (2^{m-1} c_2 + d_2) + B_{\pi(b_2)}(c_2, d_2)\) are mutually disjoint.

**Proof:** Make use of an argument as in the proof of Corollary 7.2, and invoke Corollary 5.6.

**Lemma 7.5.** If \(0 \leq b \leq 2^{m-k} - 1\); \(0 \leq c \leq 2^{k-1}\); and \(0 \leq d \leq 2^{m-1} - 1\), then \(2^{m-k+2} b + 2^{m-2} (2^{m-1} c + d) + C_{\pi(b)}(c, d)\) consists of the following sets that are mutually disjoint:

- \(X(b, c, d) := 2^{m-k+2} b + 2^{m-2} (2^{m-1} c + d) + (C_{\pi(b)}(c, d) \subseteq D_{\pi(b)}(c, d) \subseteq \delta(d) \subseteq \delta(m+1)) \cup A_{\pi(b)}(c, d) \subseteq \delta(m+2))\),
- \(Y(b, c, d) := 2^{m-k+2} b + \bigcup_{t=0}^{m-1} (2^{m-2} (2^{m-1} c + d) + C_{\pi(b)}(c, d) \subseteq \delta(d) \subseteq \delta(m+1))\),
- \(Z(b, c, d) := \bigcup_{t=0}^{m} (2^{m-2} (2^{m-1} c + d) + C_{\pi(b)}(c, d) \subseteq \delta(d) \subseteq \delta(m+1))\).

**Proof:** Similar to that of Lemma 5.9.

The following result is analogous to Corollary 5.8.

**Corollary 7.6.** If \(0 \leq b \leq 2^{m-k} - 1\); \(0 \leq c \leq 2^{k-1}\); and \(0 \leq d \leq 2^{m-1} - 1\), then \(2^{m-k+2} b + 2^{m-2} (2^{m-1} c + d) + C_{\pi(b)}(c, d)\) is among the following sets that are mutually disjoint:

1. \(X(b, c, d) := 2^{m-k+2} b + 2^{m-2} (2^{m-1} c + d) + (C_{\pi(b)}(c, d) \subseteq D_{\pi(b)}(c, d) \subseteq \delta(d) \subseteq \delta(m+1)) \cup A_{\pi(b)}(c, d) \subseteq \delta(m+2))\),
2. \(Y(b, c, d) := \bigcup_{t=0}^{m-1} (2^{m-2} (2^{m-1} c + d) + C_{\pi(b)}(c, d) \subseteq \delta(d) \subseteq \delta(m+1))\),
3. \(Z(b, c, d) := \bigcup_{t=0}^{m} (2^{m-2} (2^{m-1} c + d) + C_{\pi(b)}(c, d) \subseteq \delta(d) \subseteq \delta(m+1))\).

**Proof:** First note the following:

- If \(b_1 = b_2\) (in which case \(c_1 = c_2\) or \(d_1 = d_2\)), then the claim follows from Corollary 5.10.
- If \(b_1 \neq b_2\) and \(b_1 \neq b_2\), then \(C_{\pi(b)}(c, d) \subseteq \delta(d) \subseteq \delta(m+1)\).

In what follows, let \(1 \leq b \leq 2^{m-k+2} b + 2^{m-2} (2^{m-1} c + d) + C_{\pi(b)}(c, d) \subseteq \delta(d) \subseteq \delta(m+1)\) and \(2^{m-k+2} b + 2^{m-2} (2^{m-1} c + d) + C_{\pi(b)}(c, d) \subseteq \delta(d) \subseteq \delta(m+1)\).

**Theorem 7.10:** Algorithm 5 returns the set \(\bigcup_{b=0}^{2^{m-k-1}} (2^{m-k+2} b + \bigcup_{c=0}^{2^{m-1}} (2^{m-k+2} b + 2^{m-2} (2^{m-1} c + d) + V_{\pi(b)}(c, d) \subseteq \delta(d)))\) that dominates the following sets that are mutually disjoint:

1. The set of all elements of Type 0, between 0 and \(2^{3m-2} - 1\), the count being \(2^{3m}\).
2. The set of all elements of Type 1, between 0 and \(2^{3m-2} - 1\), the count being \(2^{3m}\).
3) The set returned by Algorithm 5 is a superset of those not dominated by the set returned by Algorithm 4, vide Theorem 7.10(4), the count being $2^{3m+2}$.

4) a) Immediate from Lemmas 7.8(1), 7.3(1) and 7.5(1).

The disjointness of the sets in this case follows from Corollary 7.7.

b) Immediate from Lemmas 7.8(2).

The disjointness of various sets in this case follows from Corollary 7.9.

Figure 22 presents the count of the elements of Type 3, dominated by the set returned by Algorithm 5. Meanwhile the following is analogous to Corollary 5.15 and Corollary 6.2.

**Corollary 7.11:** Among the elements between $2^{3m+2} - 2$ and $2^{3m+2} - 1$, the following are not dominated by the set returned by Algorithm 5, vide Theorem 7.10:

1) The set of elements of Type 0 between $2^{3m+2}$ and $2^{3m+2} - 2$, the count being $2^{3m+2}(2^m - 1)$.

2) The set of elements of Type 1 between $2^{3m+2}$ and $2^{3m+2} - 1$, the count being $2^{3m+2}(2^m - 1)$.

3) The set of elements of Type 2 between $2^{3m+2}$ and $2^{3m+2} - 2$, the count being $2^{3m+2}(2^m - 1)$.

4) The set of elements of Type 3 between 0 and $2^{3m+2} - 1$, other than those appearing in the statement of Theorem 7.10(4), the count being $2^{3m+2}(2^m - 1)$.

VIII. Step 4

This section zeroes in on the main result. See Algorithm 6 that is a miniature of Algorithm 2 in Section IV. Further, see Figure 23 for the element used in this section. As usual, $k \geq 3$ and $m = 2^k - 3$.

**Algorithm 6 Main Scheme (Algorithm 2) in a Miniature Form**

1: $Z = \emptyset$;
2: for $(a = 0$ to $2^m - 1)$ do
3: \hspace{1cm} for $(b = 0$ to $2^{m-k} - 1)$ do
4: \hspace{2cm} for $(c = 0$ to $2^k - 1)$ do
5: \hspace{3cm} for $(d = 0$ to $2^k - 1)$ do
6: \hspace{4cm} $Z = Z \cup (2^{3m+2} a + 2^{3m+k+2} b + 2^{3m+2} c + 2^{3m+2} d + V_{\delta}(a, b, c, d))$
7: \hspace{3cm} end for
8: \hspace{2cm} end for
9: \hspace{1cm} end for
10: end for
11: end for
12: Comment: At this point, $|Z| = 2^{4m-k+2}$.
13: return $Z$;
Fig. 22. Count of the elements of Type 3, vide Theorem 7.10(4).

Fig. 23. Structure of an element used in Algorithm 6.

d₁ ≠ d₂, then \(2^{3m+2} a_1 + 2^{2m+k+2} b_1 + 2^{m+2}(2m + c + d) + 4v + x \) and \(2^{3m+2} a_2 + 2^{m+k+2} b_2 + 2^{m+2}(2m + c + d) \) are mutually disjoint.

Proof: Similar to that of Lemma 7.3.

Lemma 8.3: If \(0 ≤ a ≤ 2^m - 1; 0 ≤ b ≤ 2^{m-k} - 1; 0 ≤ c ≤ 2^{k-1}; 0 ≤ d ≤ 2^{m-1} \), then \(2^{3m+2} a + 2^{m+k+2} b + 2^{m+2}(2m + c + d) + 4v + x \) consists of the following sets that are mutually disjoint:

1) \(2^{3m+2} a + 2^{m+k+2} b + 2^{m+2}(2m + c + d) + B(π(d(a) \cap φ(b) \cap c \cap δ(d))) \) and \(B(π(d(a) \cap φ(b) \cap c \cap δ(d))) \) are mutually disjoint.

Proof: Similar to that of Lemma 7.3.

Corollary 8.4: If \(0 ≤ a_1, a_2 ≤ 2^m - 1; 0 ≤ b_1, b_2 ≤ 2^{m-k} - 1; 0 ≤ c_1, c_2 ≤ 2^{k-1}; 0 ≤ d_1, d_2 ≤ 2^{m-1} \), then \(2^{3m+2} a_1 + 2^{m+k+2} b_1 + 2^{m+2}(2m + c_1 + d_1) + B(π(d(a) \cap φ(b) \cap c_1 \cap δ(d))) \) and \(2^{3m+2} a_2 + 2^{m+k+2} b_2 + 2^{m+2}(2m + c_2 + d_2) + B(π(d(a) \cap φ(b) \cap c_2 \cap δ(d))) \) are mutually disjoint.

Proof: Similar to that of Corollary 7.4.

Lemma 8.5: If \(0 ≤ a ≤ 2^m - 1; 0 ≤ b ≤ 2^{m-k} - 1; 0 ≤ c ≤ 2^{k-1}; 0 ≤ d ≤ 2^{m-1} \), then \(2^{3m+2} a + 2^{m+k+2} b + 2^{m+2}(2m + c + d) + C(π(d(a) \cap φ(b) \cap c \cap δ(d))) \) consists of the following sets that are mutually disjoint:

1) \(X(a, b, c, d) := 2^{3m+2} a + 2^{m+k+2} b + 2^{m+2}(2m + c + d) + C(π(d(a) \cap φ(b) \cap c \cap δ(d))) \) and \(A(π(d(a) \cap φ(b) \cap c \cap δ(d))) \) are mutually disjoint.

Proof: Similar to that of Lemma 5.12.

The following result is analogous to Corollary 5.8 as well as Corollary 7.6.

Corollary 8.8: If \(0 ≤ a ≤ 2^m - 1; 0 ≤ b ≤ 2^{m-k} - 1; 0 ≤ c ≤ 2^{k-1}; 0 ≤ d ≤ 2^{m-1} \), then \(2^{3m+2} a + 2^{m+k+2} b + 2^{m+2}(2m + c + d) + D(π(d(a) \cap φ(b) \cap c \cap δ(d))) \) is dominated by \(2^{3m+2} a^{(t−1)} + 2^{m+k+2} b + 2^{m+2}(2m + c + d) + D(π(d(a) \cap φ(b) \cap c \cap δ(d))) \), where \(1 ≤ t ≤ m \).
Corollary 8.9: If $0 \leq a_1, a_2 \leq 2^m - 1; 0 \leq b_1, b_2 \leq 2^{m-k} - 1; 0 \leq c_1, c_2 \leq m + 2$; and $0 \leq d_1, d_2 \leq 2^m - 1$; where $(a_1 \neq a_2$ or $b_1 \neq b_2$ or $c_1 \neq c_2$ or $d_1 \neq d_2$), then $(2^{m+2}+a_1+2^{m+k+2}b_1+2^{m}+2^{m+1}c_1+d_1)+D_π(\delta(a) \cup \phi(b) \cup c \cup \delta(d))$ and $(2^{m+2}+a_2+2^{m+k+2}b_2+2^{m}+2^{m+1}c_2+d_2)+D_π(\delta(a) \cup \phi(b) \cup c \cup \delta(d))$ are mutually disjoint.

Proof: If $a_1 = a_2$ (in which case $b_1 \neq b_2$, or $c_1 \neq c_2$, or $d_1 \neq d_2$), then the claim follows from Corollary 7.9. On the other hand, if $a_1 \neq a_2$, then the claim follows from the facts that (i) $2^{m+2}$ is greater than the maximum of $2^{m+k+2} b + 2^{m}+2^{m+k+2} c + d + 2^{m+2} - 1$, (ii) $2^{m+k+2}$ is greater than the maximum of $2^{m+2}(2^{m+c} + d) + 2^{m+2} - 1$, and (iii) $2^{m+2}$ is greater than each element of $D_x, B_y$ or $C_z$, where $0 \leq b \leq 2^{m-k} - 1, 0 \leq c \leq 2^k - 1$, and $0 \leq d \leq 2^m - 1$.

Theorem 8.10: Algorithm 6 returns the set $Z$ that is equal to

$\bigcup_{a=0}^{2^{m+1}-1} \bigcup_{b=0}^{2^{m-1}} \bigcup_{d=0}^{m-1} \bigcup_{c=0}^{m+3} \bigcup_{d=0}^{m+3}$

having cardinality $2^{4m-k-2}$, and that dominates all vertices of $CQ_1$.

Proof: The set $Z$ dominates all vertices of Type 0, Type 1 and Type 2. This follows by arguments similar to those in the proofs of Theorems 7.10(1), 7.10(2), and 7.10(3), respectively. In what follows, consider the vertices of Type 3, and let $0 \leq a \leq 2^m - 1; 0 \leq b \leq 2^m - 1; 0 \leq c \leq 2^k - 1; \text{ and } 0 \leq d \leq 2^m - 1$. By Lemmas 8.7, 8.5 and 8.3, the set

$(2^{m+2}+a + 2^{m+k+2}b + 2^{m+2}(2^{m+c} + d)) + D_π(\delta(d) \cup \phi(b) \cup c \cup \delta(d) \cup (m+1))) \cup D_π(\delta(d) \cup \phi(b) \cup c \cup \delta(d) \cup (m+2))$

is dominated by

$(2^{m+2}+a + 2^{m+k+2}b + 2^{m+2}(2^{m+c} + d)) + C_π(\delta(d) \cup \phi(b) \cup c \cup \delta(d) \cup (m+3))$

The sets that remain are as follows:

- $(2^{m+2}+a + 2^{m+k+2}b + 2^{m+2}(2^{m+c} + d))$
- $D_π(\delta(a) \cup \phi(b) \cup c \cup \delta(d) \cup (m+1))$
- $D_π(\delta(a) \cup \phi(b) \cup c \cup \delta(d) \cup (m+2))$
- $D_π(\delta(a) \cup \phi(b) \cup c \cup \delta(d) \cup (m+3))$

By Corollary 8.8, $(2^{m+2}+a + 2^{m+k+2}b + 2^{m+2}(2^{m+c} + d))$ is dominated by $(2^{m+2}+a(t-1) + 2^{m+k+2}b + 2^{m+2}(2^{m+c} + d)) + D_π(\delta(a(t-1)) \cup \phi(b) \cup c \cup \delta(d))$, where $1 \leq t \leq m$. Observe that the latter set is a subset of the set returned by Algorithm 6.

Corollary 8.11: 1) $CQ_1$ admits a 1-perfect code.

2) The (independent) domination number of $CQ_1$ is equal to the theoretical minimum of $2^{4m-k+2}$.

IX. VERTEX PARTITION OF THE QUAD-CUBE INTO 1-PERFECT CODES

It turns out that the main scheme admits a generalization. See Algorithm 7, where a new parameter $t$ has been introduced, $0 \leq t \leq 2^k - 1$.

Algorithm 7 The General Algorithm

Require: $m = 2^k - 3, k \geq 3$, and $t \in \{0, \ldots, 2^k - 1\}$

1: $Z = \emptyset$;
2: if $t = 0$ to $2^k - 1$ do
3: for $t = 0$ to $2^k - 1$ do
4: for $c = 0$ to $2^k - 1$ do
5: for $d = 0$ to $2^k - 1$ do
6: $Z = Z \cup (2^{m+2}+a + 2^{m+k+2}b + 2^{m+2}c + d) + D_π(\delta(d) \cup \phi(b) \cup c \cup \delta(d) \cup (t-1))$
7: end for
8: end for
9: end for
10: end for
11: end for
12: Comment: At this point, $|Z| = 2^{4m-k+2}$.
13: return $Z$;

Theorem 9.1: Algorithm 7 returns a 1-perfect code of $CQ_1$.

Proof: Algorithm 7 differs from Algorithm 6 at Step 7, where $V_π(\delta(a) \cup \phi(b) \cup c \cup \delta(d))$ has been replaced by $V_π(\delta(a) \cup \phi(b) \cup c \cup \delta(d) \cup (t-1))$, $0 \leq t \leq 2^k - 1$. It is easy to see that $0 \leq π(\delta(a) \cup \phi(b) \cup c \cup \delta(d) \cup (t-1)) \leq 2^k - 1$.

By symmetry, every claim relating to the set returned by Algorithm 6 holds true with respect to the set returned by Algorithm 7. Hence the result.

Corollary 9.2: If $m = 2^k - 3, k \geq 2$, then $CQ_1$ admits a vertex partition into 1-perfect codes.

Proof: See Figure 2 in Section I for a vertex partition of $CQ_1$ ($m = 3$ and $k = 2$) into 1-perfect codes. In what follows, let $k \geq 3$.

For every quadruple $(a,b,c,d)$, if $t_1 \neq t_2$, then $π(\delta(a) \cup \phi(b) \cup c \cup \delta(d) \cup (t_1))$ is different from $π(\delta(a) \cup \phi(b) \cup c \cup \delta(d) \cup (t_2))$, hence $V_π(\delta(a) \cup \phi(b) \cup c \cup \delta(d) \cup (t_1))$ and $V_π(\delta(a) \cup \phi(b) \cup c \cup \delta(d) \cup (t_2))$ are disjoint, where $a, b, c, d$ are as in Algorithm 7 and $0 \leq t_1, t_2 \leq 2^k - 1$. In that light, run Algorithm 7 systematically for $t$ ranging from $0$ to $2^k - 1$. Each time, it returns a 1-perfect code of the graph, vide Theorem 9.1. Further, the $2^k$ sets thus obtainable are vertex-disjoint. It is easy to see that the codes collectively constitute a vertex partition of the graph.

X. CONCLUDING REMARKS

A quad-cube $CQ_m$ is a special case of a more general topology, called the metacube [19] that itself is derivable from the hypercube. This paper presents a vertex partition of $CQ_m$ into 1-perfect codes, where $m = 2^k - 3, k \geq 2$. In an earlier study [14], the author presented an analogous result over the dual-cube that is a simpler version of the metacube.

There exist other more complex versions of the metacube, notably, the oct-cube that merit a similar study.

ACKNOWLEDGMENT

The author sincerely thanks the anonymous referees and Associate Editor Xiande Zhang for their helpful comments on
the earlier draft that led to an improvement in the presentation of the article.

REFERENCES

[1] G. Abay-Asmerom, R. H. Hammack, and D. T. Taylor, "Perfect r-codes in strong products of graphs," Bull. Inst. Combin. Appl., vol. 55, pp. 66–72, 2009.

[2] N. Biggs, "Perfect codes in graphs," J. Combinat. Theory, B, vol. 15, no. 3, pp. 289–296, 1973.

[3] P. Cull and I. Nelson, "Error-correcting codes on the towers of Hanoi graphs," Discrete Math., vol. 208–209, pp. 157–175, Oct. 1999.

[4] R. Feng, H. Huang, and S. Zhou, "Perfect codes in circulant graphs," Discrete Math., vol. 340, no. 7, pp. 1522–1527, Jul. 2017.

[5] D. Gale, Tracking the Automatic ANT (A Collection of Mathematical Entertainments Columns from The Mathematical Intelligencer). New York, NY, USA: Springer, 1998.

[6] R. Hammack, W. Imrich, and S. Klavžar, Handbook of Product Graphs, 2nd ed. Boca Raton, FL, USA: CRC Press, 2011.

[7] S. W. Golomb and L. R. Welch, "Perfect codes in the Lee metric and the packing of polyominoes," SIAM J. Appl. Math., vol. 18, no. 2, pp. 302–317, 1970.

[8] O. Heden, "A survey of perfect codes," Adv. Math. Commun., vol. 2, no. 2, pp. 223–247, 2008.

[9] H. Huang, B. Xia, and S. Zhou, "Perfect codes in Cayley graphs," SIAM J. Discrete Math., vol. 32, no. 1, pp. 548–559, Jan. 2018.

[10] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[11] P. K. Jha, "Smallest independent dominating sets in Kronecker products of cycles," Discrete Appl. Math., vol. 113, nos. 2–3, pp. 303–306, Oct. 2001.

[12] P. K. Jha, "Perfect r-domination in the Kronecker product of three cycles," IEEE Trans. Circuits Syst. I, Fundam. Theory Appl., vol. 49, no. 1, pp. 89–92, Aug. 2002.

[13] P. K. Jha, "Perfect r-domination in the Kronecker product of two cycles, with an application to diagonal/toroidal mesh," Inf. Process. Lett., vol. 87, no. 3, pp. 163–168, Aug. 2003.

[14] P. K. Jha, "1-perfect codes over dual-cubes vis-à-vis Hamming codes over hypercubes," IEEE Trans. Inf. Theory, vol. 61, no. 8, pp. 4259–4268, Aug. 2015.

[15] P. K. Jha and G. Slutzki, "A scheme to construct distance-three codes using Latin squares, with applications to the n-cube," Inf. Process. Lett., vol. 55, no. 3, pp. 123–127, Aug. 1995.

[16] S. Klavžar, U. C. Milutinović, and C. Petr, “1-perfect codes in Sierpiński graphs,” Bull. Austral. Math. Soc., vol. 66, no. 3, pp. 369–384, 2002.

[17] J. Kratochvíl, “Perfect codes over graphs,” J. Combinat. Theory, B, vol. 40, no. 2, pp. 224–228, Apr. 1986.

[18] J. Kratochvíl, "Regular codes in regular graphs are difficult," Discrete Math., vol. 133, nos. 1–3, pp. 191–205, Oct. 1994.

[19] Y. Li, S. Peng, and W. Chu, "Metacube—A versatile family of interconnection networks for extremely large-scale supercomputers," J. Supercomput., vol. 53, no. 2, pp. 329–351, Aug. 2010.

[20] C. Martínez, R. Beivide, and E. M. Gabidulin, "Perfect codes for metrics induced by circulant graphs," IEEE Trans. Inf. Theory, vol. 53, no. 9, pp. 3042–3052, Sep. 2007.

[21] M. Mollard, "On perfect codes in Cartesian products of graphs," Eur. J. Combinatorics, vol. 32, no. 3, pp. 398–403, Apr. 2011.

[22] S. Špacapan, "Optimal Lee-type local structures in Cartesian products of cycles and paths," SIAM J. Discrete Math., vol. 21, no. 3, pp. 750–762, Jan. 2007.

[23] D. T. Taylor, "Perfect r-codes in lexicographic products of graphs," Ars Combin., vol. 93, pp. 215–223, Oct. 2009.

[24] D. B. West, Introduction to Graph Theory, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2001.

[25] J. Žerovnik, "Perfect codes in direct products of cycles—A complete characterization," Adv. Appl. Math., vol. 41, no. 2, pp. 197–205, Aug. 2008.

Pranava K. Jha attended the Bihar Institute of Technology, Sindhri; Jawaharlal Nehru University, New Delhi; and Iowa State University, Ames, IA, USA. He is grateful to Dr. Giora Slutzki and Dr. Jonathan D.H. Smith for their help and encouragement during and after his graduate studentship at Iowa State University. In equal measure, he is thankful to Dr. K. B. Lakshmanan (formerly at SUNY at Brockport, NY, USA) for his help during the master’s work.

He taught computer science at St. Cloud State University, St. Cloud, MN, USA, from early 2001 to late 2014. Earlier, he worked at several academic institutions, including the North Eastern Regional Institute of Science and Technology, Itanagar; the Delhi Institute of Technology, Delhi (rechristened as Netaji Subhas University of Technology, Delhi); and Multimedia University, Melaka. His publications are in the areas of hypercubes, median graphs, products of graphs, and related disciplines that admit a number of applications in the digital world. Interestingly, vertex partition and edge decomposition constitute an underlying theme of a major part of his research. A paper on median graphs, jointly by him and Giora Slutzki, earned a citation in Combinatorial Algorithms, Part 1 (Don Knuth’s Vol. 4A).

Dr. Jha is a member of Upsilon, Pi, Epsilon.